Ubuntu Server Guide

Ubuntu Server Guide

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). A list of contributors is below.

Contributors to this document are:

- Members of the *Ubuntu Documentation Project*[2]
- Members of the *Ubuntu Server Team*[3]
- Contributors to the *Community Help Wiki*[4]
- Other contributors can be found in the revision history of the *serverguide*[5] and *ubuntu-docs*[6] bzr branches available on Launchpad.

[1] https://creativecommons.org/licenses/by-sa/3.0/
[2] https://launchpad.net/~ubuntu-core-doc
[3] https://launchpad.net/~ubuntu-server
[4] https://help.ubuntu.com/community/
[5] https://bazaar.launchpad.net/~ubuntu-core-doc/serverguide/trunk/changes
[6] https://bazaar.launchpad.net/~ubuntu-core-doc/ubuntu-docs/trunk/changes

Table of Contents

List of Tables

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].

[1] https://help.ubuntu.com/16.04/installation-guide/

[2] https://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 *Ubuntu Advantage*[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.ubuntu.com/management

[4] http://www.ubuntu.com/support

Chapter 2. Installation

This chapter provides a quick overview of installing Ubuntu 16.04 LTS Server Edition. For more detailed instructions, please refer to the *Ubuntu Installation Guide*[1].

[1] https://help.ubuntu.com/16.04/installation-guide/

1. Preparing to Install

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

1.1. System Requirements

Ubuntu 16.04 LTS Server Edition supports three (3) major architectures: Intel x86, AMD64 and ARM. 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	CPU	RAM	Hard Drive Space	
			Base System	All Tasks Installed
Server (Standard)	1 gigahertz	512 megabytes	1.5 gigabyte	2.5 gigabytes
Server (Minimal)	300 megahertz	256 megabytes	1.5 megabytes	2.5 gigabytes

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 and the installation process.

1.2.1. Kernel Differences:

Ubuntu version 10.10 and prior, actually had different kernels for the server and desktop editions. Ubuntu no longer has separate -server and -generic kernel flavors. These have been merged into a single -generic kernel flavor to help reduce the maintenance burden over the life of the release.

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-4.4.0-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 19, Backups [p. 321]* 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. Installation

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

- Download the appropriate ISO file from the *Ubuntu web site*[3].
- Boot the system from media (e.g. USB key) containing the ISO file.
- At the boot prompt you will be asked to select a language.
- From the main boot menu there are some additional options to install Ubuntu Server Edition. You can install a basic Ubuntu Server, check the CD-ROM for defects, check the system's RAM, boot from first hard disk, or rescue a broken system. The rest of this section will cover the basic Ubuntu Server install.
- The installer asks which language it should use. Afterwards, you are asked to select your location.
- Next, the installation process begins by asking for your keyboard layout. You can ask the installer to attempt auto-detecting it, or you can select it manually from a list.
- The installer then discovers your hardware configuration, and configures the network settings using DHCP. If you do not wish to use DHCP at the next screen choose "Go Back", and you have the option to "Configure the network manually".
- Next, the installer asks for the system's hostname.
- A new user is set up; this user will have *root* access through the sudo utility.
- After the user settings have been completed, you will be asked if you want to encrypt your `home` directory.
- Next, the installer asks for the system's Time Zone.
- You can then choose from several options to configure the hard drive layout. Afterwards you are asked which disk to install to. You may get confirmation prompts before rewriting the partition table or setting up LVM depending on disk layout. If you choose LVM, you will be asked for the size of the root logical volume. For advanced disk options see *Section 4, “Advanced Installation” [p. 10]*.
- The Ubuntu base system is then installed.
- 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*: this 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. 32]*.
  - *Manage the system with Landscape*: Landscape is a paid service provided by Canonical to help manage your Ubuntu machines. See the *Landscape*[4] site for details.

[3] http://www.ubuntu.com/download/server/download

[4] http://landscape.canonical.com/

- You now have the option to install, or not install, several package tasks. See *Section 2.1, “Package Tasks” [p. 7]* for details. Also, there is an option to launch aptitude to choose specific packages to install. For more information see *Section 4, “Aptitude” [p. 30]*.
- 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].

2.1. Package Tasks

During the Server Edition installation you have the option of installing additional packages. 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 packages 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 Java server: Installs Apache Tomcat and needed dependencies.
- Virtual Machine host: Includes packages needed to run KVM virtual machines.
- Manually select packages: Executes aptitude allowing you to individually select packages.

Installing the package groups is accomplished using the tasksel utility. One of the important differences 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
```

[5] https://help.ubuntu.com/16.04/installation-guide/

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
bind9utils
bind9
```

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 media and from a terminal:

```
sudo tasksel 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 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.

For further stability of a LTS release there is a slight change in behaviour if you are currently running a LTS version. LTS systems are only automatically considered for an upgrade to the next LTS via do-release-upgrade with the first point release. So for example 14.04 will only upgrade once 16.04.1 is released. If you want to update before, e.g. on a subset of machines to evaluate the LTS upgrade for your setup the same argument as an upgrade to a dev release has to be used via the *-d* switch.

4. Advanced Installation

4.1. Software RAID

Redundant Array of Independent Disks "RAID" is a method of using multiple disks to provide different balances of increasing data reliability and/or increasing input/output performance, depending on the RAID level being used. 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. This section will guide you through installing Ubuntu Server Edition using two RAID1 partitions on two physical hard drives, one for */* and another for *swap*.

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. This partition will be the *swap* partition, and a general rule for swap size is twice that of RAM. Enter the partition size, then choose *Primary*, then *Beginning*.

   

   A swap partition size of twice the available RAM capacity may not always be desirable, especially on systems with large amounts of RAM. Calculating the swap partition size for servers is highly dependent on how the system is going to be used.
5. Select the *"Use as:"* line at the top. By default this is *"Ext4 journaling file system"*, change that to *"physical volume for RAID"* then *"Done setting up partition"*.
6. For the */* partition once again select *"Free Space"* on the first drive then *"Create a new partition"*.
7. Use the rest of the free space on the drive and choose *Continue*, then *Primary*.
8. As with the swap partition, select the *"Use as:"* line at the top, changing it to *"physical volume for RAID"*. Also select the *"Bootable flag:"* line to change the value to *"on"*. Then choose *"Done setting up partition"*.
9. Repeat steps three through eight for the other disk and partitions.

4.1.2. RAID Configuration

With the partitions setup the arrays are 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 MD device"*.
4. For this example, select *"RAID1"*, but if you are using a different setup choose the appropriate type (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.

   For the *swap* partition choose *sda1* and *sdb1*. Select *"Continue"* to go to the next step.
8. Repeat steps *three* through *seven* for the */* partition choosing *sda2* and *sdb2*.
9. 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.

1. Select *"#1"* under the *"RAID1 device #0"* partition.
2. Choose *"Use as:"*. Then select *"swap area"*, then *"Done setting up partition"*.
3. Next, select *"#1"* under the *"RAID1 device #1"* partition.
4. Choose *"Use as:"*. Then select *"Ext4 journaling file system"*.
5. Then select the *"Mount point"* and choose *"/ - the root file system"*. Change any of the other options as appropriate, then select *"Done setting up partition"*.
6. 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 **Shift** to open the Grub menu.
  - Press **e** to edit your kernel command options.
  - Press the **down** arrow to highlight the kernel line.
  - Add *"bootdegraded=true"* (without the quotes) to the end of the line.
  - Press **Ctrl**+**x** 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 if 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:

- *Ubuntu Wiki Articles on RAID*[6].
- *Software RAID HOWTO*[7]
- *Managing RAID on Linux*[8]

4.2. Logical Volume Manager (LVM)

Logical Volume Manger, or *LVM*, allows administrators to create *logical* volumes out of one or multiple physical hard disks. LVM volumes can be created on both software RAID partitions and standard partitions

[6] https://help.ubuntu.com/community/Installation#raid
[7] http://www.faqs.org/docs/Linux-HOWTO/Software-RAID-HOWTO.html
[8] http://oreilly.com/catalog/9781565927308/

residing on a single disk. Volumes can also be extended, giving greater flexibility to systems as requirements change.

4.2.1. Overview

A side effect of LVM's power and flexibility is a greater degree of complication. Before diving into the LVM installation process, it is best to get familiar with some terms.

- *Physical Volume (PV):* physical hard disk, disk partition or software RAID partition formatted as LVM PV.
- *Volume Group (VG):* is made from one or more physical volumes. A VG can can be extended by adding more PVs. A VG is like a virtual disk drive, from which one or more logical volumes are carved.
- *Logical Volume (LV):* is similar to a partition in a non-LVM system. A LV is formatted with the desired file system (EXT3, XFS, JFS, etc), it is then available for mounting and data storage.

4.2.2. Installation

As an example this section covers installing Ubuntu Server Edition with `/srv` mounted on a LVM volume. During the initial install only one Physical Volume (PV) will be part of the Volume Group (VG). Another PV will be added after install to demonstrate how a VG can be extended.

There are several installation options for LVM, *"Guided - use the entire disk and setup LVM"* which will also allow you to assign a portion of the available space to LVM, *"Guided - use entire and setup encrypted LVM"*, or *Manually* setup the partitions and configure LVM. At this time the only way to configure a system with both LVM and standard partitions, during installation, is to use the Manual approach.

1. Follow the installation steps until you get to the *Partition disks* step, then:
2. At the *"Partition Disks* screen choose *"Manual"*.
3. Select the hard disk and on the next screen choose "yes" to *"Create a new empty partition table on this device"*.
4. Next, create standard */boot*, *swap*, and */* partitions with whichever filesystem you prefer.
5. For the LVM */srv*, create a new *Logical* partition. Then change *"Use as"* to *"physical volume for LVM"* then *"Done setting up the partition"*.
6. Now select *"Configure the Logical Volume Manager"* at the top, and choose *"Yes"* to write the changes to disk.
7. For the *"LVM configuration action"* on the next screen, choose *"Create volume group"*. Enter a name for the VG such as *vg01*, or something more descriptive. After entering a name, select the partition configured for LVM, and choose *"Continue"*.
8. Back at the *"LVM configuration action"* screen, select *"Create logical volume"*. Select the newly created volume group, and enter a name for the new LV, for example *srv* since that is the intended mount point. Then choose a size, which may be the full partition because it can always be extended later. Choose *"Finish"* and you should be back at the main *"Partition Disks"* screen.
9. Now add a filesystem to the new LVM. Select the partition under *"LVM VG vg01, LV srv"*, or whatever name you have chosen, the choose *Use as*. Setup a file system as normal selecting */srv* as the mount point. Once done, select *"Done setting up the partition"*.

10. Finally, select *"Finish partitioning and write changes to disk"*. Then confirm the changes and continue with the rest of the installation.

There are some useful utilities to view information about LVM:

- *pvdisplay:* shows information about Physical Volumes.
- *vgdisplay:* shows information about Volume Groups.
- *lvdisplay:* shows information about Logical Volumes.

4.2.3. Extending Volume Groups

Continuing with *srv* as an LVM volume example, this section covers adding a second hard disk, creating a Physical Volume (PV), adding it to the volume group (VG), extending the logical volume `srv` and finally extending the filesystem. This example assumes a second hard disk has been added to the system. In this example, this hard disk will be named `/dev/sdb` and we will use the entire disk as a physical volume (you could choose to create partitions and use them as different physical volumes)

Make sure you don't already have an existing `/dev/sdb` before issuing the commands below. You could lose some data if you issue those commands on a non-empty disk.

1. First, create the physical volume, in a terminal execute:

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

2. Now extend the Volume Group (VG):

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

3. Use vgdisplay to find out the free physical extents - Free PE / size (the size you can allocate). We will assume a free size of 511 PE (equivalent to 2GB with a PE size of 4MB) and we will use the whole free space available. Use your own PE and/or free space.

   The Logical Volume (LV) can now be extended by different methods, we will only see how to use the PE to extend the LV:

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

   The *-l* option allows the LV to be extended using PE. The *-L* option allows the LV to be extended using Meg, Gig, Tera, etc bytes.

4. Even though you are supposed to be able to *expand* an ext3 or ext4 filesystem without unmounting it first, it may be a good practice to unmount it anyway and check the filesystem, so that you don't mess up the day you want to reduce a logical volume (in that case unmounting first is compulsory).

   The following commands are for an *EXT3* or *EXT4* filesystem. If you are using another filesystem there may be other utilities available.

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

The *-f* option of e2fsck forces checking even if the system seems clean.

5. Finally, resize the filesystem:

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

6. Now mount the partition and check its size.

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

4.2.4. Resources

- See the *Ubuntu Wiki LVM Articles*[9].
- See the *LVM HOWTO*[10] for more information.
- Another good article is *Managing Disk Space with LVM*[11] on O'Reilly's linuxdevcenter.com site.
- For more information on fdisk see the *fdisk man page*[12].

4.3. iSCSI

The iSCSI protocol can be used to install Ubuntu on systems with or without hard disks attached.

4.3.1. Installation on a diskless system

The first steps of a diskless iSCSI installation are identical to the *Section 2, “Installation” [p. 6]* section up to "Hard drive layout".

1. The installer will display a warning with the following message:

```
No disk drive was detected. If you know the name of the driver needed by your disk
 drive, you can select it from the list.
```

2. Select the item in the list titled *login to iSCSI targets.*
3. You will be prompted to Enter an IP address to scan for iSCSI targets with a description of the format for the address. Enter the IP address for the location of your iSCSI target and navigate to <*continue*> then hit **ENTER**
4. If authentication is required in order to access the iSCSI device, provide the *username* in the next field. Otherwise leave it blank.
5. If your system is able to connect to the iSCSI provider, you should see a list of available iSCSI targets where the operating system can be installed. The list should be similar to the following :

[9] https://help.ubuntu.com/community/Installation#lvm
[10] http://tldp.org/HOWTO/LVM-HOWTO/index.html
[11] http://www.linuxdevcenter.com/pub/a/linux/2006/04/27/managing-disk-space-with-lvm.html
[12] http://manpages.ubuntu.com/manpages/xenial/en/man8/fdisk.8.html

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

iSCSI targets on 192.168.1.29:3260:

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

<Go Back>                          <Continue>
```

6. Select the iSCSI target that you want to use with the space bar. Use the arrow keys to navigate to the target that you want to select.
7. Navigate to <*Continue*> and hit **ENTER**.

If the connection to the iSCSI target is successful, you will be prompted with the *[!!] Partition disks* installation menu. The rest of the procedure is identical to any normal installation on attached disks. Once the installation is completed, you will be asked to reboot.

4.3.2. Installation on a system with disk attached

Again, the iSCSI installation on a normal server with one or many disks attached is identical to the *Section 2, “Installation” [p. 6]* section until we reach the disk partitioning menu. Instead of using any of the Guided selection, we need to perform the following steps :

1. Navigate to the Manual menu entry
2. Select the Configure iSCSI Volumes menu entry
3. Choose the Log into iSCSI targets
4. You will be prompted to Enter an IP address to scan for iSCSI targets. with a description of the format for the address. Enter the IP address and navigate to <*continue*> then hit **ENTER**
5. If authentication is required in order to access the iSCSI device, provide the *username* in the next field or leave it blank.
6. If your system is able to connect to the iSCSI provider, you should see a list of available iSCSI targets where the operating system can be installed. The list should be similar to the following :

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

iSCSI targets on 192.168.1.29:3260:

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

<Go Back>                          <Continue>
```

7. Select the iSCSI target that you want to use with the space bar. Use the arrow keys to navigate to the target that you want to select
8. Navigate to <Continue> and hit **ENTER**.
9. If successful, you will come back to the menu asking you to Log into iSCSI targets. Navigate to Finish and hit **ENTER**

The newly connected iSCSI disk will appear in the overview section as a device prefixed with SCSI. This is the disk that you should select as your installation disk. Once identified, you can choose any of the partitioning methods.

Depending on your system configuration, there may be other SCSI disks attached to the system. Be very careful to identify the proper device before proceeding with the installation. Otherwise, irreversible data loss may result from performing an installation on the wrong disk.

4.3.3. Rebooting to an iSCSI target

The procedure is specific to your hardware platform. As an example, here is how to reboot to your iSCSI target using iPXE

```
iPXE> dhcp

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

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

If the procedure is successful, you should see the Grub menu appear on the screen.

5. Kernel Crash Dump

5.1. Introduction

A Kernel Crash Dump refers to a portion of the contents of volatile memory (RAM) that is copied to disk whenever the execution of the kernel is disrupted. The following events can cause a kernel disruption :

- Kernel Panic
- Non Maskable Interrupts (NMI)
- Machine Check Exceptions (MCE)
- Hardware failure
- Manual intervention

For some of those events (panic, NMI) the kernel will react automatically and trigger the crash dump mechanism through *kexec*. In other situations a manual intervention is required in order to capture the memory. Whenever one of the above events occurs, it is important to find out the root cause in order to prevent it from happening again. The cause can be determined by inspecting the copied memory contents.

5.2. Kernel Crash Dump Mechanism

When a kernel panic occurs, the kernel relies on the *kexec* mechanism to quickly reboot a new instance of the kernel in a pre-reserved section of memory that had been allocated when the system booted (see below). This permits the existing memory area to remain untouched in order to safely copy its contents to storage.

5.3. Installation

The kernel crash dump utility is installed with the following command:

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

Starting with 16.04, the kernel crash dump mechanism is enabled by default. During the installation, you will be prompted with the following dialog. Unless chosen otherwise, the kdump mechanism will be enabled.

```
|-----------------------| Configuring kdump-tools |-----------------------|
|                                                                         |
|                                                                         |
| If you choose this option, the kdump-tools mechanism will be enabled. A |
| reboot is still required in order to enable the crashkernel kernel      |
| parameter.                                                              |
|                                                                         |
| Should kdump-tools be enabled by default?                               |
|                                                                         |
|                    <Yes>                      <No>                      |
|                                                                         |
|-------------------------------------------------------------------------|
```

If you ever need to manually enable the functionality, you can use the **dpkg-reconfigure kdump-tools** command and answer Yes to the question. You can also edit `/etc/default/kdump-tools` by including the following line:

```
USE_KDUMP=1
```

If a reboot has not been done since installation of the linux-crashdump package, a reboot will be required in order to activate the crashkernel= boot parameter. Upon reboot, kdump-tools will be enabled and active.

If you enable kdump-tools after a reboot, you will only need to issue the **kdump-config load** command to activate the kdump mechanism.

5.4. Configuration

In addition to local dump, it is now possible to use the remote dump functionality to send the kernel crash dump to a remote server, using either the *SSH* or *NFS* protocols.

5.4.1. Local Kernel Crash Dumps

Local dumps are configured automatically and will remain in use unless a remote protocol is chosen. Many configuration options exist and are thoroughly documented in the `/etc/default/kdump-tools` file.

5.4.2. Remote Kernel Crash Dumps using the SSH protocol

To enable remote dumps using the *SSH* protocol, the `/etc/default/kdump-tools` must be modified in the following manner :

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

The only mandatory variable to define is SSH. It must contain the username and hostname of the remote server using the format {username}@{remote server}.

SSH_KEY may be used to provide an existing private key to be used. Otherwise, the **kdump-config propagate** command will create a new keypair. The HOSTTAG variable may be used to use the hostname of the system as a prefix to the remote directory to be created instead of the IP address.

The following example shows how **kdump-config propagate** is used to create and propagate a new keypair to the remote server :

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

The password of the account used on the remote server will be required in order to successfully send the public key to the server

The **kdump-config show** command can be used to confirm that kdump is correctly configured to use the SSH protocol :

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

5.4.3. Remote Kernel Crash Dumps using the NFS protocol

To enable remote dumps using the *NFS* protocol, the `/etc/default/kdump-tools` must be modified in the following manner :

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

As with the SSH protocol, the HOSTTAG variable can be used to replace the IP address by the hostname as the prefix of the remote directory.

The **kdump-config show** command can be used to confirm that kdump is correctly configured to use the NFS protocol :

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

5.5. Verification

To confirm that the kernel dump mechanism is enabled, there are a few things to verify. First, confirm that the *crashkernel* boot parameter is present (note: The following line has been split into two to fit the format of this document:

```
cat /proc/cmdline

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

The *crashkernel* parameter has the following syntax:

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

So for the crashkernel parameter found in `/proc/cmdline` we would have :

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

The above value means:

- if the RAM is smaller than 384M, then don't reserve anything (this is the "rescue" case)
- if the RAM size is between 386M and 2G (exclusive), then reserve 64M
- if the RAM size is larger than 2G, then reserve 128M

Second, verify that the kernel has reserved the requested memory area for the kdump kernel by doing:

```
dmesg | grep -i crash

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

Finally, as seen previously, the **kdump-config show** command displays the current status of the kdump-tools configuration :

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

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

5.6. Testing the Crash Dump Mechanism

Testing the Crash Dump Mechanism will cause *a system reboot.* In certain situations, this can cause data loss if the system is under heavy load. If you want to test the mechanism, make sure that the system is idle or under very light load.

Verify that the *SysRQ* mechanism is enabled by looking at the value of the `/proc/sys/kernel/sysrq` kernel parameter :

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

If a value of *0* is returned the feature is disabled. Enable it with the following command :

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

Once this is done, you must become root, as just using **sudo** will not be sufficient. As the *root* user, you will have to issue the command **echo c > /proc/sysrq-trigger**. If you are using a network connection, you will lose contact with the system. This is why it is better to do the test while being connected to the system console. This has the advantage of making the kernel dump process visible.

A typical test output should look like the following :

```
sudo -s
[sudo] password for ubuntu:
# echo c > /proc/sysrq-trigger
```

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

The rest of the output is truncated, but you should see the system rebooting and somewhere in the log, you will see the following line :

```
Begin: Saving vmcore from kernel crash ...
```

Once completed, the system will reboot to its normal operational mode. You will then find Kernel Crash Dump file in the `/var/crash` directory :

```
ls /var/crash
linux-image-3.0.0-12-server.0.crash
```

5.7. Resources

Kernel Crash Dump is a vast topic that requires good knowledge of the linux kernel. You can find more information on the topic here :

- *Kdump kernel documentation*[13].
- *The crash tool*[14]
- *Analyzing Linux Kernel Crash*[15] (Based on Fedora, it still gives a good walkthrough of kernel dump analysis)

[13] http://www.kernel.org/doc/Documentation/kdump/kdump.txt
[14] http://people.redhat.com/~anderson/
[15] http://www.dedoimedo.com/computers/crash-analyze.html

Chapter 3. Package Management

Ubuntu features a comprehensive package management system for installing, upgrading, configuring, and removing software. In addition to providing access to an organized base of over 45,000 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 usually exist in *repositories* which are collections of packages found on various media, such as CD-ROM discs, or online. Packages are normally in a pre-compiled binary format; thus installation is quick, and requires no compiling of software.

Many complex packages use *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 systems, it cannot automatically download and install packages or their dependencies. This section covers using dpkg to manage locally installed packages:

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

```
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_3.0-4_i386.deb
```

  Change `zip_3.0-4_i386.deb` to the actual file name of the local .deb file you wish to install.

- 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 zip** will 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

The apt command is a powerful command-line tool, which works 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 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 utility:

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

  ```
  sudo apt install nmap
  ```

- **Remove a Package**: Removal of a package (or packages) is also straightforward. To remove the package installed in the previous example, type the following:

  ```
  sudo apt remove nmap
  ```

  

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

  Also, adding the *--purge* option to **apt 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 and in the `/etc/apt/sources.list.d` directory. To update the local package index with the latest changes made in the repositories, type the following:

  ```
  sudo apt 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 upgrade
  ```

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

Actions of the apt 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 help
```

[1] http://www.debian.org/doc/user-manuals#apt-howto

4. Aptitude

Launching Aptitude with no command-line options, will give you 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, can be 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 the menu-driven interface of Aptitude as a normal user by typing 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, by using the keyboard arrow keys and the **ENTER** key. Highlight the desired package, then press the **+** key. The package entry should turn *green*, indicating that it has been marked for installation. Now press **g** to be presented with a summary of package actions. Press **g** again, and downloading and installation of the package will commence. When finished, press **ENTER**, to return to the menu.
- **Remove Packages**: To remove a package, locate the package via the *Installed Packages* package category, by using the keyboard arrow keys and the **ENTER** key. Highlight the desired package you wish to remove, then press the **-** key. 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 removal of the package will commence. When finished, press **ENTER**, to return to the menu.
- **Update Package Index**: To update the package index, simply press the **u** key. Updating of the package index will commence.
- **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 the download and installation will commence. When finished, press **ENTER**, to return to the menu.

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.

4.1. Command Line Aptitude

You can also use Aptitude as a command-line tool, similar to apt. To install the nmap package with all necessary dependencies, as in the apt example, you would use the following command:

```
sudo aptitude install nmap
```

To remove the same package, you would use the command:

```
sudo aptitude remove nmap
```

Consult the man pages for more details of command line options for Aptitude.

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 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 {
        "${distro_id}:${distro_codename}";
        "${distro_id}:${distro_codename}-security";
//      "${distro_id}:${distro_codename}-updates";
//      "${distro_id}:${distro_codename}-proposed";
//      "${distro_id}:${distro_codename}-backports";
};
```

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.

To enable automatic updates, edit `/etc/apt/apt.conf.d/20auto-upgrades` and set the appropriate apt configuration options:

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

The above configuration updates the package list, downloads, and installs available upgrades every day. The local download archive is cleaned every week. On servers upgraded to newer versions of Ubuntu, depending on your responses, the file listed above may not be there. In this case, creating a new file of this name should also work.

You can read more about apt Periodic configuration options in the `/etc/cron.daily/apt` script header.

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 have updates available, as well as a summary of changes in each package.

To install the apticron package, in a terminal enter:

```
sudo apt 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` file and the `/etc/apt/sources.list.d` directory. An example of this file is referenced here, along with information on adding or removing repository references from the 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 16.04 _Xenial Xerus_ - Release i386 (20111013.1)]/ xenial 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 packages for potential 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 xenial universe multiverse
deb-src http://archive.ubuntu.com/ubuntu xenial universe multiverse

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

deb http://us.archive.ubuntu.com/ubuntu/ xenial multiverse
```

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

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

7. References

Most of the material covered in this chapter is available in man pages, many of which are available online.

- The *InstallingSoftware*[2] Ubuntu wiki page has more information.
- For more dpkg details see the *dpkg man page*[3].
- The *APT HOWTO*[4] and *apt man page*[5] contain useful information regarding apt usage.
- See the *aptitude man page*[6] for more aptitude options.
- The *Adding Repositories HOWTO (Ubuntu Wiki)*[7] page contains more details on adding repositories.

[2] https://help.ubuntu.com/community/InstallingSoftware
[3] http://manpages.ubuntu.com/manpages/xenial/en/man1/dpkg.1.html
[4] http://www.debian.org/doc/manuals/apt-howto/
[5] http://manpages.ubuntu.com/manpages/xenial/en/man8/apt.8.html
[6] http://manpages.ubuntu.com/manpages/xenial/man8/aptitude.8.html
[7] 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 Interfaces

Ethernet interfaces are identified by the system using the naming convention of *ethX*, where *X* represents a numeric value. The first Ethernet interface is typically identified as *eth0*, the second as *eth1*, and all others should move up in numerical order.

1.1.1. Identify Ethernet Interfaces

To quickly identify all available Ethernet interfaces, you can use the ifconfig command as shown below.

```
ifconfig -a | grep eth
eth0      Link encap:Ethernet  HWaddr 00:15:c5:4a:16:5a
```

Another application that can help identify all network interfaces available to your system is the lshw command. In the example below, lshw shows a single Ethernet interface with the logical name of *eth0* along with bus information, driver details and all supported capabilities.

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

1.1.2. Ethernet Interface Logical Names

Interface logical names are configured in the file `/etc/udev/rules.d/70-persistent-net.rules`. If you would like control which interface receives a particular logical name, find the line matching the interfaces physical MAC address and modify the value of *NAME=ethX* to the desired logical name. Reboot the system to commit your changes.

1.1.3. Ethernet Interface Settings

ethtool is a program that displays and changes Ethernet card settings such as auto-negotiation, port speed, duplex mode, and Wake-on-LAN. It is not installed by default, but is available for installation in the repositories.

```
sudo apt install ethtool
```

The following is an example of how to view supported features and configured settings of an Ethernet interface.

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

Changes made with the ethtool command are temporary and will be lost after a reboot. If you would like to retain settings, simply add the desired ethtool command to a *pre-up* statement in the interface configuration file `/etc/network/interfaces`.

The following is an example of how the interface identified as *eth0* could be permanently configured with a port speed of 1000Mb/s running in full duplex mode.

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

Although the example above shows the interface configured to use the *static* method, it actually works with other methods as well, such as DHCP. The example is meant to demonstrate only proper placement of the *pre-up* statement in relation to the rest of the interface configuration.

1.2. IP Addressing

The following section describes the process of configuring your systems IP address and default gateway needed for communicating on a local area network and the Internet.

1.2.1. Temporary IP Address Assignment

For temporary network configurations, you can use standard commands such as ip, ifconfig and route, which are also found on most other GNU/Linux operating systems. These commands allow you to configure settings which take effect immediately, however they are not persistent and will be lost after a reboot.

To temporarily configure an IP address, you can use the ifconfig command in the following manner. Just modify the IP address and subnet mask to match your network requirements.

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

To verify the IP address configuration of eth0, you can use the ifconfig command in the following manner.

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

To configure a default gateway, you can use the route command in the following manner. Modify the default gateway address to match your network requirements.

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

To verify your default gateway configuration, you can use the route command in the following manner.

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

If you require DNS for your temporary network configuration, you can add DNS server IP addresses in the file `/etc/resolv.conf`. In general, editing `/etc/resolv.conf` directly is not recommanded, but this is a temporary and non-persistent configuration. The example below shows how to enter two DNS servers to `/etc/resolv.conf`, which should be changed to servers appropriate for your network. A more lengthy description of the proper persistent way to do DNS client configuration is in a following section.

```
nameserver 8.8.8.8
nameserver 8.8.4.4
```

If you no longer need this configuration and wish to purge all IP configuration from an interface, you can use the ip command with the flush option as shown below.

```
ip addr flush eth0
```

Flushing the IP configuration using the ip command does not clear the contents of `/etc/resolv.conf`. You must remove or modify those entries manually, or re-boot which should also cause `/etc/resolv.conf`, which is actually now a symlink to `/run/resolvconf/resolv.conf`, to be re-written.

1.2.2. Dynamic IP Address Assignment (DHCP Client)

To configure your server to use DHCP for dynamic address assignment, add the *dhcp* method to the inet address family statement for the appropriate interface in the file `/etc/network/interfaces`. The example below assumes you are configuring your first Ethernet interface identified as *eth0*.

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

By adding an interface configuration as shown above, you can manually enable the interface through the ifup command which initiates the DHCP process via dhclient.

```
sudo ifup eth0
```

To manually disable the interface, you can use the ifdown command, which in turn will initiate the DHCP release process and shut down the interface.

```
sudo ifdown eth0
```

1.2.3. Static IP Address Assignment

To configure your system to use a static IP address assignment, add the *static* method to the inet address family statement for the appropriate interface in the file `/etc/network/interfaces`. The example below assumes you are configuring your first Ethernet interface identified as *eth0*. Change the *address*, *netmask*, and *gateway* values to meet the requirements of your network.

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

By adding an interface configuration as shown above, you can manually enable the interface through the ifup command.

```
sudo ifup eth0
```

To manually disable the interface, you can use the ifdown command.

```
sudo ifdown eth0
```

1.2.4. Loopback Interface

The loopback interface is identified by the system as *lo* and has a default IP address of 127.0.0.1. It can be viewed using the ifconfig command.

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

By default, there should be two lines in `/etc/network/interfaces` responsible for automatically configuring your loopback interface. It is recommended that you keep the default settings unless you have a specific purpose for changing them. An example of the two default lines are shown below.

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

1.3. Name Resolution

Name resolution as it relates to IP networking is the process of mapping IP addresses to hostnames, making it easier to identify resources on a network. The following section will explain how to properly configure your system for name resolution using DNS and static hostname records.

1.3.1. DNS Client Configuration

Traditionally, the file `/etc/resolv.conf` was a static configuration file that rarely needed to be changed or automatically changed via DCHP client hooks. Nowadays, a computer can switch from one network to another quite often and the *resolvconf* framework is now being used to track these changes and update the resolver's configuration automatically. It acts as an intermediary between programs that supply nameserver information and applications that need nameserver information. Resolvconf gets populated with information by a set of hook scripts related to network interface configuration. The most notable difference for the user is that any change manually done to `/etc/resolv.conf` will be lost as it gets overwritten each time something

triggers resolvconf. Instead, resolvconf uses DHCP client hooks, and `/etc/network/interfaces` to generate a list of nameservers and domains to put in `/etc/resolv.conf`, which is now a symlink:

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

To configure the resolver, add the IP addresses of the nameservers that are appropriate for your network in the file `/etc/network/interfaces`. You can also add an optional DNS suffix search-lists to match your network domain names. For each other valid resolv.conf configuration option, you can include, in the stanza, one line beginning with that option name with a **dns-** prefix. The resulting file might look like the following:

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

The *search* option can also be used with multiple domain names so that DNS queries will be appended in the order in which they are entered. For example, your network may have multiple sub-domains to search; a parent domain of *example.com*, and two sub-domains, *sales.example.com* and *dev.example.com*.

If you have multiple domains you wish to search, your configuration might look like the following:

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

If you try to ping a host with the name of *server1*, your system will automatically query DNS for its Fully Qualified Domain Name (FQDN) in the following order:

1. server1**.example.com**
2. server1**.sales.example.com**
3. server1**.dev.example.com**

If no matches are found, the DNS server will provide a result of *notfound* and the DNS query will fail.

1.3.2. Static Hostnames

Static hostnames are locally defined hostname-to-IP mappings located in the file `/etc/hosts`. Entries in the `hosts` file will have precedence over DNS by default. This means that if your system tries to resolve a hostname and it matches an entry in /etc/hosts, it will not attempt to look up the record in DNS. In some configurations, especially when Internet access is not required, servers that communicate with a limited number of resources can be conveniently set to use static hostnames instead of DNS.

The following is an example of a `hosts` file where a number of local servers have been identified by simple hostnames, aliases and their equivalent Fully Qualified Domain Names (FQDN's).

```
127.0.0.1 localhost
127.0.1.1 ubuntu-server
10.0.0.11 server1 server1.example.com vpn
10.0.0.12 server2 server2.example.com mail
10.0.0.13 server3 server3.example.com www
10.0.0.14 server4 server4.example.com file
```

In the above example, notice that each of the servers have been given aliases in addition to their proper names and FQDN's. *Server1* has been mapped to the name *vpn*, *server2* is referred to as *mail*, *server3* as *www*, and *server4* as *file*.

1.3.3. Name Service Switch Configuration

The order in which your system selects a method of resolving hostnames to IP addresses is controlled by the Name Service Switch (NSS) configuration file `/etc/nsswitch.conf`. As mentioned in the previous section, typically static hostnames defined in the systems `/etc/hosts` file have precedence over names resolved from DNS. The following is an example of the line responsible for this order of hostname lookups in the file `/etc/nsswitch.conf`.

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

- **files** first tries to resolve static hostnames located in `/etc/hosts`.
- **mdns4_minimal** attempts to resolve the name using Multicast DNS.
- **[NOTFOUND=return]** means that any response of *notfound* by the preceding *mdns4_minimal* process should be treated as authoritative and that the system should not try to continue hunting for an answer.
- **dns** represents a legacy unicast DNS query.
- **mdns4** represents a Multicast DNS query.

To modify the order of the above mentioned name resolution methods, you can simply change the *hosts:* string to the value of your choosing. For example, if you prefer to use legacy Unicast DNS versus Multicast DNS, you can change the string in `/etc/nsswitch.conf` as shown below.

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

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 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 bring up the bridge:

```
sudo ifup br0
```

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.

1.5. Resources

- The *Ubuntu Wiki Network page*[1] has links to articles covering more advanced network configuration.
- The *resolvconf man page*[2] has more information on resolvconf.
- The *interfaces man page*[3] has details on more options for `/etc/network/interfaces`.
- The *dhclient man page*[4] has details on more options for configuring DHCP client settings.
- For more information on DNS client configuration see the *resolver man page*[5]. Also, Chapter 6 of O'Reilly's *Linux Network Administrator's Guide*[6] is a good source of resolver and name service configuration information.

[1] https://help.ubuntu.com/community/Network
[2] http://manpages.ubuntu.com/manpages/man8/resolvconf.8.html
[3] http://manpages.ubuntu.com/manpages/man5/interfaces.5.html
[4] http://manpages.ubuntu.com/manpages/man8/dhclient.8.html
[5] http://manpages.ubuntu.com/manpages/man5/resolver.5.html
[6] http://oreilly.com/catalog/linag2/book/ch06.html

- For more information on *bridging* see the *brctl man page*[7] and the Linux Foundation's *Networking-Bridge*[8] page.

[7] http://manpages.ubuntu.com/manpages/man8/brctl.8.html

[8] http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge

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, Gateway Address, and Nameserver Addresses are typically specified via the appropriate directives in the file `/etc/network/interfaces`. For more information, view the system manual page for `interfaces`, with the following command typed at a terminal prompt:

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

```
man interfaces
```

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.

2.7. Resources

- There are man pages for *TCP*[9] and *IP*[10] that contain more useful information.
- Also, see the *TCP/IP Tutorial and Technical Overview*[11] IBM Redbook.
- Another resource is O'Reilly's *TCP/IP Network Administration*[12].

[9] http://manpages.ubuntu.com/manpages/xenial/en/man7/tcp.7.html
[10] http://manpages.ubuntu.com/manpages/xenial/man7/ip.7.html
[11] http://www.redbooks.ibm.com/abstracts/gg243376.html
[12] http://oreilly.com/catalog/9780596002978/

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
- IP address of the default-gateway to use
- IP adresses of the DNS servers to use

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

- Host Name
- Domain Name
- 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 the following methods:

Manual allocation (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. This ensures that a particular address is assigned automatically to that network card, based on it's MAC address.

Dynamic allocation (address pool)

> In this method, the DHCP server will assign an IP address from a pool of addresses (sometimes also called a range or scope) for a period of time or lease, that is configured on the server or until the client informs the server that it doesn't need the address anymore. This way, the clients will be receiving their configuration properties dynamically and on a "first come, first served" 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. This way, an address can be leased or used for a period of time. After this period, the client has to renegociate the lease with the server to maintain use of the address.

Automatic allocation

> Using this method, the DHCP automatically assigns an IP address permanently to a device, selecting it from a pool of available addresses. Usually DHCP is used to assign a temporary address to a client, but a DHCP server can allow an infinite lease time.

The last two methods can be considered "automatic" because in each case the DHCP server assigns an address with no extra intervention needed. The only difference between them is in how long the IP address is leased, in other words whether a client's address varies over time. Ubuntu is shipped with both DHCP server and client. The server is dhcpd (dynamic host configuration protocol daemon). The client provided with Ubuntu is dhclient and should be installed on all computers required to be automatically configured. Both programs are easy to install and configure and will be automatically started at system boot.

3.1. Installation

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

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

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

You also may need to edit /etc/default/isc-dhcp-server to specify the interfaces dhcpd should listen to.

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:

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

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

This will result in the DHCP server giving clients an IP address from the range 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 to use 192.168.1.254 as the default-gateway and 192.168.1.1 and 192.168.1.2 as its DNS servers.

After changing the config file you have to restart the dhcpd:

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

3.3. References

- The *dhcp3-server Ubuntu Wiki*[13] page has more information.
- For more `/etc/dhcp/dhcpd.conf` options see the *dhcpd.conf man page*[14].
- *ISC dhcp-server*[15]

[13] https://help.ubuntu.com/community/dhcp3-server
[14] http://manpages.ubuntu.com/manpages/xenial/en/man5/dhcpd.conf.5.html
[15] http://www.isc.org/software/dhcp

4. Time Synchronisation

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, 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 by default uses *timedatectl / timesyncd* to synchronize time and users can optionally use ntpd to serve network time info.

4.1. Synchronizing your systems time

Starting with Ubuntu 16.04 *timedatectl / timesyncd* (which are part of systemd) replace most of *ntpdate / ntp*.

timesyncd is available by default and replaces not only ntpdate, but also the client portion of ntpd. So on top of the one-shot action that ntpdate provided on boot and network activation, now timesyncd by default regularly checks and keeps your local time in sync. It also stores time updates locally, so that after reboots monotonically advances if applicable.

If ntpdate / ntp are installed timedatectl steps back to let you keep your old setup. That shall ensure that no two time syncing services are fighting and also to retain any kind of old behaviour/config that you had through an upgrade. But it also implies that on an upgrade from a former release ntp/ntpdate might still be installed and therefore renders the new systemd based services disabled.

ntpdate is considered deprecated in favour of timedatectl and thereby no more installed by default.

4.1.1. Configuring timedatectl and timesyncd

The current status of time and time configuration via timedatectl and timesyncd can be checked with **timedatectl status**.

```
$ timedatectl status
      Local time: Mo 2017-06-26 12:16:16 CEST
  Universal time: Mo 2017-06-26 10:16:16 UTC
        RTC time: Mo 2017-06-26 10:16:16
       Time zone: Europe/Berlin (CEST, +0200)
 Network time on: yes
NTP synchronized: yes
 RTC in local TZ: no
```

Via timedatectl an admin can control the timezone, how the system clock should relate to the hwclock and if permanent synronization should be enabled or not. See **man timedatectl** for more details.

timesyncd itself is still a normal service, so you can check its status also more in detail via.

```
$ systemctl status systemd-timesyncd
. systemd-timesyncd.service - Network Time Synchronization
   Loaded: loaded (/lib/systemd/system/systemd-timesyncd.service; enabled; vendor preset:
 enabled)
  Drop-In: /lib/systemd/system/systemd-timesyncd.service.d
           |_disable-with-time-daemon.conf
   Active: active (running) since Mo 2017-06-26 11:12:19 CEST; 30min ago
     Docs: man:systemd-timesyncd.service(8)
 Main PID: 12379 (systemd-timesyn)
   Status: "Synchronized to time server [2001:67c:1560:8003::c8]:123 (ntp.ubuntu.com)."
    Tasks: 2
   Memory: 424.0K
      CPU: 12ms
   CGroup: /system.slice/systemd-timesyncd.service
           |_12379 /lib/systemd/systemd-timesyncd

Jun 26 11:12:19 lap systemd[1]: Starting Network Time Synchronization...
Jun 26 11:12:19 lap systemd[1]: Started Network Time Synchronization.
Jun 26 11:12:19 lap systemd-timesyncd[12379]: Synchronized to time server
 [2001:67c:1560:8003::c8]:123 (ntp.ubuntu.com).
```

The nameserver to fetch time for timedatectl and timesyncd from can be specified in `/etc/systemd/timesyncd.conf` and additional config files can be stored in `/etc/systemd/timesyncd.conf.d/`. The entries for NTP= and FallbackNTP= are space separated lists.

4.2. Serving NTP

If on top of synchronizing your system you also want to serve NTP information you need an ntp server. The most classic and supported one is ntpd, but it is also very old so there also are openntpd and chrony as alternatives available in the archive.

4.2.1. ntpd

The ntp daemon ntpd 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.

4.2.2. Installation

To install ntpd, from a terminal prompt enter:

```
sudo apt install ntp
```

4.2.3. Configuration

Edit `/etc/ntp.conf` to add/remove server lines. By default these servers are configured:

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

After changing the config file you have to reload the ntpd:

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

Of the pool number 2.ubuntu.pool.ntp.org as well as ntp.ubuntu.com also support ipv6 if needed. If one needs to force ipv6 there also is ipv6.ntp.ubuntu.com which is not configured by default.

4.2.4. View status

Use ntpq to see more info:

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

4.2.5. PPS Support

Since 16.04 ntp supports PPS discipline which can be used to augment ntp with local timesources for better accuracy. For more details on configuration see the external pps ressource listed below.

4.3. References

- See the *Ubuntu Time*[16] wiki page for more information.
- *ntp.org, home of the Network Time Protocol project*[17]
- *Freedesktop.org info on timedatectl*[18]
- *Freedesktop.org info on systemd-timesyncd service*[19]
- *ntp.org faq on configuring PPS*[20]

[16] https://help.ubuntu.com/community/UbuntuTime
[17] http://www.ntp.org/
[18] https://www.freedesktop.org/software/systemd/man/timedatectl.html
[19] https://www.freedesktop.org/software/systemd/man/systemd-timesyncd.service.html#
[20] http://www.ntp.org/ntpfaq/NTP-s-config-adv.htm#S-CONFIG-ADV-PPS

5. Data Plane Development Kit

The DPDK is a set of libraries and drivers for fast packet processing and runs mostly in Linux userland. It is a set of libraries that provide the so called "Environment Abstraction Layer" (EAL). The EAL hides the details of the environment and provides a standard programming interface. Common use cases are around special solutions for instance network function virtualization and advanced high-throughput network switching. The DPDK uses a run-to-completion model for fast data plane performance and accesses devices via polling to eliminate the latency of interrupt processing at the tradeoff of higher cpu consumption. It was designed to run on any processors. The first supported CPU was Intel x86 and it is now extended to IBM Power 8, EZchip TILE-Gx and ARM.

Ubuntu currently supports DPDK version 2.2 and provides some infrastructure to ease its usability.

5.1. Prerequisites

This package is currently compiled for the lowest possible CPU requirements. Which still requires at least SSE3 to be supported by the CPU.

The list of upstream DPDK supported network cards can be found at *supported NICs*[21]. But a lot of those are disabled by default in the upstream Project as they are not yet in a stable state. The subset of network cards that DPDK has enabled in the package as available in Ubuntu 16.04 is:

Intel

- *e1000*[22] (82540, 82545, 82546)
- *e1000e*[23] (82571..82574, 82583, ICH8..ICH10, PCH..PCH2)
- *igb*[24] (82575..82576, 82580, I210, I211, I350, I354, DH89xx)
- *ixgbe*[25] (82598..82599, X540, X550)
- *i40e*[26] (X710, XL710, X722)
- *fm10k*[27] (FM10420)

Chelsio

- *cxgbe*[28] (Terminator 5)

Cisco

- *enic*[29] (UCS Virtual Interface Card)

Paravirtualization

[21] http://dpdk.org/doc/nics
[22] http://dpdk.org/doc/guides/nics/e1000em.html
[23] http://dpdk.org/browse/dpdk/tree/drivers/net/e1000/
[24] http://dpdk.org/browse/dpdk/tree/drivers/net/e1000/
[25] http://dpdk.org/doc/guides/nics/ixgbe.html
[26] http://dpdk.org/browse/dpdk/tree/drivers/net/i40e/
[27] http://dpdk.org/doc/guides/nics/fm10k.html
[28] http://dpdk.org/doc/guides/nics/cxgbe.html
[29] http://dpdk.org/browse/dpdk/tree/drivers/net/enic

- *virtio-net*[30] (QEMU)
- *vmxnet3*[31]

Others

- *af_packet*[32] (Linux AF_PACKET socket)
- *ring*[33] (memory)

On top it experimentally enables the following two PMD drivers as they represent (virtual) devices that are very accessible to end users.

Paravirtualization

- *xenvirt*[34] (Xen)

Others

- *pcap*[35] (file or kernel driver)

Cards have to be unassigned from their kernel driver and instead be assigned to uio_pci_generic of vfio-pci. uio_pci_generic is older and usually getting to work more easily.

The newer vfio-pci requires that you activate the following kernel parameters to enable iommu.

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

On top for vfio-pci you then have to configure and assign the iommu groups accordingly.

Note: In virtio based environment it is enough to "unassign" devices from the kernel driver. Without that DPDK will reject to use the device to avoid issues with kernel and DPDK working on the device at the same time. Since DPDK can work directly on virtio devices it is not required to assign e.g. uio_pci_generic to those devices.

Manual configuration and status checks can be done via sysfs or with the tool dpdk_nic_bind

```
dpdk_nic_bind --help

Usage:
------

     dpdk_nic_bind [options] DEVICE1 DEVICE2 ....

     where DEVICE1, DEVICE2 etc, are specified via PCI "domain:bus:slot.func" syntax
     or "bus:slot.func" syntax. For devices bound to Linux kernel drivers, they may
```

[30] http://dpdk.org/doc/guides/nics/virtio.html
[31] http://dpdk.org/doc/guides/nics/vmxnet3.html
[32] http://dpdk.org/browse/dpdk/tree/drivers/net/af_packet
[33] http://dpdk.org/doc/guides/nics/pcap_ring.html#rings-based-pmd
[34] http://dpdk.org/doc/guides/xen/pkt_switch.html#xen-pmd-frontend-prerequisites
[35] http://dpdk.org/doc/guides/nics/pcap_ring.html#libpcap-based-pmd

```
also be referred to by Linux interface name e.g. eth0, eth1, em0, em1, etc.

Options:
    --help, --usage:
    Display usage information and quit

-s, --status:
        Print the current status of all known network interfaces.
        For each device, it displays the PCI domain, bus, slot and function,
        along with a text description of the device. Depending upon whether the
        device is being used by a kernel driver, the igb_uio driver, or no
        driver, other relevant information will be displayed:
        * the Linux interface name e.g. if=eth0
        * the driver being used e.g. drv=igb_uio
        * any suitable drivers not currently using that device
           e.g. unused=igb_uio
    NOTE: if this flag is passed along with a bind/unbind option, the status
    display will always occur after the other operations have taken place.

-b driver, --bind=driver:
        Select the driver to use or "none" to unbind the device

    -u, --unbind:
    Unbind a device (Equivalent to "-b none")

--force:
        By default, devices which are used by Linux - as indicated by having
        routes in the routing table - cannot be modified. Using the --force
        flag overrides this behavior, allowing active links to be forcibly
        unbound.
        WARNING: This can lead to loss of network connection and should be used
        with caution.

Examples:
---------

To display current device status:
        dpdk_nic_bind --status

To bind eth1 from the current driver and move to use igb_uio
        dpdk_nic_bind --bind=igb_uio eth1

To unbind 0000:01:00.0 from using any driver
        dpdk_nic_bind -u 0000:01:00.0

To bind 0000:02:00.0 and 0000:02:00.1 to the ixgbe kernel driver
        dpdk_nic_bind -b ixgbe 02:00.0 02:00.
```

5.2. DPDK Device configuration

The package *dpdk* provides init scripts that ease configuration of device assignment and huge pages. It also makes them persistent accross reboots.

The following is an example of the file /etc/dpdk/interfaces configuring two ports of a network card. One with uio_pci_generic and the other one with vfio-pci

```
# <bus>         Currently only "pci" is supported
# <id>          Device ID on the specified bus
# <driver>      Driver to bind against (vfio-pci or uio_pci_generic)
#
# Be aware that the two DPDK compatible drivers uio_pci_generic and vfio-pci are
# part of linux-image-extra-<VERSION> package.
# This package is not always installed by default - for example in cloud-images.
# So please install it in case you run into missing module issues.
#
# <bus> <id>     <driver>
pci 0000:04:00.0 uio_pci_generic
pci 0000:04:00.1 vfio-pci
```

Cards are identified by their PCI-ID. If you are unsure you might use the tool dpdk_nic_bind to show the current available devices and the drivers they are assigned to.

```
dpdk_nic_bind --status

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

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

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

5.3. DPDK HugePage configuration

DPDK makes heavy use of huge pages to eliminate pressure on the TLB. Therefore hugepages have to be configured in your system.

The *dpdk* package has a config file and scripts that try to ease hugepage configuration for DPDK in the form of */etc/dpdk/dpdk.conf*. If you have more consumers of hugepages than just DPDK in your system or very special requirements how your hugepages are going to be set up you likely want to allocate/control them by yourself. If not this can be a great simplification to get DPDK configured for your needs.

Here an example configuring 1024 Hugepages of 2M each and 4 1G pages.

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

As shown this supports configuring 2M and the larger 1G hugepages (or a mix of both). It will make sure there are proper hugetlbfs mountpoints for DPDK to find both sizes no matter what your default huge page size is. The config file itself holds more details on certain corner cases and a few hints if you want to allocate hugepages manually via a kernel parameter.

It depends on your needs which size you want - 1G pages are certainly more effective regarding TLB pressure. But there were reports of them fragmenting inside the DPDK memory alloactions. Also it can be harder to grab enough free space to set up a certain amount of 1G pages later in the lifecycle of a system.

5.4. Compile DPDK Applications

Currently there are not a lot consumers of the DPDK library that are stable and released. OpenVswitch-DPDK being an exception to that (see below), but in general it is very likely that you might want / have to compile an app against the library.

You will often find guides that tell you to fetch the DPDK sources, build them to your needs and eventually build your application based on DPDK by setting values RTE_* for the build system. Since Ubunutu provides an already compiled DPDK for you can can skip all that. To simplify setting the proper variables you can source the file /usr/share/dpdk/dpdk-sdk-env.sh before building your application. Here an excerpt building the l2fwd example application delivered with the dpdk-doc package.

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

Depending on what you build it might be a good addition to install all of DPDK build dependencies before the make.

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

5.5. OpenVswitch-DPDK

Being a library it doesn't do a lot on its own, so it depends on emerging projects making use of it. One consumer of the library that already is bundled in the Ubuntu 16.04 release is OpenVswitch with DPDK support in the package openvswitch-switch-dpdk.

Here an example how to install and configure a basic OpenVswitch using DPDK for later use via libvirt/qemu-kvm.

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

Please remember that you have to assign devices to DPDK compatible drivers (see above) before restarting.

The section *--vhost-owner libvirt-qemu:kvm --vhost-perm 0664* will set vhost_user ports up with owner/permissions to be compatible with Ubuntus way of running qemu-kvm/libvirt with reduced privileges for more security.

Please note that the section *-m 2048* is the most basic numa setup for a single socket system. If you have multiple sockets you might want to define how to split your memory among them, for example *-m 1024, 1024*. Please be aware that DPDK will try to work only with local memory to the network cards it works with (for performance reasons). That said if you have multiple nodes, but all network cards on one, you should consider spreading your cards. If not at least allocate your memory to the node where the cards reside, for example in a two node all to node #2: *-m 0, 2048*. You can use the tool *lstopo* from the package *hwloc-nox* to see on which socket your cards are located.

The OpenVswitch you now started supports all port types OpenVswitch usually does, plus DPDK port types. Here an example how to create a bridge and - instead of a normal external port - add an external DPDK port to it.

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

The enablement of DPDK in Open vSwitch has changed in version 2.6. So for users of releases >=16.10, but also for users of the *Ubuntu Cloud Archive*[36] >=neutron the enablement has changed compared to that for users of Ubuntu 16.04. The options formerly passed via *DPDK_OPTS* are now configured via ovs-vsctl into the Open vSwitch configuration database.

The same example as above would in the new way look like:

[36] https://wiki.ubuntu.com/OpenStack/CloudArchive

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

Please see the associated upstream documentation and the man page of the vswitch configuration as provided by the package for more details:

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

5.6. OpenVswitch DPDK to KVM Guests

If you are not building some sort of SDN switch or NFV on top of DPDK it is very likely that you want to forward traffic to KVM guests. The good news is, that with the new qemu/libvirt/dpdk/openvswitch versions in Ubuntu 16.04 this is no more about manually appending commandline string. This chapter covers a basic configuration how to connect a KVM guest to a OpenVswitch-DPDK instance.

The Guest has to be backed by shared hugepages for DPDK/vhost_user to work. To ensure in general that libvirt/qemu-kvm finds a proper hugepage mountpoint you can just enable KVM_HUGEPAGES in /etc/default/qemu-kvm. Afterwards restart the service to pick up the changed configuration.

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

To let a guest be backed by hugepages is now also supported via recent libvirt, just add the following snippet to your virsh xml (or the equivalent libvirt interface you use). Those xmls can also be used as templates to easily spawn guests with "uvt-kvm create".

```
<numa>
<cell id='0' cpus='0' memory='6291456' unit='KiB' memAccess='shared'/>
</numa>
[...]
<memoryBacking>
<hugepages>
<page size="2" unit="M" nodeset="0"/>
</hugepages>
</memoryBacking>
```

The new and recommended way to get to a KVM guest is using vhost_user. This will cause DPDK to create a socket that qemu will connect the guest to. Here an example how to add such a port to the bridge you created (see above).

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

This will create a vhost_user socket at /var/run/openvswitch/vhost-user-1

To let libvirt/kvm consume this socket and create a guest virtio network device for it add a snippet like this to your guest definition as the network definition.

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

5.7. DPDK in KVM Guests

If you have no access to DPDK supported network cards you can still work with DPDK by using its support for virtio. To do so you have to create guests backed by hugepages (see above).

On top of that there it is required to have at least SSE3. The default CPU model qemu/libvirt uses is only up to SSE2. So you will have to define a model that passed the proper feature flag - and of course have a Host system that supportes it. An example can be found in following snippet to your virsh xml (or the equivalent virsh interface you use).

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

This example is rather offensive and passes all host features. That in turn makes the guest not very migratable as the target would need all the features as well. A "softer" way is to just add sse3 to the default model like the following example.

```
<cpu mode='custom' match='exact'>
<model fallback='allow'>qemu64</model>
<feature policy='require' name='ssse3'/>
</cpu>
```

Also virtio nowadays supports multiqueue which DPDK in turn can exploit for better speed. To modify a normal virtio definition to have multiple queues add the following to your interface definition. This is about enhancing a normal virtio nic to have multiple queues, to later on be consumed e.g. by DPDK in the guest.

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

5.8. Tuning Openvswitch-DPDK

DPDK has plenty of options - in combination with Openvswitch-DPDK the two most commonly used are:

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

The first select how many rx queues are to be used for each DPDK interface, while the second controls how many and where to run PMD threads. The example above will utilize two rx queues and run PMD threads on CPU 1 and 2. See the referred links to "EAL Command-line Options" and "OpenVswitch DPDK installation" at the end of this document for more.

As usual with tunings you have to know your system and workload really well - so please verify any tunings with workloads matching your real use case.

5.9. Support and Troubleshooting

DPDK is a fast evolving project. In any case of a search for support and further guides it is highly recommended to first check if they apply to the current version.

- *DPDK Mailing Lists*[37]
- For OpenVswitch-DPDK *OpenStack Mailing Lists*[38]
- Known issues in *DPDK Launchpad Area*[39]
- Join the IRC channels #DPDK or #openvswitch on freenode.

Issues are often due to missing small details in the general setup. Later on, these missing details cause problems which can be hard to track down to their root cause. A common case seems to be the "could not open network device dpdk0 (No such device)" issue. This occurs rather late when setting up a port in Open vSwitch with DPDK. But the root cause most of the time is very early in the setup and initialization. Here an example how a proper initialization of a device looks - this can be found in the syslog/journal when starting Open vSwitch with DPDK enabled.

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

[37] http://dpdk.org/ml
[38] http://openvswitch.org/mlists
[39] https://bugs.launchpad.net/ubuntu/+source/dpdk

If this is missing, either by ignored cards, failed initialization or other reasons, later on there will be no DPDK device to refer to. Unfortunately the logging is spread across syslog/journal and the openvswitch log. To allow some cross checking here an example what can be found in these logs, relative to the entered command.

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

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

CMD: sudo service openvswitch-switch restart

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

OVS-LOG:
systemd[1]: Stopping Open vSwitch...
systemd[1]: Stopped Open vSwitch.
systemd[1]: Stopping Open vSwitch Internal Unit...
ovs-ctl[3541]: * Killing ovs-vswitchd (3329)
ovs-ctl[3541]: * Killing ovsdb-server (3318)
systemd[1]: Stopped Open vSwitch Internal Unit.
systemd[1]: Starting Open vSwitch Internal Unit...
ovs-ctl[3560]: * Starting ovsdb-server
ovs-vsctl: ovs|00001|vsctl|INFO|Called as ovs-vsctl --no-wait -- init -- set Open_vSwitch .
 db-version=7.12.1
ovs-vsctl: ovs|00001|vsctl|INFO|Called as ovs-vsctl --no-wait set Open_vSwitch . ovs-
version=2.5.0 "external-ids:system-id=\"e7c5ba80-bb14-45c1-b8eb-628f3ad03903\"" "system-
type=\"Ubuntu\"" "system-version=\"16.04-xenial\""
ovs-ctl[3560]: * Configuring Open vSwitch system IDs
ovs-ctl[3560]: 2016-01-22T08:58:31Z|00001|dpdk|INFO|No -vhost_sock_dir provided - defaulting
 to /var/run/openvswitch
ovs-vswitchd: ovs|00001|dpdk|INFO|No -vhost_sock_dir provided - defaulting to /var/run/
openvswitch
ovs-ctl[3560]: EAL: Detected lcore 0 as core 0 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 1 as core 1 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 2 as core 2 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 3 as core 3 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 4 as core 4 on socket 0
```

```
ovs-ctl[3560]: EAL: Detected lcore 5 as core 5 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 6 as core 0 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 7 as core 1 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 8 as core 2 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 9 as core 3 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 10 as core 4 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 11 as core 5 on socket 0
ovs-ctl[3560]: EAL: Support maximum 128 logical core(s) by configuration.
ovs-ctl[3560]: EAL: Detected 12 lcore(s)
ovs-ctl[3560]: EAL: VFIO modules not all loaded, skip VFIO support...
ovs-ctl[3560]: EAL: Setting up physically contiguous memory...
ovs-ctl[3560]: EAL: Ask a virtual area of 0x100000000 bytes
ovs-ctl[3560]: EAL: Virtual area found at 0x7f2040000000 (size = 0x100000000)
ovs-ctl[3560]: EAL: Requesting 4 pages of size 1024MB from socket 0
ovs-ctl[3560]: EAL: TSC frequency is ~2397202 KHz
ovs-vswitchd[3592]: EAL: TSC frequency is ~2397202 KHz
ovs-vswitchd[3592]: EAL: Master lcore 0 is ready (tid=fc6cbb00;cpuset=[0])
ovs-vswitchd[3592]: EAL: PCI device 0000:04:00.0 on NUMA socket 0
ovs-vswitchd[3592]: EAL:   probe driver: 8086:1528 rte_ixgbe_pmd
ovs-vswitchd[3592]: EAL:   Not managed by a supported kernel driver, skipped
ovs-vswitchd[3592]: EAL: PCI device 0000:04:00.1 on NUMA socket 0
ovs-vswitchd[3592]: EAL:   probe driver: 8086:1528 rte_ixgbe_pmd
ovs-vswitchd[3592]: EAL:   PCI memory mapped at 0x7f2140000000
ovs-vswitchd[3592]: EAL:   PCI memory mapped at 0x7f2140200000
ovs-ctl[3560]: EAL: Master lcore 0 is ready (tid=fc6cbb00;cpuset=[0])
ovs-ctl[3560]: EAL: PCI device 0000:04:00.0 on NUMA socket 0
ovs-ctl[3560]: EAL:   probe driver: 8086:1528 rte_ixgbe_pmd
ovs-ctl[3560]: EAL:   Not managed by a supported kernel driver, skipped
ovs-ctl[3560]: EAL: PCI device 0000:04:00.1 on NUMA socket 0
ovs-ctl[3560]: EAL:   probe driver: 8086:1528 rte_ixgbe_pmd
ovs-ctl[3560]: EAL:   PCI memory mapped at 0x7f2140000000
ovs-ctl[3560]: EAL:   PCI memory mapped at 0x7f2140200000
ovs-vswitchd[3592]: PMD: eth_ixgbe_dev_init(): MAC: 4, PHY: 3
ovs-vswitchd[3592]: PMD: eth_ixgbe_dev_init(): port 0 vendorID=0x8086 deviceID=0x1528
ovs-ctl[3560]: PMD: eth_ixgbe_dev_init(): MAC: 4, PHY: 3
ovs-ctl[3560]: PMD: eth_ixgbe_dev_init(): port 0 vendorID=0x8086 deviceID=0x1528
ovs-ctl[3560]: Zone 0: name:<RG_MP_log_history>, phys:0x83fffdec0, len:0x2080,
 virt:0x7f213fffdec0, socket_id:0, flags:0
ovs-ctl[3560]: Zone 1: name:<MP_log_history>, phys:0x83fd73d40, len:0x28a0c0,
 virt:0x7f213fd73d40, socket_id:0, flags:0
ovs-ctl[3560]: Zone 2: name:<rte_eth_dev_data>, phys:0x83fd43380, len:0x2f700,
 virt:0x7f213fd43380, socket_id:0, flags:0
ovs-ctl[3560]: * Starting ovs-vswitchd
ovs-ctl[3560]: * Enabling remote OVSDB managers
systemd[1]: Started Open vSwitch Internal Unit.
systemd[1]: Starting Open vSwitch...
systemd[1]: Started Open vSwitch.


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

SYSLOG:
```

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

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


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

SYSLOG:
2016-01-22T08:59:06.369Z|00019|memory|INFO|peak resident set size grew 155% in last 10.0
 seconds, from 37256 kB to 95008 kB
2016-01-22T08:59:06.369Z|00020|memory|INFO|handlers:4 ports:1 revalidators:2 rules:5
2016-01-22T08:59:30.989Z|00021|dpdk|INFO|Port 0: 8c:dc:d4:b3:6d:e9
2016-01-22T08:59:31.520Z|00022|dpdk|INFO|Port 0: 8c:dc:d4:b3:6d:e9
2016-01-22T08:59:31.521Z|00023|dpif_netdev|INFO|Created 1 pmd threads on numa node 0
2016-01-22T08:59:31.522Z|00001|dpif_netdev(pmd16)|INFO|Core 0 processing port 'dpdk0'
2016-01-22T08:59:31.522Z|00024|bridge|INFO|bridge ovsdpdkbr0: added interface dpdk0 on port
 1
2016-01-22T08:59:31.522Z|00025|bridge|INFO|bridge ovsdpdkbr0: using datapath ID
 00008cdcd4b36de9
2016-01-22T08:59:31.523Z|00002|dpif_netdev(pmd16)|INFO|Core 0 processing port 'dpdk0'

OVS-LOG:
ovs-vsctl: ovs|00001|vsctl|INFO|Called as ovs-vsctl add-port ovsdpdkbr0 dpdk0 -- set
 Interface dpdk0 type=dpdk
```

```
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a79ebc0
 hw_ring=0x7f211a7a6c00 dma_addr=0x81a7a6c00
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_rx_queue_setup(): sw_ring=0x7f211a78a6c0
 sw_sc_ring=0x7f211a786580 hw_ring=0x7f211a78e800 dma_addr=0x81a78e800
ovs-vswitchd[3595]: PMD: ixgbe_set_rx_function(): Vector rx enabled, please make sure RX
 burst size no less than 4 (port=0).
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a79ebc0
 hw_ring=0x7f211a7a6c00 dma_addr=0x81a7a6c00
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a76e4c0
 hw_ring=0x7f211a776500 dma_addr=0x81a776500
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a756440
 hw_ring=0x7f211a75e480 dma_addr=0x81a75e480
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a73e3c0
 hw_ring=0x7f211a746400 dma_addr=0x81a746400
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a726340
 hw_ring=0x7f211a72e380 dma_addr=0x81a72e380
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a70e2c0
 hw_ring=0x7f211a716300 dma_addr=0x81a716300
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a6f6240
 hw_ring=0x7f211a6fe280 dma_addr=0x81a6fe280
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a6de1c0
 hw_ring=0x7f211a6e6200 dma_addr=0x81a6e6200
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a6c6140
 hw_ring=0x7f211a6ce180 dma_addr=0x81a6ce180
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a6ae0c0
 hw_ring=0x7f211a6b6100 dma_addr=0x81a6b6100
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a696040
 hw_ring=0x7f211a69e080 dma_addr=0x81a69e080
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
```

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


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

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

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

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

5.10. Resources

- *DPDK Documentation*[40]
- *Release Notes matching the version packages in Ubuntu 16.04*[41]
- *Linux DPDK User Getting Started*[42]
- *EAL Command-line Options*[43]
- *DPDK Api Documentation*[44]
- *OpenVswitch DPDK installation*[45]

[40] http://dpdk.org/doc
[41] http://dpdk.org/doc/guides/rel_notes/release_2_2.html
[42] http://dpdk.org/doc/guides/linux_gsg/index.html
[43] http://dpdk.org/doc/guides/testpmd_app_ug/run_app.html
[44] http://dpdk.org/doc/api/
[45] https://github.com/openvswitch/ovs/blob/branch-2.5/INSTALL.DPDK.md

- *Wikipedias definition of DPDK*[46]

[46] https://en.wikipedia.org/wiki/Data_Plane_Development_Kit

Chapter 5. DM-Multipath

1. Device Mapper Multipathing

Device mapper multipathing (DM-Multipath) allows you to configure multiple I/O paths between server nodes and storage arrays into a single device. These I/O paths are physical SAN connections that can include separate cables, switches, and controllers. Multipathing aggregates the I/O paths, creating a new device that consists of the aggregated paths. This chapter provides a summary of the features of DM-Multipath that are new for the initial release of Ubuntu Server 12.04. Following that, this chapter provides a high-level overview of DM Multipath and its components, as well as an overview of DM-Multipath setup.

1.1. New and Changed Features for Ubuntu Server 12.04

Migrated from multipath-0.4.8 to multipath-0.4.9

1.1.1. Migration from 0.4.8

The priority checkers are no longer run as standalone binaries, but as shared libraries. The key value name for this feature has also slightly changed. Copy the attribute named **prio_callout** to **prio**, also modify the argument the name of the priority checker, a system path is no longer necessary. Example conversion:

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

See Table *Priority Checker Conversion [p. 73]* for a complete listing

Table 5.1. Priority Checker Conversion

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

Since the multipath config file parser essentially parses all key/value pairs it finds and then makes use of them, it is safe for both **prio_callout** and **prio** to coexist and is recommended that the **prio** attribute be inserted before beginning migration. After which you can safely delete the legacy **prio_calliout** attribute without interrupting service.

1.2. Overview

DM-Multipath can be used to provide:

- *Redundancy* DM-Multipath can provide failover in an active/passive configuration. In an active/passive configuration, only half the paths are used at any time for I/O. If any element of an I/O path (the cable, switch, or controller) fails, DM-Multipath switches to an alternate path.
- *Improved Performance* Performance DM-Multipath can be configured in active/active mode, where I/O is spread over the paths in a round-robin fashion. In some configurations, DM-Multipath can detect loading on the I/O paths and dynamically re-balance the load.

1.3. Storage Array Overview

By default, DM-Multipath includes support for the most common storage arrays that support DM-Multipath. The supported devices can be found in the multipath.conf.defaults file. If your storage array supports DM-Multipath and is not configured by default in this file, you may need to add them to the DM-Multipath configuration file, multipath.conf. For information on the DM-Multipath configuration file, see Section, *The DM-Multipath Configuration File*. Some storage arrays require special handling of I/O errors and path switching. These require separate hardware handler kernel modules.

1.4. DM-Multipath components

Table *DM-Multipath Components* describes the components of the DM-Multipath package.

Table 5.2. DM-Multipath Components

Component	Description
dm_multipath kernel module	Reroutes I/O and supports **failover** for paths and path groups.
multipath command	Lists and configures **multipath** devices. Normally started up with `/etc/rc.sysinit`, it can also be started up by a udev program whenever a block device is added or it can be run by the initramfs file system.
multipathd daemon	Monitors paths; as paths fail and come back, it may initiate path group switches. Provides for interactive changes to **multipath** devices. This daemon must be restarted for any changes to the `/etc/multipath.conf` file to take effect.
kpartx command	Creates device mapper devices for the partitions on a device It is necessary to use this command for DOS-based partitions with DM-Multipath. The kpartx is provided in its own package, but the **multipath-tools** package depends on it.

1.5. DM-Multipath Setup Overview

DM-Multipath includes compiled-in default settings that are suitable for common multipath configurations. Setting up DM-multipath is often a simple procedure. The basic procedure for configuring your system with DM-Multipath is as follows:

1. Install the **multipath-tools** and **multipath-tools-boot** packages

2. Create an empty config file, `/etc/multipath.conf`, that re-defines the *following*
3. If necessary, edit the **multipath.conf** configuration file to modify default values and save the updated file.
4. Start the multipath daemon
5. Update initial ramdisk

For detailed setup instructions for multipath configuration see Section, *Setting Up DM-Multipath*.

2. Multipath Devices

Without DM-Multipath, each path from a server node to a storage controller is treated by the system as a separate device, even when the I/O path connects the same server node to the same storage controller. DM-Multipath provides a way of organizing the I/O paths logically, by creating a single multipath device on top of the underlying devices.

2.1. Multipath Device Identifiers

Each multipath device has a World Wide Identifier (WWID), which is guaranteed to be globally unique and unchanging. By default, the name of a multipath device is set to its WWID. Alternately, you can set the ***user_friendly_names*** option in the multipath configuration file, which causes DM-Multipath to use a node-unique alias of the form **mpathn** as the name. For example, a node with two HBAs attached to a storage controller with two ports via a single unzoned FC switch sees four devices: **/dev/sda**, **/dev/sdb**, **/dev/sdc**, and **/dev/sdd**. DM-Multipath creates a single device with a unique WWID that reroutes I/O to those four underlying devices according to the multipath configuration. When the ***user_friendly_names*** configuration option is set to **yes**, the name of the multipath device is set to **mpathn**. When new devices are brought under the control of DM-Multipath, the new devices may be seen in two different places under the **/dev** directory: **/dev/mapper/mpathn** and **/dev/dm-n**.

- The devices in **/dev/mapper** are created early in the boot process. Use these devices to access the multipathed devices, for example when creating logical volumes.
- Any devices of the form **/dev/dm-n** are for internal use only and should never be used.

For information on the multipath configuration defaults, including the ***user_friendly_names*** configuration option, see Section , *Configuration File Defaults*. You can also set the name of a multipath device to a name of your choosing by using the ***alias*** option in the **multipaths** section of the multipath configuration file. For information on the **multipaths** section of the multipath configuration file, see Section, *Multipaths Device Configuration Attributes*.

2.2. Consistent Multipath Device Names in a Cluster

When the **user_friendly_names** configuration option is set to yes, the name of the multipath device is unique to a node, but it is not guaranteed to be the same on all nodes using the multipath device. Similarly, if you set the **alias** option for a device in the **multipaths** section of the `multipath.conf` configuration file, the name is not automatically consistent across all nodes in the cluster. This should not cause any difficulties if you use LVM to create logical devices from the multipath device, but if you require that your multipath device names be consistent in every node it is recommended that you leave the **user_friendly_names** option set to **no** and that you not configure aliases for the devices. By default, if you do not set **user_friendly_names** to yes or configure an alias for a device, a device name will be the WWID for the device, which is always the same. If you want the system-defined user-friendly names to be consistent across all nodes in the cluster, however, you can follow this procedure:

1. Set up all of the multipath devices on one machine.
2. Disable all of your multipath devices on your other machines by running the following commands:

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

3. Copy the `/etc/multipath/bindings` file from the first machine to all the other machines in the cluster.
4. Re-enable the multipathd daemon on all the other machines in the cluster by running the following command:

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

If you add a new device, you will need to repeat this process.

Similarly, if you configure an alias for a device that you would like to be consistent across the nodes in the cluster, you should ensure that the `/etc/multipath.conf` file is the same for each node in the cluster by following the same procedure:

1. Configure the aliases for the multipath devices in the in the `multipath.conf` file on one machine.
2. Disable all of your multipath devices on your other machines by running the following commands:

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

3. Copy the `multipath.conf` file from the first machine to all the other machines in the cluster.
4. Re-enable the multipathd daemon on all the other machines in the cluster by running the following command:

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

When you add a new device you will need to repeat this process.

2.3. Multipath Device attributes

In addition to the **user_friendly_names** and **alias** options, a multipath device has numerous attributes. You can modify these attributes for a specific multipath device by creating an entry for that device in the **multipaths** section of the **multipath** configuration file. For information on the **multipaths** section of the multipath configuration file, see Section, "*Configuration File Multipath Attributes*".

2.4. Multipath Devices in Logical Volumes

After creating multipath devices, you can use the multipath device names just as you would use a physical device name when creating an LVM physical volume. For example, if /dev/mapper/mpatha is the name of a multipath device, the following command will mark /dev/mapper/mpatha as a physical volume.

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

You can use the resulting LVM physical device when you create an LVM volume group just as you would use any other LVM physical device.

If you attempt to create an LVM physical volume on a whole device on which you have configured partitions, the pvcreate command will fail.

When you create an LVM logical volume that uses active/passive multipath arrays as the underlying physical devices, you should include filters in the **lvm.conf** to exclude the disks that underlie the multipath devices. This is because if the array automatically changes the active path to the passive path when it receives I/O, multipath will failover and failback whenever LVM scans the passive path if these devices are not filtered. For active/passive arrays that require a command to make the passive path active, LVM prints a warning message when this occurs. To filter all SCSI devices in the LVM configuration file (lvm.conf), include the following filter in the devices section of the file.

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

After updating `/etc/lvm.conf`, it's necessary to update the **initrd** so that this file will be copied there, where the filter matters the most, during boot. Perform:

```
update-initramfs -u -k all
```

Every time either `/etc/lvm.conf` or `/etc/multipath.conf` is updated, the initrd should be rebuilt to reflect these changes. This is imperative when blacklists and filters are necessary to maintain a stable storage configuration.

3. Setting up DM-Multipath Overview

This section provides step-by-step example procedures for configuring DM-Multipath. It includes the following procedures:

- Basic DM-Multipath setup
- Ignoring local disks
- Adding more devices to the configuration file

3.1. Setting Up DM-Multipath

Before setting up DM-Multipath on your system, ensure that your system has been updated and includes the **multipath-tools** package. If boot from SAN is desired, then the **multipath-tools-boot** package is also required.

A basic **/etc/multipath.conf** need not even exist, when **multpath** is run without an accompanying `/etc/multipath.conf`, it draws from it's internal database to find a suitable configuration, it also draws from it's internal blacklist. If after running **multipath -ll** without a config file, no multipaths are discovered. One must proceed to increase the verbosity to discover why a multipath was not created. Consider referencing the SAN vendor's documentation, the multipath example config files found in `/usr/share/doc/multipath-tools/examples`, and the live multipathd database:

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

To work around a quirk in multipathd, when an `/etc/multipath.conf` doesn't exist, the previous command will return nothing, as it is the result of a *merge* between the `/etc/multipath.conf` and the database in memory. To remedy this, either define an empty `/etc/multipath.conf`, by using **touch**, or create one that redefines a default value like:

```
defaults {
        user_friendly_names no
}
```

and restart multipathd:

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

Now the "show config" command will return the live database.

3.2. Installing with Multipath Support

To enable *multipath support during installation*[1] use

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

at the installer prompt. If multipath devices are found these will show up as **/dev/mapper/mpath<X>** during installation.

[1] http://wiki.debian.org/DebianInstaller/MultipathSupport

3.3. Ignoring Local Disks When Generating Multipath Devices

Some machines have local SCSI cards for their internal disks. DM-Multipath is not recommended for these devices. The following procedure shows how to modify the multipath configuration file to ignore the local disks when configuring multipath.

1. Determine which disks are the internal disks and mark them as the ones to blacklist. In this example, **/dev/sda** is the internal disk. Note that as originally configured in the default multipath configuration file, executing the **multipath -v2** shows the local disk, **/dev/sda**, in the multipath map. For further information on the **multipath** command output, see Section *Multipath Command Output*.

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

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

create: 3600a0b800013275100000009a436215ec undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:1 sdc 8:32 undef ready  running
    `- 3:0:0:1 sdg 8:96 undef ready  running

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

create: 3600a0b800013275100000009b4362163e undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:3 sdd 8:64 undef ready  running
    `- 3:0:0:3 sdg 8:128 undef ready  running
```

2. In order to prevent the device mapper from mapping **/dev/sda** in its multipath maps, edit the blacklist section of the `/etc/multipath.conf` file to include this device. Although you could blacklist the **sda** device using a **devnode** type, that would not be safe procedure since **/dev/sda** is not guaranteed to be the same on reboot. To blacklist individual devices, you can blacklist using the WWID of that device. Note that in the output to the **multipath -v2** command, the WWID of the `/dev/sda` device is SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1. To blacklist this device, include the following in the `/etc/multipath.conf` file.

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

3. After you have updated the `/etc/multipath.conf` file, you must manually tell the **multipathd** daemon to reload the file. The following command reloads the updated `/etc/multipath.conf` file.

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

4. Run the following command to remove the multipath device:

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

5. To check whether the device removal worked, you can run the **multipath -ll** command to display the current multipath configuration. For information on the **multipath -ll** command, see Section *Multipath Queries with multipath Command*. To check that the blacklisted device was not added back, you can run the multipath command, as in the following example. The multipath command defaults to a verbosity level of **v2** if you do not specify a **-v** option.

```
# multipath

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

create: 3600a0b800013275100000009a436215ec undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:1 sdc 8:32 undef ready  running
    `- 3:0:0:1 sdg 8:96 undef ready  running

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

create: 3600a0b800013275100000009b4362163e undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:3 sdd 8:64 undef ready  running
    `- 3:0:0:3 sdg 8:128 undef ready  running
```

3.4. Configuring Storage Devices

By default, DM-Multipath includes support for the most common storage arrays that support DM-Multipath. The default configuration values, including supported devices, can be found in the `multipath.conf.defaults` file.

If you need to add a storage device that is not supported by default as a known multipath device, edit the `/etc/multipath.conf` file and insert the appropriate device information.

For example, to add information about the HP Open-V series the entry looks like this, where **%n** is the device name:

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

For more information on the devices section of the configuration file, see Section *Configuration File Devices [p. 91]*.

4. The DM-Multipath Configuration File

By default, DM-Multipath provides configuration values for the most common uses of multipathing. In addition, DM-Multipath includes support for the most common storage arrays that support DM-Multipath. The default configuration values and the supported devices can be found in the `multipath.conf.defaults` file.

You can override the default configuration values for DM-Multipath by editing the `/etc/multipath.conf` configuration file. If necessary, you can also add a storage array that is not supported by default to the configuration file. This chapter provides information on parsing and modifying the `multipath.conf` file. It contains sections on the following topics:

- *Configuration File Overview [p. 83]*
- *Configuration File Blacklist [p. 84]*
- *Configuration File Defaults [p. 86]*
- *Configuration File Multipath Attributes [p. 90]*
- *Configuration File Devices [p. 91]*

In the multipath configuration file, you need to specify only the sections that you need for your configuration, or that you wish to change from the default values specified in the `multipath.conf.defaults` file. If there are sections of the file that are not relevant to your environment or for which you do not need to override the default values, you can leave them commented out, as they are in the initial file.

The configuration file allows regular expression description syntax.

An annotated version of the configuration file can be found in `/usr/share/doc/multipath-tools/examples/multipath.conf.annotated.gz`.

4.1. Configuration File Overview

The multipath configuration file is divided into the following sections:

blacklist

Listing of specific devices that will not be considered for multipath.

blacklist_exceptions

Listing of multipath candidates that would otherwise be blacklisted according to the parameters of the blacklist section.

defaults

General default settings for DM-Multipath.

multipath

Settings for the characteristics of individual multipath devices. These values overwrite what is specified in the **defaults** and **devices** sections of the configuration file.

devices

Settings for the individual storage controllers. These values overwrite what is specified in the **defaults** section of the configuration file. If you are using a storage array that is not supported by default, you may need to create a devices subsection for your array.

When the system determines the attributes of a multipath device, first it checks the multipath settings, then the per devices settings, then the multipath system defaults.

4.2. Configuration File Blacklist

The blacklist section of the multipath configuration file specifies the devices that will not be used when the system configures multipath devices. Devices that are blacklisted will not be grouped into a multipath device.

- If you do need to blacklist devices, you can do so according to the following criteria:
  - By WWID, as described *Blacklisting By WWID [p. 84]*
  - By device name, as described in *Blacklisting By Device Name [p. 84]*
  - By device type, as described in *Blacklisting By Device Type [p. 85]*

  By default, a variety of device types are blacklisted, even after you comment out the initial blacklist section of the configuration file. For information, see *Blacklisting By Device Name [p. 84]*

4.2.1. Blacklisting By WWID

You can specify individual devices to blacklist by their World-Wide IDentification with a **wwid** entry in the **blacklist** section of the configuration file.

The following example shows the lines in the configuration file that would blacklist a device with a WWID of 26353900f02796769.

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

4.2.2. Blacklisting By Device Name

You can blacklist device types by device name so that they will not be grouped into a multipath device by specifying a **devnode** entry in the **blacklist** section of the configuration file.

The following example shows the lines in the configuration file that would blacklist all SCSI devices, since it blacklists all sd* devices.

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

You can use a **devnode** entry in the **blacklist** section of the configuration file to specify individual devices to blacklist rather than all devices of a specific type. This is not recommended, however, since unless it is

statically mapped by udev rules, there is no guarantee that a specific device will have the same name on reboot. For example, a device name could change from `/dev/sda` to `/dev/sdb` on reboot.

By default, the following **devnode** entries are compiled in the default blacklist; the devices that these entries blacklist do not generally support DM-Multipath. To enable multipathing on any of these devices, you would need to specify them in the **blacklist_exceptions** section of the configuration file, as described in *Blacklist Exceptions [p. 85]*

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

4.2.3. Blacklisting By Device Type

You can specify specific device types in the **blacklist** section of the configuration file with a device section. The following example blacklists all IBM DS4200 and HP devices.

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

4.2.4. Blacklist Exceptions

You can use the **blacklist_exceptions** section of the configuration file to enable multipathing on devices that have been blacklisted by default.

For example, if you have a large number of devices and want to multipath only one of them (with the WWID of 3600d0230000000000e13955cc3757803), instead of individually blacklisting each of the devices except the one you want, you could instead blacklist all of them, and then allow only the one you want by adding the following lines to the `/etc/multipath.conf` file.

```
blacklist {
        wwid "*"
}

blacklist_exceptions {
        wwid "3600d0230000000000e13955cc3757803"
}
```

When specifying devices in the **blacklist_exceptions** section of the configuration file, you must specify the exceptions in the same way they were specified in the **blacklist**. For example, a WWID exception will not

apply to devices specified by a **devnode** blacklist entry, even if the blacklisted device is associated with that WWID. Similarly, devnode exceptions apply only to devnode entries, and device exceptions apply only to device entries.

4.3. Configuration File Defaults

The `/etc/multipath.conf` configuration file includes a **defaults** section that sets the **user_friendly_names** parameter to **yes**, as follows.

```
defaults {
        user_friendly_names yes
}
```

This overwrites the default value of the **user_friendly_names** parameter.

The configuration file includes a template of configuration defaults. This section is commented out, as follows.

```
#defaults {
#       udev_dir                /dev
#       polling_interval        5
#       selector                "round-robin 0"
#       path_grouping_policy    failover
#       getuid_callout          "/lib/dev/scsi_id --whitelisted --device=/dev/%n"
# prio   const
# path_checker  directio
# rr_min_io  1000
# rr_weight  uniform
# failback  manual
# no_path_retry  fail
# user_friendly_names no
#}
```

To overwrite the default value for any of the configuration parameters, you can copy the relevant line from this template into the **defaults** section and uncomment it. For example, to overwrite the **path_grouping_policy** parameter so that it is **multibus** rather than the default value of **failover**, copy the appropriate line from the template to the initial **defaults** section of the configuration file, and uncomment it, as follows.

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

Table *Multipath Configuration Defaults [p. 87]* describes the attributes that are set in the **defaults** section of the `multipath.conf` configuration file. These values are used by DM-Multipath unless they are overwritten by the attributes specified in the **devices** and **multipaths** sections of the `multipath.conf` file.

Table 5.3. Multipath Configuration Defaults

Attribute	Description
polling_interval	Specifies the interval between two path checks in seconds. For properly functioning paths, the interval between checks will gradually increase to (4 * **polling_interval**). The default value is **5**.
udev_dir	The directory where udev device nodes are created. The default value is /dev.
multipath_dir	The directory where the dynamic shared objects are stored. The default value is system dependent, commonly `/lib/multipath`.
verbosity	The default verbosity. Higher values increase the verbosity level. Valid levels are between 0 and 6. The default value is 2.
path_selector	Specifies the default algorithm to use in determining what path to use for the next I/O operation. Possible values include: • **round-robin 0**: Loop through every path in the path group, sending the same amount of I/O to each. • **queue-length 0**: Send the next bunch of I/O down the path with the least number of outstanding I/O requests. • **service-time 0**: Send the next bunch of I/O down the path with the shortest estimated service time, which is determined by dividing the total size of the outstanding I/O to each path by its relative throughput. The default value is **round-robin 0**.
path_grouping_policy	Specifies the default path grouping policy to apply to unspecified multipaths. Possible values include: • **failover** = 1 path per priority group • **multibus** = all valid paths in 1 priority group • **group_by_serial** = 1 priority group per detected serial number • **group_by_prio** = 1 priority group per path priority value • **group_by_node_name** = 1 priority group per target node name. The default value is **failover.**
getuid_callout	Specifies the default program and arguments to call out to obtain a unique path identifier. An absolute path is required. The default value is **/lib/udev/scsi_id --whitelisted --device=/dev/%n.**

Attribute	Description
prio	Specifies the default function to call to obtain a path priority value. For example, the ALUA bits in SPC-3 provide an exploitable prio value. Possible values include: • **const**: Set a priority of 1 to all paths. • **emc**: Generate the path priority for EMC arrays. • **alua**: Generate the path priority based on the SCSI-3 ALUA settings. • **netapp**: Generate the path priority for NetApp arrays. • **rdac**: Generate the path priority for LSI/Engenio RDAC controller. • **hp_sw**: Generate the path priority for Compaq/HP controller in active/standby mode. • **hds**: Generate the path priority for Hitachi HDS Modular storage arrays. The default value is **const**.
prio_args	The arguments string passed to the prio function Most prio functions do not need arguments. The datacore prioritizer need one. Example, **"timeout=1000 preferredsds=foo"**. The default value is (null) **""**.
features	The extra features of multipath devices. The only existing feature is **queue_if_no_path**, which is the same as setting **no_path_retry** to **queue**. For information on issues that may arise when using this feature, see Section, *"Issues with queue_if_no_path feature"*.
path_checker	Specifies the default method used to determine the state of the paths. Possible values include: • **readsector0**: Read the first sector of the device. • **tur**: Issue a TEST UNIT READY to the device. • **emc_clariion**: Query the EMC Clariion specific EVPD page 0xC0 to determine the path. • **hp_sw**: Check the path state for HP storage arrays with Active/Standby firmware. • **rdac**: Check the path status for LSI/Engenio RDAC storage controller. • **directio**: Read the first sector with direct I/O. The default value is **directio**.
failback	Manages path group failback. • A value of **immediate** specifies immediate failback to the highest priority path group that contains active paths.

Attribute	Description
	• A value of **manual** specifies that there should not be immediate failback but that failback can happen only with operator intervention. • A numeric value greater than zero specifies deferred failback, expressed in seconds. The default value is **manual**.
rr_min_io	Specifies the number of I/O requests to route to a path before switching to the next path in the current path group. The default value is `1000`.
rr_weight	If set to **priorities**, then instead of sending **rr_min_io** requests to a path before calling **path_selector** to choose the next path, the number of requests to send is determined by **rr_min_io** times the path's priority, as determined by the prio function. If set to **uniform**, all path weights are equal. The default value is **uniform**.
no_path_retry	A numeric value for this attribute specifies the number of times the system should attempt to use a failed path before disabling queueing. A value of fail indicates **immediate** failure, without queueing. A value of **queue** indicates that queueing should not stop until the path is fixed. The default value is `0`.
user_friendly_names	If set to yes, specifies that the system should use the `/etc/multipath/bindings` file to assign a persistent and unique **alias** to the **multipath**, in the form of mpathn. If set to no, specifies that the system should use the WWID as the **alias** for the **multipath**. In either case, what is specified here will be overridden by any device-specific aliases you specify in the multipaths section of the configuration file. The default value is **no**.
queue_without_daemon	If set to no, the **multipathd** daemon will disable queueing for all devices when it is shut down. The default value is **yes**.
flush_on_last_del	If set to yes, then **multipath** will disable queueing when the last path to a device has been deleted. The default value is **no**.
max_fds	Sets the maximum number of open file descriptors that can be opened by **multipath** and the **multipathd** daemon. This is equivalent to the

Attribute	Description
	ulimit -n command. A value of max will set this to the system limit from `/proc/sys/fs/nr_open`. If this is not set, the maximum number of open file descriptors is taken from the calling process; it is usually 1024. To be safe, this should be set to the maximum number of paths plus 32, if that number is greater than 1024.
checker_timer	The timeout to use for path checkers that issue SCSI commands with an explicit timeout, in seconds. The default value is taken from `/sys/block/sdx/device/timeout`, which is `30` seconds as of 12.04 LTS
fast_io_fail_tmo	The number of seconds the SCSI layer will wait after a problem has been detected on an FC remote port before failing I/O to devices on that remote port. This value should be smaller than the value of dev_loss_tmo. Setting this to off will disable the timeout. The default value is determined by the OS.
dev_loss_tmo	The number of seconds the SCSI layer will wait after a problem has been detected on an FC remote port before removing it from the system. Setting this to infinity will set this to 2147483647 seconds, or 68 years. The default value is determined by the OS.

4.4. Configuration File Multipath Attributes

Table *Multipath Attributes [p. 90]* shows the attributes that you can set in the **multipaths** section of the `multipath.conf` configuration file for each specific multipath device. These attributes apply only to the one specified multipath. These defaults are used by DM-Multipath and override attributes set in the **defaults** and **devices** sections of the multipath.conf file.

Table 5.4. Multipath Attributes

Attribute	Description
wwid	Specifies the WWID of the **multipath** device to which the **multipath** attributes apply. This parameter is mandatory for this section of the `multipath.conf` file.
alias	Specifies the symbolic name for the **multipath** device to which the **multipath** attributes apply. If you are using **user_friendly_names**, do not set this value to mpathn; this may conflict with an automatically assigned user friendly name and give you incorrect device node names.

In addition, the following parameters may be overridden in this **multipath** section

- *`path_grouping_policy`*
- *`path_selector`*

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

The following example shows multipath attributes specified in the configuration file for two specific multipath devices. The first device has a WWID of 3600508b4000156d70001200000b0000 and a symbolic name of yellow.

The second multipath device in the example has a WWID of 1DEC_____321816758474 and a symbolic name of red. In this example, the *rr_weight* attributes are set to priorities.

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

4.5. Configuration File Devices

Table *Device Attributes [p. 92]* shows the attributes that you can set for each individual storage device in the devices section of the multipath.conf configuration file. These attributes are used by DM-Multipath unless they are overwritten by the attributes specified in the **multipaths** section of the `multipath.conf` file for paths that contain the device. These attributes override the attributes set in the **defaults** section of the `multipath.conf` file.

Many devices that support multipathing are included by default in a multipath configuration. The values for the devices that are supported by default are listed in the `multipath.conf.defaults` file. You probably will not need to modify the values for these devices, but if you do you can overwrite the default values by including an entry in the configuration file for the device that overwrites those values. You can copy the device configuration defaults from the `multipath.conf.annotated.gz` or if you wish to have a brief config file, `multipath.conf.synthetic` file for the device and override the values that you want to change.

To add a device to this section of the configuration file that is not configured automatically by default, you must set the **vendor** and **product** parameters. You can find these values by looking at **/sys/block/device_name/device/vendor** and **/sys/block/device_name/device/model** where device_name is the device to be multipathed, as in the following example:

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

The additional parameters to specify depend on your specific device. If the device is active/active, you will usually not need to set additional parameters. You may want to set *path_grouping_policy* to **multibus**. Other parameters you may need to set are *no_path_retry* and *rr_min_io*, as described in Table *Multipath Attributes [p. 90]*.

If the device is active/passive, but it automatically switches paths with I/O to the passive path, you need to change the checker function to one that does not send I/O to the path to test if it is working (otherwise, your device will keep failing over). This almost always means that you set the *path_checker* to **tur**; this works for all SCSI devices that support the Test Unit Ready command, which most do.

If the device needs a special command to switch paths, then configuring this device for multipath requires a hardware handler kernel module. The current available hardware handler is emc. If this is not sufficient for your device, you may not be able to configure the device for multipath.

Table 5.5. Device Attributes

Attribute	Description
vendor	Specifies the vendor name of the storage device to which the device attributes apply, for example **COMPAQ**.
product	Specifies the product name of the storage device to which the device attributes apply, for example **HSV110 (C)COMPAQ**.
revision	Specifies the product revision identifier of the storage device.
product_blacklist	Specifies a regular expression used to blacklist devices by product.
hardware_handler	Specifies a module that will be used to perform hardware specific actions when switching path groups or handling I/O errors. Possible values include: • **1 emc**: hardware handler for EMC storage arrays • **1 alua**: hardware handler for SCSI-3 ALUA arrays. • **1 hp_sw**: hardware handler for Compaq/HP controllers. • **1 rdac**: hardware handler for the LSI/Engenio RDAC controllers.

In addition, the following parameters may be overridden in this **device** section

- *path_grouping_policy*

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

Whenever a hardware_handler is specified, it is your responsibility to ensure that the appropriate kernel module is loaded to support the specified interface. These modules can be found in **/lib/modules/`uname -r`/kernel/drivers/scsi/device_handler/** . The requisite module should be integrated into the initrd to ensure the necessary discovery and failover-failback capacity is available during boot time. Example,

```
# echo scsi_dh_alua >> /etc/initramfs-tools/modules  ## append module to file
# update-initramfs -u -k all
```

The following example shows a device entry in the multipath configuration file.

```
#devices {
# device {
#  vendor   "COMPAQ  "
#  product   "MSA1000         "
#  path_grouping_policy multibus
#  path_checker  tur
#  rr_weight  priorities
# }
#}
```

The spacing reserved in the **vendor**, **product**, and **revision** fields are significant as multipath is performing a direct match against these attributes, whose format is defined by the SCSI specification, specifically the *Standard INQUIRY*[2] command. When quotes are used, the vendor, product, and revision fields will be interpreted strictly according to the spec. Regular expressions may be integrated into the quoted strings. Should a field be defined without the requisite spacing, multipath will copy the string into the properly sized buffer and pad with the appropriate number of spaces. The specification expects the entire field to be populated by printable characters or spaces, as seen in the example above

[2] http://en.wikipedia.org/wiki/SCSI_Inquiry_Command

- vendor: 8 characters
- product: 16 characters
- revision: 4 characters

To create a more robust configuration file, regular expressions can also be used. Operators include **^ $ [ ] . * ? +**. Examples of functional regular expressions can be found by examining the live multipath database and `multipath.conf` example files found in `/usr/share/doc/multipath-tools/examples`:

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

5. DM-Multipath Administration and Troubleshooting

5.1. Resizing an Online Multipath Device

If you need to resize an online multipath device, use the following procedure

1. Resize your physical device. This is storage platform specific.
2. Use the following command to find the paths to the LUN:

   ```
   # multipath -l
   ```
3. Resize your paths. For SCSI devices, writing 1 to the `rescan` file for the device causes the SCSI driver to rescan, as in the following command:

   ```
   # echo 1 > /sys/block/device_name/device/rescan
   ```
4. Resize your multipath device by running the multipathd resize command:

   ```
   # multipathd -k 'resize map mpatha'
   ```
5. Resize the file system (assuming no LVM or DOS partitions are used):

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

5.2. Moving root File Systems from a Single Path Device to a Multipath Device

This is dramatically simplified by the use of UUIDs to identify devices as an intrinsic label. Simply install **multipath-tools-boot** and reboot. This will rebuild the initial ramdisk and afford multipath the opportunity to build it's paths before the root file system is mounted by UUID.

Whenever `multipath.conf` is updated, so should the initrd by executing **update-initramfs -u -k all**. The reason being is `multipath.conf` is copied to the ramdisk and is integral to determining the available devices for grouping via it's blacklist and device sections.

5.3. Moving swap File Systems from a Single Path Device to a Multipath Device

The procedure is exactly the same as illustrated in the previous section called *Moving root File Systems from a Single Path to a Multipath Device*.

5.4. The Multipath Daemon

If you find you have trouble implementing a multipath configuration, you should ensure the multipath daemon is running as described in *"Setting up DM-Multipath"*. The **multipathd** daemon must be running in order to use multipathd devices. Also see section *Troubleshooting with the multipathd interactive console* concerning interacting with **multipathd** as a debugging aid.

5.5. Issues with queue_if_no_path

If **features "1 queue_if_no_path"** is specified in the `/etc/multipath.conf` file, then any process that uses I/O will hang until one or more paths are restored. To avoid this, set the ***no_path_retry*** **N** parameter in the `/etc/multipath.conf`.

When you set the **no_path_retry** parameter, remove the **features "1 queue_if_no_path"** option from the `/etc/multipath.conf` file as well. If, however, you are using a multipathed device for which the `features "1 queue_if_no_path"` option is set as a compiled in default, as it is for many SAN devices, you must add `features "0"` to override this default. You can do this by copying the existing **devices** section, and just that section (not the entire file), from `/usr/share/doc/multipath-tools/examples/multipath.conf.annotated.gz` into `/etc/multipath.conf` and editing to suit your needs.

If you need to use the `features "1 queue_if_no_path"` option and you experience the issue noted here, use the **dmsetup** command to edit the policy at runtime for a particular LUN (that is, for which all the paths are unavailable). For example, if you want to change the policy on the multipath device `mpathc` from `"queue_if_no_path"` to `"fail_if_no_path"`, execute the following command.

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

You must specify the `mpathN` alias rather than the path

5.6. Multipath Command Output

When you create, modify, or list a multipath device, you get a printout of the current device setup. The format is as follows. For each multipath device:

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

For each path group:

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

For each path:

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

For example, the output of a multipath command might appear as follows:

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

If the path is up and ready for I/O, the status of the path is **ready** or *ghost*. If the path is down, the status is **faulty** or **shaky**. The path status is updated periodically by the **multipathd** daemon based on the polling interval defined in the `/etc/multipath.conf` file.

The dm status is similar to the path status, but from the kernel's point of view. The dm status has two states: **failed**, which is analogous to **faulty**, and **active** which covers all other path states. Occasionally, the path state and the dm state of a device will temporarily not agree.

The possible values for **online_status** are **running** and **offline**. A status of *offline* means that the SCSI device has been disabled.

When a multipath device is being created or modified , the path group status, the dm device name, the write permissions, and the dm status are not known. Also, the features are not always correct

5.7. Multipath Queries with multipath Command

You can use the **-l** and **-ll** options of the **multipath** command to display the current multipath configuration. The **-l** option displays multipath topology gathered from information in sysfs and the device mapper. The **-ll** option displays the information the **-l** displays in addition to all other available components of the system.

When displaying the multipath configuration, there are three verbosity levels you can specify with the **-v** option of the multipath command. Specifying **-v0** yields no output. Specifying **-v1** outputs the created or updated multipath names only, which you can then feed to other tools such as kpartx. Specifying **-v2** prints all detected paths, multipaths, and device maps.

The default **verbosity** level of multipath is **2** and can be globally modified by defining the *verbosity attribute* in the **defaults** section of `multipath.conf`.

The following example shows the output of a **multipath -l** command.

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

The following example shows the output of a **multipath -ll** command.

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

5.8. Multipath Command Options

Table *Useful multipath Command Options [p. 98]* describes some options of the **multipath** command that you might find useful.

Table 5.6. Useful multipath Command Options

Option	Description
-l	Display the current multipath configuration gathered from **sysfs** and the device mapper.
-ll	Display the current multipath configuration gathered from **sysfs**, the device mapper, and all other available components on the system.
-f device	Remove the named multipath device.
-F	Remove all unused multipath devices.

5.9. Determining Device Mapper Entries with dmsetup Command

You can use the **dmsetup** command to find out which device mapper entries match the **multipathed** devices.

The following command displays all the device mapper devices and their major and minor numbers. The minor numbers determine the name of the dm device. For example, a minor number of **3** corresponds to the multipathed device **/dev/dm-3**.

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

5.10. Troubleshooting with the multipathd interactive console

The **multipathd -k** command is an interactive interface to the **multipathd** daemon. Entering this command brings up an interactive multipath console. After entering this command, you can enter help to get a list of available commands, you can enter a interactive command, or you can enter **CTRL-D** to quit.

The multipathd interactive console can be used to troubleshoot problems you may be having with your system. For example, the following command sequence displays the multipath configuration, including the defaults, before exiting the console. See the IBM article *"Tricks with Multipathd"*[3] for more examples.

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

The following command sequence ensures that multipath has picked up any changes to the multipath.conf,

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

Use the following command sequence to ensure that the path checker is working properly.

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

Commands can also be streamed into multipathd using stdin like so:

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

[3] http://www-01.ibm.com/support/docview.wss?uid=isg3T1011985

Chapter 6. Remote Administration

There are many ways to remotely administer a Linux server. This chapter will cover three of the most popular applications OpenSSH, Puppet, and Zentyal.

1. OpenSSH Server

1.1. Introduction

This section of the Ubuntu Server Guide introduces a powerful collection of tools for the remote control of, 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, 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 install openssh-client
```

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

```
sudo apt 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 communication 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

  If the line is already present, then ensure it 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 systemctl restart sshd.service
```

Many other configuration directives for sshd are available to change 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. Additionally, if an incorrect configuration directive is supplied, the sshd server may refuse to start, 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 rsa
```

This will generate the keys using the *RSA Algorithm*. 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_rsa.pub`, while `~/.ssh/id_rsa` is the *private* key. Now copy the `id_rsa.pub` file to the remote host and append it to `~/.ssh/authorized_keys` by entering:

```
ssh-copy-id username@remotehost
```

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

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

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

1.5. References

- *Ubuntu Wiki SSH*[1] page.
- *OpenSSH Website*[2]
- *Advanced OpenSSH Wiki Page*[3]

[1] https://help.ubuntu.com/community/SSH
[2] http://www.openssh.org/
[3] https://wiki.ubuntu.com/AdvancedOpenSSH

2. Puppet

Puppet is a cross platform framework enabling system administrators to perform common tasks using code. The code can do a variety of tasks from installing new software, to checking file permissions, or updating user accounts. Puppet is great not only during the initial installation of a system, but also throughout the system's entire life cycle. In most circumstances puppet will be used in a client/server configuration.

This section will cover installing and configuring Puppet in a client/server configuration. This simple example will demonstrate how to install Apache using Puppet.

2.1. Preconfiguration

Prior to configuring puppet you may want to add a DNS *CNAME* record for *puppet.example.com*, where *example.com* is your domain. By default Puppet clients check DNS for puppet.example.com as the puppet server name, or *Puppet Master*. See *Chapter 8, Domain Name Service (DNS) [p. 163]* for more DNS details.

If you do not wish to use DNS, you can add entries to the server and client `/etc/hosts` file. For example, in the Puppet server's `/etc/hosts` file add:

```
127.0.0.1 localhost.localdomain localhost puppet
192.168.1.17 puppetclient.example.com puppetclient
```

On each Puppet client, add an entry for the server:

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

Replace the example IP addresses and domain names above with your actual server and client addresses and domain names.

2.2. Installation

To install Puppet, in a terminal on the *server* enter:

```
sudo apt install puppetmaster
```

On the *client* machine, or machines, enter:

```
sudo apt install puppet
```

2.3. Configuration

Create a folder path for the apache2 class:

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

Now setup some resources for apache2. Create a file `/etc/puppet/modules/apache2/manifests/init.pp` containing the following:

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

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

Next, create a node file `/etc/puppet/manifests/site.pp` with:

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

Replace *puppetclient.example.com* with your actual Puppet client's host name.

The final step for this simple Puppet server is to restart the daemon:

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

Now everything is configured on the Puppet server, it is time to configure the client.

First, configure the Puppet agent daemon to start. Edit `/etc/default/puppet`, changing *START* to yes:

```
START=yes
```

Then start the service:

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

View the client cert fingerprint

```
sudo puppet agent --fingerprint
```

Back on the Puppet server, view pending certificate signing requests:

```
sudo puppet cert list
```

On the Puppet server, verify the fingerprint of the client and sign puppetclient's cert:

```
sudo puppet cert sign puppetclient.example.com
```

On the Puppet client, run the puppet agent manually in the foreground. This step isn't strictly speaking necessary, but it is the best way to test and debug the puppet service.

```
sudo puppet agent --test
```

Check `/var/log/syslog` on both hosts for any errors with the configuration. If all goes well the apache2 package and it's dependencies will be installed on the Puppet client.

This example is *very* simple, and does not highlight many of Puppet's features and benefits. For more information see *Section 2.4, “Resources” [p. 106]*.

2.4. Resources

- See the *Official Puppet Documentation*[4] web site.
- See the *Puppet forge*[5], online repository of puppet modules.
- Also see *Pro Puppet*[6].

[4] http://docs.puppetlabs.com/
[5] http://forge.puppetlabs.com/
[6] http://www.apress.com/9781430230571

3. Zentyal

Zentyal is a Linux small business server that can be configured as a gateway, infrastructure manager, unified threat manager, office server, unified communication server or a combination of them. All network services managed by Zentyal are tightly integrated, automating most tasks. This saves time and helps to avoid errors in network configuration and administration. Zentyal is open source, released under the GNU General Public License (GPL) and runs on top of Ubuntu GNU/Linux.

Zentyal consists of a series of packages (usually one for each module) that provide a web interface to configure the different servers or services. The configuration is stored on a key-value Redis database, but users, groups, and domains-related configuration is on OpenLDAP . When you configure any of the available parameters through the web interface, final configuration files are overwritten using the configuration templates provided by the modules. The main advantage of using Zentyal is a unified, graphical user interface to configure all network services and high, out-of-the-box integration between them.

Zentyal publishes one major stable release once a year based on the latest Ubuntu LTS release.

3.1. Installation

If you would like to create a new user to access the Zentyal web interface, run:

```
sudo adduser username sudo
```

Add the Zentyal repository to your repository list:

```
sudo add-apt-repository "deb http://archive.zentyal.org/zentyal 3.5 main extra"
```

Import the public keys from Zentyal:

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 10E239FF
wget -q http://keys.zentyal.org/zentyal-4.2-archive.asc -O- | sudo apt-key add -
```

Update your packages and install Zentyal:

```
sudo apt update
sudo apt install zentyal
```

During installation you will be asked to set a root MySQL password and confirm port 443.

3.2. First steps

Any system account belonging to the sudo group is allowed to log into the Zentyal web interface. The user created while installing Ubuntu Server will belong to the sudo group by default.

To access the Zentyal web interface, point a browser to https://localhost/ or to the IP address of your remote server. As Zentyal creates its own self-signed SSL certificate, you will have to accept a security exception on your browser. Log in with the same username and password used to log in to your server.

Once logged in you will see an overview of your server. Individual modules, such as Antivirus or Firewall, can be installed by simply clicking them and then clicking Install. Selecting server roles like Gateway or Infrastructure can be used to install multiple modules at once.

Modules can also be installed via the command line:

```
sudo apt install <zentyal-module>
```

See the list of available modules below.

To enable a module, go to the Dashboard, then click Module Status. Click the check box for the module, then Save changes.

To configure any of the features of your installed modules, click the different sections on the left menu. When you make any changes, a red "Save changes" button appears in the upper right corner.

If you need to customize any configuration file or run certain actions (scripts or commands) to configure features not available on Zentyal, place the custom configuration file templates on /etc/zentyal/stubs/<module>/ and the hooks on /etc/zentyal/hooks/<module>.<action>. Read more about stubs and hooks *here*[7].

3.3. Modules

Zentyal 2.3 is available on Ubuntu 16.04 Universe repository. The modules available are:

- zentyal-core & zentyal-common: the core of the Zentyal interface and the common libraries of the framework. Also includes the logs and events modules that give the administrator an interface to view the logs and generate events from them.
- zentyal-network: manages the configuration of the network. From the interfaces (supporting static IP, DHCP, VLAN, bridges or PPPoE), to multiple gateways when having more than one Internet connection, load balancing and advanced routing, static routes or dynamic DNS.
- zentyal-objects & zentyal-services: provide an abstraction level for network addresses (e.g. LAN instead of 192.168.1.0/24) and ports named as services (e.g. HTTP instead of 80/TCP).
- zentyal-firewall: configures the iptables rules to block forbiden connections, NAT and port redirections.
- zentyal-ntp: installs the NTP daemon to keep server on time and allow network clients to synchronize their clocks against the server.
- zentyal-dhcp: configures ISC DHCP server supporting network ranges, static leases and other advanced options like NTP, WINS, dynamic DNS updates and network boot with PXE.
- zentyal-dns: brings ISC Bind9 DNS server into your server for caching local queries as a forwarder or as an authoritative server for the configured domains. Allows to configure A, CNAME, MX, NS, TXT and SRV records.
- zentyal-ca: integrates the management of a Certification Authority within Zentyal so users can use certificates to authenticate against the services, like with OpenVPN.

[7] https://wiki.zentyal.org/wiki/En/4.0/Appendix_B:_Development_and_advanced_configuration#Advanced_Service_Customization

- zentyal-openvpn: allows to configure multiple VPN servers and clients using OpenVPN with dynamic routing configuration using Quagga.
- zentyal-users: provides an interface to configure and manage users and groups on OpenLDAP. Other services on Zentyal are authenticated against LDAP having a centralized users and groups management. It is also possible to synchronize users, passwords and groups from a Microsoft Active Directory domain.
- zentyal-squid: configures Squid and Dansguardian for speeding up browsing thanks to the caching capabilities and content filtering.
- zentyal-samba: allows Samba configuration and integration with existing LDAP. From the same interface you can define password policies, create shared resources and assign permissions.
- zentyal-printers: integrates CUPS with Samba and allows not only to configure the printers but also give them permissions based on LDAP users and groups.

Not present on Ubuntu Universe repositories, but on *Zentyal Team PPA*[8] you will find these other modules:

- zentyal-antivirus: integrates ClamAV antivirus with other modules like the proxy, file sharing or mailfilter.
- zentyal-asterisk: configures Asterisk to provide a simple PBX with LDAP based authentication.
- zentyal-bwmonitor: allows to monitor bandwith usage of your LAN clients.
- zentyal-captiveportal: integrates a captive portal with the firewall and LDAP users and groups.
- zentyal-ebackup: allows to make scheduled backups of your server using the popular duplicity backup tool.
- zentyal-ftp: configures a FTP server with LDAP based authentication.
- zentyal-ids: integrates a network intrusion detection system.
- zentyal-ipsec: allows to configure IPsec tunnels using OpenSwan.
- zentyal-jabber: integrates ejabberd XMPP server with LDAP users and groups.
- zentyal-thinclients: a LTSP based thin clients solution.
- zentyal-mail: a full mail stack including Postfix and Dovecot with LDAP backend.
- zentyal-mailfilter: configures amavisd with mail stack to filter spam and attached virus.
- zentyal-monitor: integrates collectd to monitor server performance and running services.
- zentyal-pptp: configures a PPTP VPN server.
- zentyal-radius: integrates FreeRADIUS with LDAP users and groups.
- zentyal-software: simple interface to manage installed Zentyal modules and system updates.
- zentyal-trafficshaping: configures traffic limiting rules to do bandwidth throttling and improve latency.
- zentyal-usercorner: allows users to edit their own LDAP attributes using a web browser.
- zentyal-virt: simple interface to create and manage virtual machines based on libvirt.
- zentyal-webmail: allows to access your mail using the popular Roundcube webmail.
- zentyal-webserver: configures Apache webserver to host different sites on your machine.
- zentyal-zarafa: integrates Zarafa groupware suite with Zentyal mail stack and LDAP.

[8] https://launchpad.net/~zentyal/

3.4. References

Zentyal Official Documentation [9] page.

Zentyal Community Wiki[10].

Visit the *Zentyal forum* [11] for community support, feedback, feature requests, etc.

[9] http://doc.zentyal.org/
[10] http://trac.zentyal.org/wiki/Documentation
[11] http://forum.zentyal.org/

Chapter 7. Network Authentication

This section applies LDAP to network authentication and authorization.

1. OpenLDAP Server

The Lightweight Directory Access Protocol, or LDAP, is a protocol for querying and modifying a X.500-based directory service running over TCP/IP. The current LDAP version is LDAPv3, as defined in *RFC4510*[1], and the implementation in Ubuntu is OpenLDAP."

So the LDAP protocol accesses LDAP directories. Here are some key concepts and terms:

- A LDAP directory is a tree of data *entries* that is hierarchical in nature and is called the Directory Information Tree (DIT).
- An entry consists of a set of *attributes*.
- An attribute has a *type* (a name/description) and one or more *values*.
- Every attribute must be defined in at least one *objectClass*.
- Attributes and objectclasses are defined in *schemas* (an objectclass is actually considered as a special kind of attribute).
- Each entry has a unique identifier: its *Distinguished Name* (DN or dn). This, in turn, consists of a *Relative Distinguished Name* (RDN) followed by the parent entry's DN.
- The entry's DN is not an attribute. It is not considered part of the entry itself.

The terms *object*, *container*, and *node* have certain connotations but they all essentially mean the same thing as *entry*, the technically correct term.

For example, below we have a single entry consisting of 11 attributes where the following is true:

- DN is "cn=John Doe,dc=example,dc=com"
- RDN is "cn=John Doe"
- parent DN is "dc=example,dc=com"

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Larry Smith,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

The above entry is in *LDIF* format (LDAP Data Interchange Format). Any information that you feed into your DIT must also be in such a format. It is defined in *RFC2849*[2].

[1] http://tools.ietf.org/html/rfc4510
[2] http://tools.ietf.org/html/rfc2849

Although this guide will describe how to use it for central authentication, LDAP is good for anything that involves a large number of access requests to a mostly-read, attribute-based (name:value) backend. Examples include an address book, a list of email addresses, and a mail server's configuration.

1.1. Installation

Install the OpenLDAP server daemon and the traditional LDAP management utilities. These are found in packages slapd and ldap-utils respectively.

The installation of slapd will create a working configuration. In particular, it will create a database instance that you can use to store your data. However, the suffix (or base DN) of this instance will be determined from the domain name of the host. If you want something different, you can change it right after the installation when you still don't have any useful data.

This guide will use a database suffix of *dc=example,dc=com*.

Proceed with the install:

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

If you want to change your DIT suffix, now would be a good time, because changing it discards your existing one. To change the suffix, run the following command:

```
sudo dpkg-reconfigure slapd
```

To switch your DIT suffix to *dc=example,dc=com*, for example, so you can follow this guide more closely, answer *example.com* when asked about the DNS domain name.

Since Ubuntu 8.10 slapd is designed to be configured within slapd itself by dedicating a separate DIT for that purpose. This allows one to dynamically configure slapd without the need to restart the service. This configuration database consists of a collection of text-based LDIF files located under `/etc/ldap/slapd.d`. This way of working is known by several names: the slapd-config method, the RTC method (Real Time Configuration), or the cn=config method. You can still use the traditional flat-file method (slapd.conf) but it's not recommended; the functionality will be eventually phased out.

Ubuntu now uses the *slapd-config* method for slapd configuration and this guide reflects that.

During the install you were prompted to define administrative credentials. These are LDAP-based credentials for the *rootDN* of your database instance. By default, this user's DN is *cn=admin,dc=example,dc=com*. Also by default, there is no administrative account created for the slapd-config database and you will therefore need to authenticate externally to LDAP in order to access it. We will see how to do this later on.

Some classical schemas (cosine, nis, inetorgperson) come built-in with slapd nowadays. There is also an included "core" schema, a pre-requisite for any schema to work.

1.2. Post-install Inspection

The installation process set up 2 DITs. One for slapd-config and one for your own data (dc=example,dc=com). Let's take a look.

- This is what the slapd-config database/DIT looks like. Recall that this database is LDIF-based and lives under `/etc/ldap/slapd.d`:

```
/etc/ldap/slapd.d/
/etc/ldap/slapd.d/cn=config.ldif
/etc/ldap/slapd.d/cn=config
/etc/ldap/slapd.d/cn=config/cn=schema
/etc/ldap/slapd.d/cn=config/cn=schema/cn={1}cosine.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={0}core.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={2}nis.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={3}inetorgperson.ldif
/etc/ldap/slapd.d/cn=config/cn=module{0}.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={0}config.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={-1}frontend.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={1}mdb.ldif
/etc/ldap/slapd.d/cn=config/olcBackend={0}mdb.ldif
/etc/ldap/slapd.d/cn=config/cn=schema.ldif
```

Do not edit the slapd-config database directly. Make changes via the LDAP protocol (utilities).

- This is what the slapd-config DIT looks like via the LDAP protocol:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn

dn: cn=config

dn: cn=module{0},cn=config

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: olcBackend={0}mdb,cn=config

dn: olcDatabase={-1}frontend,cn=config

dn: olcDatabase={0}config,cn=config
```

```
dn: olcDatabase={1}mdb,cn=config
```

Explanation of entries:

- *cn=config*: global settings
- *cn=module{0},cn=config*: a dynamically loaded module
- *cn=schema,cn=config*: contains hard-coded system-level schema
- *cn={0}core,cn=schema,cn=config*: the hard-coded core schema
- *cn={1}cosine,cn=schema,cn=config*: the cosine schema
- *cn={2}nis,cn=schema,cn=config*: the nis schema
- *cn={3}inetorgperson,cn=schema,cn=config*: the inetorgperson schema
- *olcBackend={0}mdb,cn=config*: the 'mdb' backend storage type
- *olcDatabase={-1}frontend,cn=config*: frontend database, default settings for other databases
- *olcDatabase={0}config,cn=config*: slapd configuration database (cn=config)
- *olcDatabase={1}mdb,cn=config*: your database instance (dc=example,dc=com)

- This is what the dc=example,dc=com DIT looks like:

```
ldapsearch -x -LLL -H ldap:/// -b dc=example,dc=com dn

dn: dc=example,dc=com

dn: cn=admin,dc=example,dc=com
```

Explanation of entries:

- *dc=example,dc=com*: base of the DIT
- *cn=admin,dc=example,dc=com*: administrator (rootDN) for this DIT (set up during package install)

1.3. Modifying/Populating your Database

Let's introduce some content to our database. We will add the following:

- a node called *People* (to store users)
- a node called *Groups* (to store groups)
- a group called *miners*
- a user called *john*

Create the following LDIF file and call it `add_content.ldif`:

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

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

dn: cn=miners,ou=Groups,dc=example,dc=com
objectClass: posixGroup
cn: miners
gidNumber: 5000

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: 10000
gidNumber: 5000
userPassword: johnldap
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
```

It's important that uid and gid values in your directory do not collide with local values. Use high number ranges, such as starting at 5000. By setting the uid and gid values in ldap high, you also allow for easier control of what can be done with a local user vs a ldap one. More on that later.

Add the content:

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

Enter LDAP Password: ********
adding new entry "ou=People,dc=example,dc=com"

adding new entry "ou=Groups,dc=example,dc=com"

adding new entry "cn=miners,ou=Groups,dc=example,dc=com"

adding new entry "uid=john,ou=People,dc=example,dc=com"
```

We can check that the information has been correctly added with the ldapsearch utility:

```
ldapsearch -x -LLL -b dc=example,dc=com 'uid=john' cn gidNumber

dn: uid=john,ou=People,dc=example,dc=com
cn: John Doe
gidNumber: 5000
```

Explanation of switches:

- *-x:* "simple" binding; will not use the default SASL method
- *-LLL:* disable printing extraneous information
- *uid=john:* a "filter" to find the john user
- *cn gidNumber:* requests certain attributes to be displayed (the default is to show all attributes)

1.4. Modifying the slapd Configuration Database

The slapd-config DIT can also be queried and modified. Here are a few examples.

- Use ldapmodify to add an "Index" (DbIndex attribute) to your {1}mdb,cn=config database (dc=example,dc=com). Create a file, call it `uid_index.ldif`, with the following contents:

```
dn: olcDatabase={1}mdb,cn=config
add: olcDbIndex
olcDbIndex: mail eq,sub
```

Then issue the command:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f uid_index.ldif

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

You can confirm the change in this way:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={1}mdb)' olcDbIndex

dn: olcDatabase={1}mdb,cn=config
olcDbIndex: objectClass eq
olcDbIndex: cn,uid eq
olcDbIndex: uidNumber,gidNumber eq
olcDbIndex: member,memberUid eq
olcDbIndex: mail eq,sub
```

- Let's add a schema. It will first need to be converted to LDIF format. You can find unconverted schemas in addition to converted ones in the `/etc/ldap/schema` directory.

  - It is not trivial to remove a schema from the slapd-config database. Practice adding schemas on a test system.
  - Before adding any schema, you should check which schemas are already installed (shown is a default, out-of-the-box output):

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=schema,cn=config dn

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config
```

In the following example we'll add the CORBA schema.

1. Create the conversion configuration file `schema_convert.conf` 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/ldapns.schema
include /etc/ldap/schema/pmi.schema
```

2. Create the output directory `ldif_output`.
3. Determine the index of the schema:

```
slapcat -f schema_convert.conf -F ldif_output -n 0 | grep corba,cn=schema

cn={2}corba,cn=schema,cn=config
```

When slapd ingests objects with the same parent DN it will create an *index* for that object. An index is contained within braces: {X}.

4. Use slapcat to perform the conversion:

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H \
ldap:///cn={2}corba,cn=schema,cn=config -l cn=corba.ldif
```

The converted schema is now in `cn=corba.ldif`

5. Edit `cn=corba.ldif` to arrive at the following attributes:

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

Also remove the following lines from the bottom:

```
structuralObjectClass: olcSchemaConfig
entryUUID: 52109a02-66ab-1030-8be2-bbf166230478
creatorsName: cn=config
createTimestamp: 20110829165435Z
entryCSN: 20110829165435.935248Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20110829165435Z
```

Your attribute values will vary.

6. Finally, use ldapadd to add the new schema to the slapd-config DIT:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=corba.ldif

adding new entry "cn=corba,cn=schema,cn=config"
```

7. Confirm currently loaded schemas:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config dn

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: cn={4}corba,cn=schema,cn=config
```

For external applications and clients to authenticate using LDAP they will each need to be specifically configured to do so. Refer to the appropriate client-side documentation for details.

1.5. Logging

Activity logging for slapd is indispensible when implementing an OpenLDAP-based solution yet it must be manually enabled after software installation. Otherwise, only rudimentary messages will appear in the logs. Logging, like any other slapd configuration, is enabled via the slapd-config database.

OpenLDAP comes with multiple logging subsystems (levels) with each one containing the lower one (additive). A good level to try is *stats*. The *slapd-config*[3] man page has more to say on the different subsystems.

Create the file `logging.ldif` with the following contents:

```
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats
```

Implement the change:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f logging.ldif
```

This will produce a significant amount of logging and you will want to throttle back to a less verbose level once your system is in production. While in this verbose mode your host's syslog engine (rsyslog) may have a hard time keeping up and may drop messages:

```
rsyslogd-2177: imuxsock lost 228 messages from pid 2547 due to rate-limiting
```

You may consider a change to rsyslog's configuration. In `/etc/rsyslog.conf`, put:

```
# Disable rate limiting
# (default is 200 messages in 5 seconds; below we make the 5 become 0)
$SystemLogRateLimitInterval 0
```

And then restart the rsyslog daemon:

```
sudo systemctl restart syslog.service
```

1.6. Replication

The LDAP service becomes increasingly important as more networked systems begin to depend on it. In such an environment, it is standard practice to build redundancy (high availability) into LDAP to prevent havoc should the LDAP server become unresponsive. This is done through *LDAP replication.*

Replication is achieved via the *Syncrepl* engine. This allows changes to be synchronized using a *Consumer - Provider* model. The specific kind of replication we will implement in this guide is a combination of the

[3] http://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html

following modes: *refreshAndPersist* and *delta-syncrepl*. This has the Provider push changed entries to the Consumer as soon as they're made but, in addition, only actual changes will be sent, not entire entries.

1.6.1. Provider Configuration

Begin by configuring the *Provider*.

1. Create an LDIF file with the following contents and name it `provider_sync.ldif`:

```
# Add indexes to the frontend db.
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq

#Load the syncprov and accesslog modules.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov
-
add: olcModuleLoad
olcModuleLoad: accesslog

# Accesslog database definitions
dn: olcDatabase={2}mdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: {2}mdb
olcDbDirectory: /var/lib/ldap/accesslog
olcSuffix: cn=accesslog
olcRootDN: cn=admin,dc=example,dc=com
olcDbIndex: default eq
olcDbIndex: entryCSN,objectClass,reqEnd,reqResult,reqStart

# Accesslog db syncprov.
dn: olcOverlay=syncprov,olcDatabase={2}mdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE

# syncrepl Provider for primary db
dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
changetype: add
objectClass: olcOverlayConfig
```

```
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE

# accesslog overlay definitions for primary db
dn: olcOverlay=accesslog,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcAccessLogConfig
olcOverlay: accesslog
olcAccessLogDB: cn=accesslog
olcAccessLogOps: writes
olcAccessLogSuccess: TRUE
# scan the accesslog DB every day, and purge entries older than 7 days
olcAccessLogPurge: 07+00:00 01+00:00
```

Change the rootDN in the LDIF file to match the one you have for your directory.

2. Create a directory:

```
sudo -u openldap mkdir /var/lib/ldap/accesslog
```

3. Add the new content:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f provider_sync.ldif
```

The Provider is now configured.

1.6.2. Consumer Configuration

And now configure the *Consumer*.

1. Install the software by going through *Section 1.1, “Installation” [p. 113]*. Make sure the slapd-config database is identical to the Provider's. In particular, make sure schemas and the databse suffix are the same.
2. Create an LDIF file with the following contents and name it `consumer_sync.ldif`:

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

dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID eq
-
add: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://ldap01.example.com bindmethod=simple
 binddn="cn=admin,dc=example,dc=com"
  credentials=secret searchbase="dc=example,dc=com" logbase="cn=accesslog"
  logfilter="(&(objectClass=auditWriteObject)(reqResult=0))" schemachecking=on
```

```
  type=refreshAndPersist retry="60 +" syncdata=accesslog
-
add: olcUpdateRef
olcUpdateRef: ldap://ldap01.example.com
```

Ensure the following attributes have the correct values:

- *provider* (Provider server's hostname -- ldap01.example.com in this example -- or IP address)
- *binddn* (the admin DN you're using)
- *credentials* (the admin DN password you're using)
- *searchbase* (the database suffix you're using)
- *olcUpdateRef* (Provider server's hostname or IP address)
- *rid* (Replica ID, an unique 3-digit that identifies the replica. Each consumer should have at least one rid)

3. Add the new content:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f consumer_sync.ldif
```

You're done. The two databases (suffix: dc=example,dc=com) should now be synchronizing.

1.6.3. Testing

Once replication starts, you can monitor it by running

```
ldapsearch -z1 -LLLQY EXTERNAL -H ldapi:/// -s base -b dc=example,dc=com contextCSN

dn: dc=example,dc=com
contextCSN: 20120201193408.178454Z#000000#000#000000
```

on both the provider and the consumer. Once the output (`20120201193408.178454Z#000000#000#000000` in the above example) for both machines match, you have replication. Every time a change is done in the provider, this value will change and so should the one in the consumer(s).

If your connection is slow and/or your ldap database large, it might take a while for the consumer's *contextCSN* match the provider's. But, you will know it is progressing since the consumer's *contextCSN* will be steadly increasing.

If the consumer's *contextCSN* is missing or does not match the provider, you should stop and figure out the issue before continuing. Try checking the slapd (syslog) and the auth log files in the provider to see if the consumer's authentication requests were successful or its requests to retrieve data (they look like a lot of ldapsearch statements) return no errors.

To test if it worked simply query, on the Consumer, the DNs in the database:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b dc=example,dc=com dn
```

You should see the user 'john' and the group 'miners' as well as the nodes 'People' and 'Groups'.

1.7. Access Control

The management of what type of access (read, write, etc) users should be granted to resources is known as *access control*. The configuration directives involved are called *access control lists* or ACL.

When we installed the slapd package various ACL were set up automatically. We will look at a few important consequences of those defaults and, in so doing, we'll get an idea of how ACLs work and how they're configured.

To get the effective ACL for an LDAP query we need to look at the ACL entries of the database being queried as well as those of the special frontend database instance. The ACLs belonging to the latter act as defaults in case those of the former do not match. The frontend database is the second to be consulted and the ACL to be applied is the first to match ("first match wins") among these 2 ACL sources. The following commands will give, respectively, the ACLs of the mdb database ("dc=example,dc=com") and those of the frontend database:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={1}mdb)' olcAccess

dn: olcDatabase={1}mdb,cn=config
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to * by * read
```

The rootDN always has full rights to its database and does not need to be included in any ACL.

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={-1}frontend)' olcAccess

dn: olcDatabase={-1}frontend,cn=config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external
 ,cn=auth manage by * break
olcAccess: {1}to dn.exact="" by * read
olcAccess: {2}to dn.base="cn=Subschema" by * read
```

The very first two ACLs are crucial:

```
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
```

This can be represented differently for easier digestion:

```
to attrs=userPassword
```

```
 by self write
 by anonymous auth
 by * none

to attrs=shadowLastChange
 by self write
 by * read
```

These ACLs enforce the following:

- Anonymous 'auth' access is provided to the *userPassword* attribute so that users can authenticate, or *bind*. Perhaps counter-intuitively, 'by anonymous auth' is needed even when anonymous access to the DIT is unwanted, otherwise this would be a chicken and egg problem: before authentication, all users are anonymous.
- The *by self write* ACL grants write access to the *userPassword* attribute to users who authenticated as the *dn* where the attribute lives. In other words, users can update the *userPassword* attribute of their own entries.
- The *userPassword* attribute is otherwise unaccessible by all other users, with the exception of the rootDN, who always has access and doesn't need to be mentioned explicitly.
- In order for users to change their own password, using **passwd** or other utilities, the user's own *shadowLastChange* attribute needs to be writable. All other directory users get to read this attribute's contents.

This DIT can be searched anonymously because of 'to * by * read' in this ACL, which grants read access to everything else, by anyone (including anonymous):

```
to *
 by * read
```

If this is unwanted then you need to change the ACLs. To force authentication during a bind request you can alternatively (or in combination with the modified ACL) use the 'olcRequire: authc' directive.

As previously mentioned, there is no administrative account ("rootDN") created for the slapd-config database. There is, however, a SASL identity that is granted full access to it. It represents the localhost's superuser (root/sudo). Here it is:

```
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

The following command will display the ACLs of the slapd-config database:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={0}config)' olcAccess

dn: olcDatabase={0}config,cn=config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,
              cn=external,cn=auth manage by * break
```

Since this is a SASL identity we need to use a SASL *mechanism* when invoking the LDAP utility in question and we have seen it plenty of times in this guide. It is the EXTERNAL mechanism. See the previous command for an example. Note that:

1. You must use *sudo* to become the root identity in order for the ACL to match.
2. The EXTERNAL mechanism works via *IPC* (UNIX domain sockets). This means you must use the *ldapi* URI format.

A succinct way to get all the ACLs is like this:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcAccess=*)' olcAccess olcSuffix
```

There is much to say on the topic of access control. See the man page for *slapd.access*[4].

1.8. TLS

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).

Here, we will be our own *Certificate Authority* and then create and sign our LDAP server certificate as that CA. Since slapd is compiled using the gnutls library, we will use the certtool utility to complete these tasks.

1. Install the gnutls-bin and ssl-cert packages:

   ```
   sudo apt install gnutls-bin ssl-cert
   ```

2. Create a private key for the Certificate Authority:

   ```
   sudo sh -c "certtool --generate-privkey > /etc/ssl/private/cakey.pem"
   ```

3. Create the template/file `/etc/ssl/ca.info` to define the CA:

   ```
   cn = Example Company
   ca
   cert_signing_key
   ```

4. Create the self-signed CA certificate:

   ```
   sudo certtool --generate-self-signed \
   --load-privkey /etc/ssl/private/cakey.pem \
   --template /etc/ssl/ca.info \
   --outfile /etc/ssl/certs/cacert.pem
   ```

5. Make a private key for the server:

[4] http://manpages.ubuntu.com/manpages/en/man5/slapd.access.5.html

```
sudo certtool --generate-privkey \
--bits 1024 \
--outfile /etc/ssl/private/ldap01_slapd_key.pem
```

Replace *ldap01* in the filename with your server's hostname. Naming the certificate and key for the host and service that will be using them will help keep things clear.

6. Create the `/etc/ssl/ldap01.info` info file containing:

```
organization = Example Company
cn = ldap01.example.com
tls_www_server
encryption_key
signing_key
expiration_days = 3650
```

The above certificate is good for 10 years. Adjust accordingly.

7. Create the server's certificate:

```
sudo certtool --generate-certificate \
--load-privkey /etc/ssl/private/ldap01_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template /etc/ssl/ldap01.info \
--outfile /etc/ssl/certs/ldap01_slapd_cert.pem
```

8. Adjust permissions and ownership:

```
sudo chgrp openldap /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod 0640 /etc/ssl/private/ldap01_slapd_key.pem
sudo gpasswd -a openldap ssl-cert
```

9. Now restart slapd, since we added the 'openldap' user to the 'ssl-cert' group:

```
sudo systemctl restart slapd.service
```

Your server is now ready to accept the new TLS configuration.

Create the file `certinfo.ldif` with the following contents (adjust accordingly, our example assumes we created certs using https://www.cacert.org):

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap01_slapd_cert.pem
-
```

```
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap01_slapd_key.pem
```

Use the ldapmodify command to tell slapd about our TLS work via the slapd-config database:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f certinfo.ldif
```

Contratry to popular belief, you do not need *ldaps://* in `/etc/default/slapd` in order to use encryption. You should have just:

```
SLAPD_SERVICES="ldap:/// ldapi:///"
```

LDAP over TLS/SSL (ldaps://) is deprecated in favour of *StartTLS*. The latter refers to an existing LDAP session (listening on TCP port 389) becoming protected by TLS/SSL whereas LDAPS, like HTTPS, is a distinct encrypted-from-the-start protocol that operates over TCP port 636.

1.9. Replication and TLS

If you have set up replication between servers, it is common practice to encrypt (StartTLS) the replication traffic to prevent evesdropping. This is distinct from using encryption with authentication as we did above. In this section we will build on that TLS-authentication work.

The assumption here is that you have set up replication between Provider and Consumer according to *Section 1.6, “Replication” [p. 120]* and have configured TLS for authentication on the Provider by following *Section 1.8, “TLS” [p. 126]*.

As previously stated, the objective (for us) with replication is high availablity for the LDAP service. Since we have TLS for authentication on the Provider we will require the same on the Consumer. In addition to this, however, we want to encrypt replication traffic. What remains to be done is to create a key and certificate for the Consumer and then configure accordingly. We will generate the key/certificate on the Provider, to avoid having to create another CA certificate, and then transfer the necessary material over to the Consumer.

1. On the Provider,

   Create a holding directory (which will be used for the eventual transfer) and then the Consumer's private key:

   ```
   mkdir ldap02-ssl
   cd ldap02-ssl
   sudo certtool --generate-privkey \
   --bits 1024 \
   --outfile ldap02_slapd_key.pem
   ```

   Create an info file, `ldap02.info`, for the Consumer server, adjusting its values accordingly:

   ```
   organization = Example Company
   cn = ldap02.example.com
   ```

```
tls_www_server
encryption_key
signing_key
expiration_days = 3650
```

Create the Consumer's certificate:

```
sudo certtool --generate-certificate \
--load-privkey ldap02_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template ldap02.info \
--outfile ldap02_slapd_cert.pem
```

Get a copy of the CA certificate:

```
cp /etc/ssl/certs/cacert.pem .
```

We're done. Now transfer the `ldap02-ssl` directory to the Consumer. Here we use scp (adjust accordingly):

```
cd ..
scp -r ldap02-ssl user@consumer:
```

2. On the Consumer,

   Configure TLS authentication:

```
sudo apt install ssl-cert
sudo gpasswd -a openldap ssl-cert
sudo cp ldap02_slapd_cert.pem cacert.pem /etc/ssl/certs
sudo cp ldap02_slapd_key.pem /etc/ssl/private
sudo chgrp openldap /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod 0640 /etc/ssl/private/ldap02_slapd_key.pem
sudo systemctl restart slapd.service
```

   Create the file `/etc/ssl/certinfo.ldif` with the following contents (adjust accordingly):

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap02_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap02_slapd_key.pem
```

   Configure the slapd-config database:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f certinfo.ldif
```

Configure `/etc/default/slapd` as on the Provider (SLAPD_SERVICES).

3. On the Consumer,

   Configure TLS for Consumer-side replication. Modify the existing *olcSyncrepl* attribute by tacking on some TLS options. In so doing, we will see, for the first time, how to change an attribute's value(s).

   Create the file `consumer_sync_tls.ldif` with the following contents:

```
dn: olcDatabase={1}mdb,cn=config
replace: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://ldap01.example.com bindmethod=simple
 binddn="cn=admin,dc=example,dc=com" credentials=secret searchbase="dc=example,dc=com"
 logbase="cn=accesslog" logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
 schemachecking=on type=refreshAndPersist retry="60 +" syncdata=accesslog
 starttls=critical tls_reqcert=demand
```

   The extra options specify, respectively, that the consumer must use StartTLS and that the CA certificate is required to verify the Provider's identity. Also note the LDIF syntax for changing the values of an attribute ('replace').

   Implement these changes:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f consumer_sync_tls.ldif
```

   And restart slapd:

```
sudo systemctl restart slapd.service
```

4. On the Provider,

   Check to see that a TLS session has been established. In `/var/log/syslog`, providing you have 'conns'-level logging set up, you should see messages similar to:

```
slapd[3620]: conn=1047 fd=20 ACCEPT from IP=10.153.107.229:57922 (IP=0.0.0.0:389)
slapd[3620]: conn=1047 op=0 EXT oid=1.3.6.1.4.1.1466.20037
slapd[3620]: conn=1047 op=0 STARTTLS
slapd[3620]: conn=1047 op=0 RESULT oid= err=0 text=
slapd[3620]: conn=1047 fd=20 TLS established tls_ssf=128 ssf=128
slapd[3620]: conn=1047 op=1 BIND dn="cn=admin,dc=example,dc=com" method=128
slapd[3620]: conn=1047 op=1 BIND dn="cn=admin,dc=example,dc=com" mech=SIMPLE ssf=0
slapd[3620]: conn=1047 op=1 RESULT tag=97 err=0 text
```

1.10. LDAP Authentication

Once you have a working LDAP server, you will need to install libraries on the client that will know how and when to contact it. On Ubuntu, this has been traditionally accomplished by installing the libnss-ldap package. This package will bring in other tools that will assist you in the configuration step. Install this package now:

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

You will be prompted for details of your LDAP server. If you make a mistake you can try 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 configure the LDAP profile for NSS:

```
sudo auth-client-config -t nss -p lac_ldap
```

Configure the system to use LDAP for authentication:

```
sudo pam-auth-update
```

From the menu, choose LDAP and any other authentication mechanisms you need.

You should now be able to log in using LDAP-based credentials.

LDAP clients will need to refer to multiple servers if replication is in use. In `/etc/ldap.conf` you would have something like:

```
uri ldap://ldap01.example.com ldap://ldap02.example.com
```

The request will time out and the Consumer (ldap02) will attempt to be reached if the Provider (ldap01) becomes unresponsive.

If you are going to use LDAP to store Samba users you will need to configure the Samba server to authenticate using LDAP. See *Section 2, “Samba and LDAP” [p. 137]* for details.

An alternative to the libnss-ldap package is the libnss-ldapd package. This, however, will bring in the nscd package which is problably not wanted. Simply remove it afterwards.

1.11. User and Group Management

The ldap-utils package comes with enough utilities to manage the directory but the long string of options needed can make them a burden to use. The ldapscripts package contains wrapper scripts to these utilities that some people find easier to use.

Install the package:

```
sudo apt install ldapscripts
```

Then edit the file `/etc/ldapscripts/ldapscripts.conf` to arrive at something similar to the following:

```
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 rootDN 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 database's rootDN user.

The scripts are now ready to help manage your directory. Here are some examples of how to use them:

- 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:: e1NTSEF9eXFsTFcyWlhwWkF1eGUybVdFWHZKRzJVMjFTSG9vcHk=

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

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

- A nice 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 `/usr/share/doc/ldapscripts/examples` directory. Copy or rename the `ldapadduser.template.sample` file to `/etc/ldapscripts/ldapadduser.template`:

```
sudo cp /usr/share/doc/ldapscripts/examples/ldapadduser.template.sample \
/etc/ldapscripts/ldapadduser.template
```

Edit the new template to add the desired attributes. The following will create new users 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 *sn* attribute. This will make ldapadduser prompt you for its value.

There are utilities in the package that were not covered here. Here is a complete list:

ldaprenamemachine[5]
ldapadduser[6]
ldapdeleteuserfromgroup[7]
ldapfinger[8]
ldapid[9]
ldapgid[10]
ldapmodifyuser[11]
ldaprenameuser[12]
lsldap[13]
ldapaddusertogroup[14]
ldapsetpasswd[15]
ldapinit[16]
ldapaddgroup[17]
ldapdeletegroup[18]

[5] http://manpages.ubuntu.com/manpages/en/man1/ldaprenamemachine.1.html
[6] http://manpages.ubuntu.com/manpages/en/man1/ldapadduser.1.html
[7] http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuserfromgroup.1.html
[8] http://manpages.ubuntu.com/manpages/en/man1/ldapfinger.1.html
[9] http://manpages.ubuntu.com/manpages/en/man1/ldapid.1.html
[10] http://manpages.ubuntu.com/manpages/en/man1/ldapgid.1.html
[11] http://manpages.ubuntu.com/manpages/en/man1/ldapmodifyuser.1.html
[12] http://manpages.ubuntu.com/manpages/en/man1/ldaprenameuser.1.html
[13] http://manpages.ubuntu.com/manpages/en/man1/lsldap.1.html
[14] http://manpages.ubuntu.com/manpages/en/man1/ldapaddusertogroup.1.html
[15] http://manpages.ubuntu.com/manpages/en/man1/ldapsetpasswd.1.html
[16] http://manpages.ubuntu.com/manpages/en/man1/ldapinit.1.html
[17] http://manpages.ubuntu.com/manpages/en/man1/ldapaddgroup.1.html
[18] http://manpages.ubuntu.com/manpages/en/man1/ldapdeletegroup.1.html

ldapmodifygroup[19]
ldapdeletemachine[20]
ldaprenamegroup[21]
ldapaddmachine[22]
ldapmodifymachine[23]
ldapsetprimarygroup[24]
ldapdeleteuser[25]

1.12. Backup and Restore

Now we have ldap running just the way we want, it is time to ensure we can save all of our work and restore it as needed.

What we need is a way to backup the ldap database(s), specifically the backend (cn=config) and frontend (dc=example,dc=com). If we are going to backup those databases into, say, `/export/backup`, we could use slapcat as shown in the following script, called `/usr/local/bin/ldapbackup`:

```
#!/bin/bash

BACKUP_PATH=/export/backup
SLAPCAT=/usr/sbin/slapcat

nice ${SLAPCAT} -n 0 > ${BACKUP_PATH}/config.ldif
nice ${SLAPCAT} -n 1 > ${BACKUP_PATH}/example.com.ldif
nice ${SLAPCAT} -n 2 > ${BACKUP_PATH}/access.ldif
chmod 640 ${BACKUP_PATH}/*.ldif
```

These files are uncompressed text files containing everything in your ldap databases including the tree layout, usernames, and every password. So, you might want to consider making `/export/backup` an encrypted partition and even having the script encrypt those files as it creates them. Ideally you should do both, but that depends on your security requirements.

Then, it is just a matter of having a cron script to run this program as often as we feel comfortable with. For many, once a day suffices. For others, more often is required. Here is an example of a cron script called `/etc/cron.d/ldapbackup` that is run every night at 22:45h:

```
MAILTO=backup-emails@domain.com
45 22 * * *  root    /usr/local/bin/ldapbackup
```

Now the files are created, they should be copied to a backup server.

Assuming we did a fresh reinstall of ldap, the restore process could be something like this:

[19] http://manpages.ubuntu.com/manpages/en/man1/ldapmodifygroup.1.html
[20] http://manpages.ubuntu.com/manpages/en/man1/ldapdeletemachine.1.html
[21] http://manpages.ubuntu.com/manpages/en/man1/ldaprenamegroup.1.html
[22] http://manpages.ubuntu.com/manpages/en/man1/ldapaddmachine.1.html
[23] http://manpages.ubuntu.com/manpages/en/man1/ldapmodifymachine.1.html
[24] http://manpages.ubuntu.com/manpages/en/man1/ldapsetprimarygroup.1.html
[25] http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuser.1.html

```
sudo systemctl stop slapd.service
sudo mkdir /var/lib/ldap/accesslog
sudo slapadd -F /etc/ldap/slapd.d -n 0 -l /export/backup/config.ldif
sudo slapadd -F /etc/ldap/slapd.d -n 1 -l /export/backup/domain.com.ldif
sudo slapadd -F /etc/ldap/slapd.d -n 2 -l /export/backup/access.ldif
sudo chown -R openldap:openldap /etc/ldap/slapd.d/
sudo chown -R openldap:openldap /var/lib/ldap/
sudo systemctl start slapd.service
```

1.13. Resources

- The primary resource is the upstream documentation: *www.openldap.org*[26]
- There are many man pages that come with the slapd package. Here are some important ones, especially considering the material presented in this guide:

  slapd[27]
  slapd-config[28]
  slapd.access[29]
  slapo-syncprov[30]
- Other man pages:

  auth-client-config[31]
  pam-auth-update[32]
- Zytrax's *LDAP for Rocket Scientists*[33]; a less pedantic but comprehensive treatment of LDAP
- A Ubuntu community *OpenLDAP wiki*[34] page has a collection of notes
- O'Reilly's *LDAP System Administration*[35] (textbook; 2003)
- Packt's *Mastering OpenLDAP*[36] (textbook; 2007)

[26] http://www.openldap.org/
[27] http://manpages.ubuntu.com/manpages/en/man8/slapd.8.html
[28] http://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html
[29] http://manpages.ubuntu.com/manpages/en/man5/slapd.access.5.html
[30] http://manpages.ubuntu.com/manpages/en/man5/slapo-syncprov.5.html
[31] http://manpages.ubuntu.com/manpages/en/man8/auth-client-config.8.html
[32] http://manpages.ubuntu.com/manpages/en/man8/pam-auth-update.8.html
[33] http://www.zytrax.com/books/ldap/
[34] https://help.ubuntu.com/community/OpenLDAPServer
[35] http://www.oreilly.com/catalog/ldapsa/
[36] http://www.packtpub.com/OpenLDAP-Developers-Server-Open-Source-Linux/book

2. Samba and LDAP

This section covers the integration of Samba with LDAP. The Samba server's role will be that of a "standalone" server and the LDAP directory will provide the authentication layer in addition to containing the user, group, and machine account information that Samba requires in order to function (in any of its 3 possible roles). The pre-requisite is an OpenLDAP server configured with a directory that can accept authentication requests. See *Section 1, “OpenLDAP Server” [p. 112]* for details on fulfilling this requirement. Once this section is completed, you will need to decide what specifically you want Samba to do for you and then configure it accordingly.

This guide will assume that the LDAP and Samba services are running on the same server and therefore use SASL EXTERNAL authentication whenever changing something under *cn=config*. If that is not your scenario, you will have to run those ldap commands on the LDAP server.

2.1. Software Installation

There are two packages needed when integrating Samba with LDAP: samba and smbldap-tools.

Strictly speaking, the smbldap-tools package isn't needed, but unless you have some other way to manage the various Samba entities (users, groups, computers) in an LDAP context then you should install it.

Install these packages now:

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

2.2. LDAP Configuration

We will now configure the LDAP server so that it can accomodate Samba data. We will perform three tasks in this section:

1. Import a schema
2. Index some entries
3. Add objects

2.2.1. Samba schema

In order for OpenLDAP to be used as a backend for Samba, logically, the DIT will need to use attributes that can properly describe Samba data. Such attributes can be obtained by introducing a Samba LDAP schema. Let's do this now.

For more information on schemas and their installation see *Section 1.4, “Modifying the slapd Configuration Database” [p. 117]*.

1. The schema is found in the now-installed samba package and is already in the ldif format. We can import it with one simple command:

```
zcat /usr/share/doc/samba/examples/LDAP/samba.ldif.gz | sudo ldapadd -Q -Y EXTERNAL -H
 ldapi:///
```

2. To query and view this new schema:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config 'cn=*samba*'
```

2.2.2. Samba indices

Now that slapd knows about the Samba attributes, we can set up some indices based on them. Indexing entries is a way to improve performance when a client performs a filtered search on the DIT.

Create the file `samba_indices.ldif` with the following contents:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcDbIndex
olcDbIndex: objectClass eq
olcDbIndex: uidNumber,gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: uid,cn eq,sub
olcDbIndex: memberUid eq,sub
olcDbIndex: member,uniqueMember eq
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub,eq
```

Using the ldapmodify utility load the new indices:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f samba_indices.ldif
```

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

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H \
ldapi:/// -b cn=config olcDatabase={1}mdb olcDbIndex
```

2.2.3. Adding Samba LDAP objects

Next, configure the smbldap-tools package to match your environment. The package comes with a configuration helper script called smbldap-config. Before running it, though, you should decide on two important configuration settings in `/etc/samba/smb.conf`:

- *netbios name*: how this server will be known. The default value is derived from the server's hostname, but truncated at 15 characters.

- *workgroup*: the workgroup name for this server, or, if you later decide to make it a domain controller, this will be the domain.

It's important to make these choices now because smbldap-config will use them to generate the config that will be later stored in the LDAP directory. If you run smbldap-config now and later change these values in `/etc/samba/smb.conf` there will be an inconsistency.

Once you are happy with *netbios name* and *workgroup*, proceed to generat the smbldap-tools configuration by running the configuration script which will ask you some questions:

```
sudo smbldap-config
```

Some of the more important ones:

- *workgroup name*: has to match what you will configure in `/etc/samba/smb.conf` later on.
- *ldap suffix*: has to match the ldap suffix you chose when you configured the LDAP server.
- other ldap suffixes: they are all relative to *ldap suffix* above. For example, for *ldap user suffix* you should use *ou=People*.
- *ldap master bind dn* and *bind password*: use the rootDN credentials.

The smbldap-populate script will then add the LDAP objects required for Samba. It is a good idea to first make a backup of your DIT using slapcat:

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

Once you have a backup proceed to populate your directory. It will ask you for a password for the "domain root" user, which is also the "root" user stored in LDAP:

```
sudo smbldap-populate -g 10000 -u 10000 -r 10000
```

The *-g*, *-u* and *-r* parameters tell smbldap-tools where to start the numeric uid and gid allocation for the LDAP users. You should pick a range start that does not overlap with your local */etc/passwd* users.

You can create a 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. If it is, rerun the script without the '-e' switch. Alternatively, you can take the LDIF file and import its data per usual.

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

2.3. Samba Configuration

There are multiple ways to configure Samba. For details on some common configurations see *Chapter 18, Samba [p. 303]*. To configure Samba to use LDAP, edit its configuration file `/etc/samba/smb.conf` commenting out the default *passdb backend* parameter and adding some ldap-related ones. Make sure to use the same values you used when running smbldap-populate:

```
#  passdb backend = tdbsam
   workgroup = EXAMPLE

# LDAP Settings
   passdb backend = ldapsam:ldap://hostname
   ldap suffix = dc=example,dc=com
   ldap user suffix = ou=People
   ldap group suffix = ou=Groups
   ldap machine suffix = ou=Computers
   ldap idmap suffix = ou=Idmap
   ldap admin dn = cn=admin,dc=example,dc=com
   # or off if TLS/SSL is not configured
   ldap ssl = start tls
   ldap passwd sync = yes
```

Change the values to match your environment.

The `smb.conf` as shipped by the package is quite long and has many configuration examples. An easy way to visualize it without any comments is to run testparm -s.

Now inform Samba about the rootDN user's password (the one set during the installation of the slapd package):

```
sudo smbpasswd -W
```

As a final step to have your LDAP users be able to connect to samba and authenticate, we need these users to also show up in the system as "unix" users. One way to do this is to use libnss-ldap. Detailed instructions can be found in the *Section 1.10, “LDAP Authentication” [p. 131]* section, but we only need the NSS part.

1. Install libnss-ldap

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

   There is no need to use the LDAP rootDN login credentials, so you can skip that step.
2. Configure the LDAP profile for NSS:

   ```
   sudo auth-client-config -t nss -p lac_ldap
   ```
3. Restart the Samba services:

   ```
   sudo systemctl restart smbd.service nmbd.service
   ```
4. To quickly test the setup, see if getent can list the Samba groups:

   ```
   getent group

   ...
   Account Operators:*:548:
   Print Operators:*:550:
   Backup Operators:*:551:
   Replicators:*:552:
   ```

If you have existing LDAP users that you want to include in your new LDAP-backed Samba they will, of course, also need to be given some of the extra Samba specific attributes. The smbpasswd utility can do this for you:

```
sudo smbpasswd -a username
```

You will prompted to enter a password. It will be considered as the new password for that user. Making it the same as before is reasonable. Note that this command cannot be used to create a new user from scratch in LDAP (unless you are using *ldapsam:trusted* and *ldapsam:editposix*, not covered in this guide).

To manage user, group, and machine accounts use the utilities provided by the smbldap-tools package. Here are some examples:

- To add a new user with a home directory:

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

  The *-a* option adds the Samba attributes, and the *-P* option calls the smbldap-passwd utility after the user is created allowing you to enter a password for the user. Finally, *-m* creates a local home directory. Test with the getent command:

  ```
  getent passwd username
  ```

  If you don't get a response, then your libnss-ldap configuration is incorrect.
- To remove a user:

  ```
  sudo smbldap-userdel username
  ```

  In the above command, use the *-r* option to remove the user's home directory.
- To add a group:

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

  As for smbldap-useradd, the *-a* adds the Samba attributes.
- To make an existing user a member of a group:

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

  The *-m* option can add more than one user at a time by listing them in comma-separated format.
- To remove a user from a group:

  ```
  sudo smbldap-groupmod -x username groupname
  ```
- To add a Samba machine account:

```
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* parameter in `/etc/samba/smb.conf` was changed to use smbldap-useradd.

There are utilities in the smbldap-tools package that were not covered here. Here is a complete list:

smbldap-groupadd[37]
smbldap-groupdel[38]
smbldap-groupmod[39]
smbldap-groupshow[40]
smbldap-passwd[41]
smbldap-populate[42]
smbldap-useradd[43]
smbldap-userdel[44]
smbldap-userinfo[45]
smbldap-userlist[46]
smbldap-usermod[47]
smbldap-usershow[48]

2.4. Resources

- For more information on installing and configuring Samba see *Chapter 18, Samba [p. 303]* of this Ubuntu Server Guide.
- There are multiple places where LDAP and Samba is documented in the upstream *Samba HOWTO Collection*[49].
- Regarding the above, see specifically the *passdb section*[50].
- Although dated (2007), the *Linux Samba-OpenLDAP HOWTO*[51] contains valuable notes.
- The main page of the *Samba Ubuntu community documentation*[52] has a plethora of links to articles that may prove useful.

[37] http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupadd.8.html
[38] http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupdel.8.html
[39] http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupmod.8.html
[40] http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupshow.8.html
[41] http://manpages.ubuntu.com/manpages/en/man8/smbldap-passwd.8.html
[42] http://manpages.ubuntu.com/manpages/en/man8/smbldap-populate.8.html
[43] http://manpages.ubuntu.com/manpages/en/man8/smbldap-useradd.8.html
[44] http://manpages.ubuntu.com/manpages/en/man8/smbldap-userdel.8.html
[45] http://manpages.ubuntu.com/manpages/en/man8/smbldap-userinfo.8.html
[46] http://manpages.ubuntu.com/manpages/en/man8/smbldap-userlist.8.html
[47] http://manpages.ubuntu.com/manpages/en/man8/smbldap-usermod.8.html
[48] http://manpages.ubuntu.com/manpages/en/man8/smbldap-usershow.8.html
[49] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/
[50] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/passdb.html
[51] http://download.gna.org/smbldap-tools/docs/samba-ldap-howto/
[52] https://help.ubuntu.com/community/Samba#samba-ldap

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. Think of it as the domain or group your hosts and users belong to. Convention dictates the realm should be in uppercase. By default, ubuntu will use the DNS domain converted to uppercase (EXAMPLE.COM) as the realm.
- *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 more for redundancy, which contains a database of Principals. When a user principal logs into a workstation that is 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

For this discussion, we will create a MIT Kerberos domain with the following features (edit them to fit your needs):

- *Realm:* EXAMPLE.COM
- *Primary KDC:* kdc01.example.com (192.168.0.1)
- *Secondary KDC:* kdc02.example.com (192.168.0.2)
- *User principal:* steve
- *Admin principal:* steve/admin

It is *strongly* recommended that your network-authenticated users have their uid in a different range (say, starting at 5000) than that of your local users.

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. 166]* of the DNS documentation.

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 same *Network Time Protocol (NTP)* server. For details on setting up NTP see *Section 4, “Time Synchronisation” [p. 54]*.

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

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

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

By default the realm is created from the KDC's domain name.

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. If you need to reconfigure Kerberos from scratch, perhaps to change the realm name, you can do so by typing

```
sudo dpkg-reconfigure krb5-kdc
```

1. Once the KDC is properly running, an admin user -- the *admin principal* -- 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 above example *steve* is the *Principal*, */admin* is an *Instance*, and *@EXAMPLE.COM* signifies the realm. The *"every day"* Principal, a.k.a. the *user principal*, would be *steve@EXAMPLE.COM*, and should have only normal user rights.

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

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

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

This entry grants *steve/admin* the ability to perform any operation on all principals in the realm. You can configure principals with more restrictive privileges, which is convenient if you need an admin principal that junior staff can use in Kerberos clients. Please see the *kadm5.acl* man page for details.

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

```
sudo systemctl restart krb5-admin-server.service
```

4. 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
```

Where the cache filename `krb5cc_1000` is composed of the prefix `krb5cc_` and the user id (uid), which in this case is `1000`. You may need to add an entry into the `/etc/hosts` for the KDC so the client can find the KDC. For example:

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

Replacing *192.168.0.1* with the IP address of your KDC. This usually happens when you have a Kerberos realm encompassing different networks separated by routers.

5. The best way to allow clients to automatically determine the KDC for the Realm is using DNS SRV records. 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 8, Domain Name Service (DNS) [p. 163]* 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. Also, if you have Kerberos clients that are in different networks (possibly separated by routers using NAT), it is wise to place a secondary KDC in each of those networks.

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

```
sudo apt 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 -norandkey -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
```

The -k option indicates the file is a keytab file.

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

```
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/krb5.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 (note the long line has been split to fit the format of this document):

```
# m h  dom mon dow   command
0 * * * * /usr/sbin/kdb5_util dump /var/lib/krb5kdc/dump &&
/usr/sbin/kprop -r EXAMPLE.COM -f /var/lib/krb5kdc/dump kdc02.example.com
```

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 systemctl start krb5-kdc.service
```

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 by using kinit to request a ticket. If all goes well you should receive a ticket from the Secondary KDC. Otherwise, check `/var/log/syslog` and `/var/log/auth.log` in 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 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
        }
```

If you set the uid of each of your network-authenticated users to start at 5000, as suggested in *Section 3.2.1, “Installation” [p. 144]*, you can then tell pam to only try to authenticate using Kerberos users with uid > 5000:

```
# Kerberos should only be applied to ldap/kerberos users, not local ones.
for i in common-auth common-session common-account common-password; do
 sudo sed -i -r \
 -e 's/pam_krb5.so minimum_uid=1000/pam_krb5.so minimum_uid=5000/' \
 /etc/pam.d/$i
done
```

This will avoid being asked for the (non-existent) Kerberos password of a locally authenticated user when changing its password using **passwd**.

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 MIT's version of Kerberos, see the *MIT Kerberos*[53] site.
- The *Ubuntu Wiki Kerberos*[54] page has more details.
- O'Reilly's *Kerberos: The Definitive Guide*[55] is a great reference when setting up Kerberos.
- Also, feel free to stop by the *#ubuntu-server* and *#kerberos* IRC channels on *Freenode*[56] if you have Kerberos questions.

[53] http://web.mit.edu/Kerberos/
[54] https://help.ubuntu.com/community/Kerberos
[55] http://oreilly.com/catalog/9780596004033/
[56] http://freenode.net/

4. Kerberos and LDAP

Most people will not use Kerberos by itself; once an user is authenticated (Kerberos), we need to figure out what this user can do (authorization). And that would be the job of programs such as LDAP.

Replicating a Kerberos principal database between two servers can be complicated, and adds an additional user database to your network. Fortunately, MIT Kerberos can be configured to use an LDAP directory as a principal database. This section covers configuring a primary and secondary kerberos server to use OpenLDAP for the principal database.

The examples presented here assume MIT Kerberos and OpenLDAP.

4.1. Configuring OpenLDAP

First, the necessary *schema* needs to be loaded on an OpenLDAP server that has network connectivity to the Primary and Secondary KDCs. The rest of this section assumes that you also have LDAP replication configured between at least two servers. For information on setting up OpenLDAP see *Section 1, “OpenLDAP Server” [p. 112]*.

It is also required to configure OpenLDAP for TLS and SSL connections, so that traffic between the KDC and LDAP server is encrypted. See *Section 1.8, “TLS” [p. 126]* for details.

`cn=admin,cn=config` is a user we created with rights to edit the ldap database. Many times it is the RootDN. Change its value to reflect your setup.

- To load the schema into LDAP, on the LDAP server install the krb5-kdc-ldap package. From a terminal enter:

  ```
  sudo apt install krb5-kdc-ldap
  ```

- Next, extract the `kerberos.schema.gz` file:

  ```
  sudo gzip -d /usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz
  sudo cp /usr/share/doc/krb5-kdc-ldap/kerberos.schema /etc/ldap/schema/
  ```

- The *kerberos* schema needs to be added to the *cn=config* tree. The procedure to add a new schema to slapd is also detailed in *Section 1.4, “Modifying the slapd Configuration Database” [p. 117]*.

  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/kerberos.schema
```

2. Create a temporary directory to hold the LDIF files:

```
mkdir /tmp/ldif_output
```

3. Now use slapcat to convert the schema files:

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s \
"cn={12}kerberos,cn=schema,cn=config" > /tmp/cn=kerberos.ldif
```

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

4. Edit the generated `/tmp/cn\=kerberos.ldif` file, changing the following attributes:

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

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

```
structuralObjectClass: olcSchemaConfig
entryUUID: 18ccd010-746b-102d-9fbe-3760cca765dc
creatorsName: cn=config
createTimestamp: 20090111203515Z
entryCSN: 20090111203515.326445Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20090111203515Z
```

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

5. Load the new schema with ldapadd:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f /tmp/cn\=kerberos.ldif
```

6. Add an index for the *krb5principalname* attribute:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:///

dn: olcDatabase={1}mdb,cn=config
add: olcDbIndex
olcDbIndex: krbPrincipalName eq,pres,sub

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

7. Finally, update the Access Control Lists (ACL):

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:///

dn: olcDatabase={1}mdb,cn=config
replace: olcAccess
olcAccess: to attrs=userPassword,shadowLastChange,krbPrincipalKey by
 dn="cn=admin,dc=example,dc=com" write by anonymous auth by self write by * none
-
add: olcAccess
olcAccess: to dn.base="" by * read
-
add: olcAccess
olcAccess: to * by dn="cn=admin,dc=example,dc=com" write by * read

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

That's it, your LDAP directory is now ready to serve as a Kerberos principal database.

4.2. Primary KDC Configuration

With OpenLDAP configured it is time to configure the KDC.

- First, install the necessary packages, from a terminal enter:

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

- Now edit `/etc/krb5.conf` adding the following options to under the appropriate sections:

```
[libdefaults]
        default_realm = EXAMPLE.COM

...

[realms]
        EXAMPLE.COM = {
                kdc = kdc01.example.com
                kdc = kdc02.example.com
                admin_server = kdc01.example.com
                admin_server = kdc02.example.com
                default_domain = example.com
                database_module = openldap_ldapconf
        }

...

[domain_realm]
        .example.com = EXAMPLE.COM
```

```
...

[dbdefaults]
        ldap_kerberos_container_dn = cn=krbContainer,dc=example,dc=com

[dbmodules]
        openldap_ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read rights on
                # the realm container, principal container and realm sub-trees
                ldap_kadmind_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read and write rights on
                # the realm container, principal container and realm sub-trees
                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldaps://ldap01.example.com ldaps://ldap02.example.com
                ldap_conns_per_server = 5
        }
```

Change *example.com*, *dc=example,dc=com*, *cn=admin,dc=example,dc=com*, and *ldap01.example.com* to the appropriate domain, LDAP object, and LDAP server for your network.

- Next, use the kdb5_ldap_util utility to create the realm:

```
sudo kdb5_ldap_util -D  cn=admin,dc=example,dc=com create -subtrees \
dc=example,dc=com -r EXAMPLE.COM -s -H ldap://ldap01.example.com
```

- Create a stash of the password used to bind to the LDAP server. This password is used by the *ldap_kdc_dn* and *ldap_kadmin_dn* options in `/etc/krb5.conf`:

```
sudo kdb5_ldap_util -D  cn=admin,dc=example,dc=com stashsrvpw -f \
/etc/krb5kdc/service.keyfile cn=admin,dc=example,dc=com
```

- Copy the CA certificate from the LDAP server:

```
scp ldap01:/etc/ssl/certs/cacert.pem .
sudo cp cacert.pem /etc/ssl/certs
```

And edit `/etc/ldap/ldap.conf` to use the certificate:

```
TLS_CACERT /etc/ssl/certs/cacert.pem
```

The certificate will also need to be copied to the Secondary KDC, to allow the connection to the LDAP servers using LDAPS.

- Start the Kerberos KDC and admin server:

```
sudo systemctl start krb5-kdc.service
```

```
sudo systemctl start krb5-admin-server.service
```

You can now add Kerberos principals to the LDAP database, and they will be copied to any other LDAP servers configured for replication. To add a principal using the kadmin.local utility enter:

```
sudo kadmin.local
Authenticating as principal root/admin@EXAMPLE.COM with password.
kadmin.local:  addprinc -x dn="uid=steve,ou=people,dc=example,dc=com" steve
WARNING: no policy specified for steve@EXAMPLE.COM; defaulting to no policy
Enter password for principal "steve@EXAMPLE.COM":
Re-enter password for principal "steve@EXAMPLE.COM":
Principal "steve@EXAMPLE.COM" created.
```

There should now be krbPrincipalName, krbPrincipalKey, krbLastPwdChange, and krbExtraData attributes added to the *uid=steve,ou=people,dc=example,dc=com* user object. Use the kinit and klist utilities to test that the user is indeed issued a ticket.

If the user object is already created the *-x dn="..."* option is needed to add the Kerberos attributes. Otherwise a new *principal* object will be created in the realm subtree.

4.3. Secondary KDC Configuration

Configuring a Secondary KDC using the LDAP backend is similar to configuring one using the normal Kerberos database.

1. First, install the necessary packages. In a terminal enter:

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

2. Next, edit `/etc/krb5.conf` to use the LDAP backend:

   ```
   [libdefaults]
           default_realm = EXAMPLE.COM

   ...

   [realms]
           EXAMPLE.COM = {
                   kdc = kdc01.example.com
                   kdc = kdc02.example.com
                   admin_server = kdc01.example.com
                   admin_server = kdc02.example.com
                   default_domain = example.com
                   database_module = openldap_ldapconf
           }

   ...
   ```

```
[domain_realm]
        .example.com = EXAMPLE.COM

...

[dbdefaults]
        ldap_kerberos_container_dn = dc=example,dc=com

[dbmodules]
        openldap_ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read rights on
                # the realm container, principal container and realm sub-trees
                ldap_kadmind_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read and write rights on
                # the realm container, principal container and realm sub-trees
                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldaps://ldap01.example.com ldaps://ldap02.example.com
                ldap_conns_per_server = 5
        }
```

3. Create the stash for the LDAP bind password:

```
sudo kdb5_ldap_util -D  cn=admin,dc=example,dc=com stashsrvpw -f \
/etc/krb5kdc/service.keyfile cn=admin,dc=example,dc=com
```

4. Now, on the *Primary KDC* copy the `/etc/krb5kdc/.k5.EXAMPLE.COM` *Master Key* stash to the Secondary KDC. Be sure to copy the file over an encrypted connection such as scp, or on physical media.

```
sudo scp /etc/krb5kdc/.k5.EXAMPLE.COM steve@kdc02.example.com:~
sudo mv .k5.EXAMPLE.COM /etc/krb5kdc/
```

Again, replace *EXAMPLE.COM* with your actual realm.

5. Back on the *Secondary KDC*, (re)start the ldap server only,

```
sudo systemctl restart slapd.service
```

6. Finally, start the krb5-kdc daemon:

```
sudo systemctl start krb5-kdc.service
```

7. Verify the two ldap servers (and kerberos by extension) are in sync.

You now have redundant KDCs on your network, and with redundant LDAP servers you should be able to continue to authenticate users if one LDAP server, one Kerberos server, or one LDAP and one Kerberos server become unavailable.

4.4. Resources

- The *Kerberos Admin Guide*[57] has some additional details.
- For more information on kdb5_ldap_util see *Section 5.6*[58] and the *kdb5_ldap_util man page*[59].
- Another useful link is the *krb5.conf man page*[60].
- Also, see the *Kerberos and LDAP*[61] Ubuntu wiki page.

[57] http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Configuring-Kerberos-with-OpenLDAP-back_002dend
[58] http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Global-Operations-on-the-Kerberos-LDAP-Database
[59] http://manpages.ubuntu.com/manpages/xenial/en/man8/kdb5_ldap_util.8.html
[60] http://manpages.ubuntu.com/manpages/xenial/en/man5/krb5.conf.5.html
[61] https://help.ubuntu.com/community/Kerberos#kerberos-ldap

5. SSSD and Active Directory

This section describes the use of sssd to authenticate user logins against an Active Directory via using sssd's "ad" provider. In previous versions of sssd, it was possible to authenticate using the "ldap" provider. However, when authenticating against a Microsoft Windows AD Domain Controller, it was generally necessary to install the POSIX AD extensions on the Domain Controller. The "ad" provider simplifies the configuration and requires no modifications to the AD structure.

5.1. Prerequisites, Assumptions, and Requirements

- This guide does not explain Active Directory, how it works, how to set one up, or how to maintain it. It may not provide “best practices” for your environment.
- This guide assumes that a working Active Directory domain is already configured.
- The domain controller is acting as an authoritative DNS server for the domain.
- The domain controller is the primary DNS resolver as specified in `/etc/resolv.conf`.
- The appropriate *_kerberos*, *_ldap*, *_kpasswd*, etc. entries are configured in the DNS zone (see Resources section for external links).
- System time is synchronized on the domain controller (necessary for Kerberos).
- The domain used in this example is *myubuntu.example.com* .

5.2. Software Installation

The following packages are needed: *krb5-user*, *samba*, *sssd*, and *ntp*. Samba needs to be installed, even if the system is not exporting shares. The Kerberos realm and FQDN or IP of the domain controllers are needed for this step.

Install these packages now.

```
sudo apt install krb5-user samba sssd ntp
```

See the next section for the answers to the questions asked by the *krb5-user* postinstall script.

5.3. Kerberos Configuration

The installation of *krb5-user* will prompt for the realm name (in ALL UPPERCASE), the kdc server (i.e. domain controller) and admin server (also the domain controller in this example.) This will write the [realm] and [domain_realm] sections in `/etc/krb5.conf`. These sections may not be necessary if domain autodiscovery is working. If not, then both are needed.

If the domain is *myubuntu.example.com*, enter the realm as *MYUBUNTU.EXAMPLE.COM*

Optionally, edit */etc/krb5.conf* with a few additional settings to specify Kerberos ticket lifetime (these values are safe to use as defaults):

```
[libdefaults]

default_realm = MYUBUNTU.EXAMPLE.COM
ticket_lifetime = 24h #
renew_lifetime = 7d
```

If default_realm is not specified, it may be necessary to log in with “username@domain” instead of “username”.

The system time on the Active Directory member needs to be consistent with that of the domain controller, or Kerberos authentication may fail. Ideally, the domain controller server itself will provide the NTP service. Edit `/etc/ntp.conf`:

```
server dc.myubuntu.example.com
```

5.4. Samba Configuration

Samba will be used to perform netbios/nmbd services related to Active Directory authentication, even if no file shares are exported. Edit the file /etc/samba/smb.conf and add the following to the *[global]* section:

```
[global]

workgroup = MYUBUNTU
client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
realm = MYUBUNTU.EXAMPLE.COM
security = ads
```

Some guides specify that "password server" should be specified and pointed to the domain controller. This is only necessary if DNS is not properly set up to find the DC. By default, Samba will display a warning if "password server" is specified with "security = ads".

5.5. SSSD Configuration

There is no default/example config file for `/etc/sssd/sssd.conf` included in the sssd package. It is necessary to create one. This is a minimal working config file:

```
[sssd]
services = nss, pam
config_file_version = 2
domains = MYUBUNTU.EXAMPLE.COM

[domain/MYUBUNTU.EXAMPLE.COM]
id_provider = ad
access_provider = ad
```

```
# Use this if users are being logged in at /.
# This example specifies /home/DOMAIN-FQDN/user as $HOME.  Use with pam_mkhomedir.so
override_homedir = /home/%d/%u

# Uncomment if the client machine hostname doesn't match the computer object on the DC.
# ad_hostname = mymachine.myubuntu.example.com

# Uncomment if DNS SRV resolution is not working
# ad_server = dc.mydomain.example.com

# Uncomment if the AD domain is named differently than the Samba domain
# ad_domain = MYUBUNTU.EXAMPLE.COM

# Enumeration is discouraged for performance reasons.
# enumerate = true
```

After saving this file, set the ownership to root and the file permissions to 600:

```
sudo chown root:root /etc/sssd/sssd.conf
```

```
sudo chmod 600 /etc/sssd/sssd.conf
```

If the ownership or permissions are not correct, sssd will refuse to start.

5.6. Verify nsswitch.conf Configuration

The post-install script for the sssd package makes some modifications to /etc/nsswitch.conf automatically. It should look something like this:

```
passwd:         compat sss
group:          compat sss
...
netgroup:       nis sss
sudoers:        files sss
```

5.7. Modify /etc/hosts

Add an alias to the localhost entry in /etc/hosts specifying the FQDN. For example:

```
192.168.1.10 myserver myserver.myubuntu.example.com
```

This is useful in conjunction with dynamic DNS updates.

5.8. Join the Active Directory

Now, restart ntp and samba and start sssd.

```
sudo systemctl restart ntp.service
sudo systemctl restart smbd.service nmbd.service
sudo systemctl start sssd.service
```

Test the configuration by obtaining a Kerberos ticket:

```
sudo kinit Administrator
```

Verify the ticket with:

```
sudo klist
```

If there is a ticket with an expiration date listed, then it is time to join the domain:

```
sudo net ads join -k
```

A warning about "No DNS domain configured. Unable to perform DNS Update." probably means that there is no (correct) alias in `/etc/hosts`, and the system could not provide its own FQDN as part of the Active Directory update. This is needed for dynamic DNS updates. Verify the alias in `/etc/hosts` described in "Modify /etc/hosts" above.

(The message "NT_STATUS_UNSUCCESSFUL" indicates the domain join failed and something is incorrect. Review the prior steps before proceeding).

Here are a couple of (optional) checks to verify that the domain join was successful. Note that if the domain was successfully joined but one or both of these steps fail, it may be necessary to wait 1-2 minutes and try again. Some of the changes appear to be asynchronous.

Verification option #1:

Check the default Organizational Unit for computer accounts in the Active Directory to verify that the computer account was created. (Organizational Units in Active Directory is a topic outside the scope of this guide).

Verification option #2

Execute this command for a specific AD user (e.g. administrator)

```
getent passwd username
```

If *enumerate = true* is set in `sssd.conf`, *getent passwd* with no username argument will list all domain users. This may be useful for testing, but is slow and not recommended for production.

5.9. Test Authentication

It should now be possible to authenticate using an Active Directory User's credentials:

```
su - username
```

If this works, then other login methods (getty, ssh) should also work.

If the computer account was created, indicating that the system was "joined" to the domain, but authentication is unsuccessful, it may be helpful to review `/etc/pam.d` and `nssswitch.conf` as well as the file changes described earlier in this guide.

5.10. Home directories with pam_mkhomedir (optional)

When logging in using an Active Directory user account, it is likely that user has no home directory. This can be fixed with pam_mkdhomedir.so, which will create the user's home directory on login. Edit `/etc/pam.d/common-session`, and add this line directly after *session required pam_unix.so:*

```
session    required    pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

This may also need *override_homedir* in `sssd.conf` to function correctly, so make sure that's set.

5.11. Desktop Ubuntu Authentication

It is possible to also authenticate logins to Ubuntu Desktop using Active Directory accounts. The AD accounts will not show up in the pick list with local users, so lightdm will need to be modified. Edit the file `/etc/lightdm/lightdm.conf.d/50-unity-greeter.conf` and append the following two lines:

```
greeter-show-manual-login=true
greeter-hide-users=true
```

Reboot to restart lightdm. It should now be possible to log in using a domain account using either *username* or *username/username@domain* format.

5.12. Resources

- *SSSD Project*[62]
- *DNS Server Configuration guidelines*[63]
- *Active Directory DNS Zone Entries*[64]
- *Kerberos config options*[65]

[62] https://fedorahosted.org/sssd
[63] http://www.ucs.cam.ac.uk/support/windows-support/winsuptech/activedir/dnsconfig
[64] https://technet.microsoft.com/en-us/library/cc759550%28v=ws.10%29.aspx
[65] http://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html

Chapter 8. Domain Name Service (DNS)

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

1. Installation

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

```
sudo apt install bind9
```

A very useful package for testing and troubleshooting DNS issues is the dnsutils package. Very often these tools will be installed already, but to check and/or install dnsutils enter the following:

```
sudo apt install dnsutils
```

2. Configuration

There are many ways to configure BIND9. Some of the most common configurations are 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 it's 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 Adresses of actual nameservers.

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

```
sudo systemctl restart bind9.service
```

See *Section 3.1.2, “dig” [p. 171]* 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";
};
```

(Note, if bind will be receiving automatic updates to the file as with DDNS, then use `/var/lib/bind/db.example.com` rather than `/etc/bind/db.example.com` both here and in the copy command below.)

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. Change the comment to indicate the domain that this file is for.

Create an *A record* for the base domain, *example.com*. Also, create an *A record* for *ns.example.com*, the name server in this example:

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

```
@       IN      AAAA    ::1
ns      IN      A       192.168.1.10
```

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. 175]* for details.

Many admins like to use the last date edited as the serial of a zone, such as *2012010100* which is yyyymmddss (where *ss* is the Serial Number)

Once you have made changes to the zone file BIND9 needs to be restarted for the changes to take effect:

```
sudo systemctl restart bind9.service
```

2.3.2. Reverse Zone File

Now that the zone is setup and resolving names to IP Adresses 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;
        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 192.168.1.XXX net
;
$TTL    604800
@       IN      SOA     ns.example.com. root.example.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
```

```
@       IN      NS      ns.
10      IN      PTR     ns.example.com.
```

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

After creating the reverse zone file restart BIND9:

```
sudo systemctl restart bind9.service
```

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;
        file "/etc/bind/db.192";
 allow-transfer { 192.168.1.11; };
};
```

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

Restart BIND9 on the Primary Master:

```
sudo systemctl restart bind9.service
```

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 systemctl restart bind9.service
```

In `/var/log/syslog` you should see something similar to (some lines have been split to fit the format of this document):

```
client 192.168.1.10#39448: received notify for zone '1.168.192.in-addr.arpa'
zone 1.168.192.in-addr.arpa/IN: Transfer started.
transfer of '100.18.172.in-addr.arpa/IN' from 192.168.1.10#53:
 connected using 192.168.1.11#37531
zone 1.168.192.in-addr.arpa/IN: transferred serial 5
transfer of '100.18.172.in-addr.arpa/IN' from 192.168.1.10#53:
 Transfer completed: 1 messages,
6 records, 212 bytes, 0.002 secs (106000 bytes/sec)
zone 1.168.192.in-addr.arpa/IN: sending notifies (serial 5)

client 192.168.1.10#20329: received notify for zone 'example.com'
zone example.com/IN: Transfer started.
transfer of 'example.com/IN' from 192.168.1.10#53: connected using 192.168.1.11#38577
zone example.com/IN: transferred serial 5
transfer of 'example.com/IN' from 192.168.1.10#53: Transfer completed: 1 messages,
8 records, 225 bytes, 0.002 secs (112500 bytes/sec)
```

Note: A zone is only transferred if the *Serial Number* on the Primary is larger than the one on the Secondary. If you want to have your Primary Master DNS notifying Secondary DNS Servers of zone changes, you can add *also-notify { ipaddress; };* in to `/etc/bind/named.conf.local` as shown in the example below:

```
zone "example.com" {
 type master;
 file "/etc/bind/db.example.com";
 allow-transfer { 192.168.1.11; };
 also-notify { 192.168.1.11; };
 };

zone "1.168.192.in-addr.arpa" {
 type master;
 file "/etc/bind/db.192";
 allow-transfer { 192.168.1.11; };
 also-notify { 192.168.1.11; };
```

```
};
```

The default directory for non-authoritative zone files is `/var/cache/bind/`. This directory is also configured in AppArmor to allow the named daemon to write to it. For more information on AppArmor see *Section 4, “AppArmor” [p. 191]*.

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. Refer to *Section 1.3.1, “DNS Client Configuration” [p. 42]* for details on adding nameserver addresses to your network clients, and afterwards check that the file `/etc/resolv.conf` contains (for this example):

```
nameserver 192.168.1.10
nameserver 192.168.1.11
```

Nameservers that listen at 127.* are responsible for adding their own IP addresses to resolv.conf (using resolvconf). This is done via the file `/etc/default/bind9` by changing the line RESOLVCONF=no to RESOLVCONF=yes.

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

3.1.2. 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
```

3.1.3. ping

Now to demonstrate how applications make use of DNS to resolve a host name use the ping utility to send an ICMP echo request. From a terminal prompt enter:

```
ping example.com
```

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

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

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 1.168.192.in-addr.arpa /etc/bind/db.192
  ```

  The output should be similar to:

  ```
  zone 1.168.192.in-addr.arpa/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. 191]*

- Now restart BIND9 for the changes to take effect:

```
sudo systemctl restart bind9.service
```

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. 175]*.

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  1   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 *BIND9 Server HOWTO*[1] in the Ubuntu Wiki has a lot of useful information.
- The *DNS HOWTO*[2] at The Linux Documentation Project also has lots of information about configuring BIND9.
- *Bind9.net*[3] has links to a large collection of DNS and BIND9 resources.
- *DNS and BIND*[4] is a popular book now in it's fifth edition. There is now also a *DNS and BIND on IPv6*[5] book.
- A great place to ask for BIND9 assistance, and get involved with the Ubuntu Server community, is the *#ubuntu-server* IRC channel on *freenode*[6].

[1] https://help.ubuntu.com/community/BIND9ServerHowto
[2] http://www.tldp.org/HOWTO/DNS-HOWTO.html
[3] http://www.bind9.net/
[4] http://shop.oreilly.com/product/9780596100575.do
[5] http://shop.oreilly.com/product/0636920020158.do
[6] http://freenode.net

Chapter 9. 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 system's 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 16.04 LTS 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:

  

  Configurations with root passwords are not supported.

  ```
  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 password, use the following passwd syntax:

  ```
  sudo passwd -l root
  ```

  However, to disable the root account itself, use the following command:

  ```
  usermod --expiredate 1
  ```

- You should read more on Sudo by reading the man page:

  ```
  man sudo
  ```

By default, the initial user created by the Ubuntu installer is a member of the group "*sudo*" 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 *sudo* group.

1.2. Adding and Deleting Users

The process for managing local users and groups is straightforward 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`. 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 user 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 6 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        [success=1 default=ignore]      pam_unix.so obscure sha512
```

If you would like to adjust the minimum length to 8 characters, change the appropriate variable to min=8. The modification is outlined below.

```
password        [success=1 default=ignore]      pam_unix.so obscure sha512 minlen=8
```

Basic password entropy checks and minimum length rules do not apply to the administrator using sudo level commands to setup a new user.

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, 2015
  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 01/31/2015, 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 01/31/2015 -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, 2015
Password expires                                        : Apr 19, 2015
Password inactive                                       : May 19, 2015
Account expires                                         : Jan 31, 2015
Minimum number of days between password change          : 5
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 14
```

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.

```
who | grep username  (to get the pts/# terminal)
sudo pkill -f pts/#
```

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 systemctl restart sshd.service
```

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

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. While someone could simply unplug the power source, 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, run the following two commands:

```
sudo systemctl mask ctrl-alt-del.target
sudo systemctl daemon-reload
```

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
```

- Rules can also be added using a *numbered* format:

```
sudo ufw insert 1 allow 80
```

- 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
```

- To view the *numbered* format:

```
sudo ufw status numbered
```

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 app 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.

```
ubuntu-bug nameofpackage
```

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 back-end 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.

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 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 (single line split into 3 to fit this document):

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00
SRC=127.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=58288 DF PROTO=TCP
SPT=53981 DPT=80 WINDOW=32767 RES=0x00 SYN URGP=0
```

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 logwatch, 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:

- *fwbuilder*[1] 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*[2] is a very powerful solution to help you configure an advanced firewall for any network.

3.6. References

- The *Ubuntu Firewall*[3] 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*[4] for more information on using iptables.
- The *nat-HOWTO*[5] contains further details on masquerading.
- The *IPTables HowTo*[6] in the Ubuntu wiki is a great resource.

[1] http://www.fwbuilder.org/
[2] http://www.shorewall.net/
[3] https://wiki.ubuntu.com/UncomplicatedFirewall
[4] http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html
[5] http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO.html
[6] https://help.ubuntu.com/community/IptablesHowTo

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 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

This section is plagued by a bug (*LP #1304134*[7]) and instructions will not work as advertised.

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/*
  ```

[7] https://bugs.launchpad.net/ubuntu/+source/apparmor/+bug/1304134

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
```

- `systemctl` can be used to *reload* all profiles:

```
sudo systemctl reload apparmor.service
```

- 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 systemctl stop apparmor.service
sudo update-rc.d -f apparmor remove
```

- To re-enable AppArmor enter:

```
sudo systemctl start apparmor.service
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:* 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. 191]* 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*[8] 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*[9] for advanced configuration options.
- For details using AppArmor with other Ubuntu releases see the *AppArmor Community Wiki*[10] page.
- The *OpenSUSE AppArmor*[11] 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*[12].

[8] https://bugs.launchpad.net/ubuntu/+source/apparmor/+filebug

[9] http://www.novell.com/documentation/apparmor/apparmor201_sp10_admin/index.html?page=/documentation/apparmor/apparmor201_sp10_admin/data/book_apparmor_admin.html

[10] https://help.ubuntu.com/community/AppArmor

[11] http://en.opensuse.org/SDB:AppArmor_geeks

[12] http://freenode.net

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. One 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.

If the certificate will be used by service daemons, such as Apache, Postfix, Dovecot, etc., a key without a passphrase is often appropriate. Not having a passphrase allows the services to start without manual intervention, usually the preferred way to start a daemon.

This section will cover generating a key with a passphrase, and one without. The non-passphrase key will then be used to generate a certificate that can be used with various service daemons.

Running your secure service without a passphrase is convenient because you will not need to enter the passphrase every time you start your secure service. But it is insecure and a compromise of the key means a compromise of the server as well.

To generate the *keys* for the Certificate Signing Request (CSR) run the following command from a terminal prompt:

```
openssl genrsa -des3 -out server.key 2048
```

```
Generating RSA private key, 2048 bit long modulus
.........................++++++
.......++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

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.

Now create the insecure key, the one without a passphrase, and shuffle the key names:

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

The insecure key is now named `server.key`, and you can use this file to generate the CSR without passphrase.

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

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

It will prompt you enter the passphrase. If you enter the correct passphrase, it will prompt you to enter Company Name, Site Name, Email Id, etc. Once you enter all these details, your CSR will be created and it will be stored in the `server.csr` file.

You can 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
```

2. 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
```

3. 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
```

4. 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.

5. Now install the root certificate and key:

```
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
```

6. 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. 196]* 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.

7. There should now be a new file, `/etc/ssl/newcerts/01.pem`, containing the same output. Copy and paste everything beginning with the line: -----*BEGIN CERTIFICATE*----- and continuing through the line: ----*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*[13] by tldp.org:
- The Wikipedia *HTTPS*[14] page has more information regarding HTTPS.
- For more information on *OpenSSL* see the *OpenSSL Home Page*[15].
- Also, O'Reilly's *Network Security with OpenSSL*[16] is a good in-depth reference.

[13] http://tldp.org/HOWTO/SSL-Certificates-HOWTO/index.html
[14] http://en.wikipedia.org/wiki/HTTPS
[15] http://www.openssl.org/
[16] http://oreilly.com/catalog/9780596002701/

6. eCryptfs

eCryptfs is a POSIX-compliant enterprise-class stacked cryptographic filesystem for Linux. Layering on top of the filesystem layer *eCryptfs* protects files no matter the underlying filesystem, partition type, etc.

During installation there is an option to encrypt the `/home` partition. This will automatically configure everything needed to encrypt and mount the partition.

As an example, this section will cover configuring `/srv` to be encrypted using *eCryptfs*.

6.1. Using eCryptfs

First, install the necessary packages. From a terminal prompt enter:

```
sudo apt install ecryptfs-utils
```

Now mount the partition to be encrypted:

```
sudo mount -t ecryptfs /srv /srv
```

You will then be prompted for some details on how ecryptfs should encrypt the data.

To test that files placed in `/srv` are indeed encrypted copy the `/etc/default` folder to `/srv`:

```
sudo cp -r /etc/default /srv
```

Now unmount `/srv`, and try to view a file:

```
sudo umount /srv
cat /srv/default/cron
```

Remounting `/srv` using ecryptfs will make the data viewable once again.

6.2. Automatically Mounting Encrypted Partitions

There are a couple of ways to automatically mount an ecryptfs encrypted filesystem at boot. This example will use a `/root/.ecryptfsrc` file containing mount options, along with a passphrase file residing on a USB key.

First, create `/root/.ecryptfsrc` containing:

```
key=passphrase:passphrase_passwd_file=/mnt/usb/passwd_file.txt
ecryptfs_sig=5826dd62cf81c615
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
ecryptfs_passthrough=n
ecryptfs_enable_filename_crypto=n
```

Adjust the *ecryptfs_sig* to the signature in `/root/.ecryptfs/sig-cache.txt`.

Next, create the `/mnt/usb/passwd_file.txt` passphrase file:

```
passphrase_passwd=[secrets]
```

Now add the necessary lines to `/etc/fstab`:

```
/dev/sdb1       /mnt/usb        ext3    ro      0 0
/srv /srv ecryptfs defaults 0 0
```

Make sure the USB drive is mounted before the encrypted partition.

Finally, reboot and the `/srv` should be mounted using *eCryptfs*.

6.3. Other Utilities

The ecryptfs-utils package includes several other useful utilities:

- *ecryptfs-setup-private:* creates a `~/Private` directory to contain encrypted information. This utility can be run by unprivileged users to keep data private from other users on the system.
- *ecryptfs-mount-private* and *ecryptfs-umount-private* will mount and unmount a user's `~/Private` directory.
- *ecryptfs-add-passphrase:* adds a new passphrase to the kernel keyring.
- *ecryptfs-manager:* manages eCryptfs objects such as keys.
- *ecryptfs-stat:* allows you to view the ecryptfs meta information for a file.

6.4. References

- For more information on *eCryptfs* see the *Launchpad project page*[17].
- There is also a *Linux Journal*[18] article covering *eCryptfs*.
- Also, for more ecryptfs options and details see the *ecryptfs man page*[19].

[17] https://launchpad.net/ecryptfs
[18] http://www.linuxjournal.com/article/9400
[19] http://manpages.ubuntu.com/manpages/xenial/en/man7/ecryptfs.7.html

Chapter 10. Monitoring

1. Overview

The monitoring of essential servers and services is an important part of system administration. Most network services are monitored for performance, availability, or both. This section will cover installation and configuration of Nagios for availability monitoring, and Munin for performance monitoring.

The examples in this section will use two servers with hostnames *server01* and *server02*. *Server01* will be configured with Nagios to monitor services on itself and *server02*. Server01 will also be setup with the munin package to gather information from the network. Using the munin-node package, *server02* will be configured to send information to *server01*.

Hopefully these simple examples will allow you to monitor additional servers and services on your network.

2. Nagios

2.1. Installation

First, on *server01* install the nagios package. In a terminal enter:

```
sudo apt install nagios3 nagios-nrpe-plugin
```

You will be asked to enter a password for the *nagiosadmin* user. The user's credentials are stored in `/etc/nagios3/htpasswd.users`. To change the *nagiosadmin* password, or add additional users to the Nagios CGI scripts, use the htpasswd that is part of the apache2-utils package.

For example, to change the password for the *nagiosadmin* user enter:

```
sudo htpasswd /etc/nagios3/htpasswd.users nagiosadmin
```

To add a user:

```
sudo htpasswd /etc/nagios3/htpasswd.users steve
```

Next, on *server02* install the nagios-nrpe-server package. From a terminal on server02 enter:

```
sudo apt install nagios-nrpe-server
```

NRPE allows you to execute local checks on remote hosts. There are other ways of accomplishing this through other Nagios plugins as well as other checks.

2.2. Configuration Overview

There are a couple of directories containing Nagios configuration and check files.

- `/etc/nagios3`: contains configuration files for the operation of the nagios daemon, CGI files, hosts, etc.
- `/etc/nagios-plugins`: houses configuration files for the service checks.
- `/etc/nagios`: on the remote host contains the nagios-nrpe-server configuration files.
- `/usr/lib/nagios/plugins/`: where the check binaries are stored. To see the options of a check use the *-h* option.

  For example: **/usr/lib/nagios/plugins/check_dhcp -h**

There are a plethora of checks Nagios can be configured to execute for any given host. For this example Nagios will be configured to check disk space, DNS, and a MySQL hostgroup. The DNS check will be on *server02*, and the MySQL hostgroup will include both *server01* and *server02*.

See *Section 1, “HTTPD - Apache2 Web Server” [p. 211]* for details on setting up Apache, *Chapter 8, Domain Name Service (DNS) [p. 163]* for DNS, and *Section 1, “MySQL” [p. 230]* for MySQL.

Additionally, there are some terms that once explained will hopefully make understanding Nagios configuration easier:

- *Host*: a server, workstation, network device, etc that is being monitored.
- *Host Group*: a group of similar hosts. For example, you could group all web servers, file server, etc.
- *Service*: the service being monitored on the host. Such as HTTP, DNS, NFS, etc.
- *Service Group*: allows you to group multiple services together. This is useful for grouping multiple HTTP for example.
- *Contact*: person to be notified when an event takes place. Nagios can be configured to send emails, SMS messages, etc.

By default Nagios is configured to check HTTP, disk space, SSH, current users, processes, and load on the *localhost*. Nagios will also ping check the *gateway*.

Large Nagios installations can be quite complex to configure. It is usually best to start small, one or two hosts, get things configured the way you like then expand.

2.3. Configuration

- 1. First, create a *host* configuration file for *server02*. Unless otherwise specified, run all these commands on *server01*. In a terminal enter:

```
sudo cp /etc/nagios3/conf.d/localhost_nagios2.cfg \
/etc/nagios3/conf.d/server02.cfg
```

In the above and following command examples, replace *"server01"*, *"server02"* *172.18.100.100*, and *172.18.100.101* with the host names and IP addresses of your servers.

2. Next, edit `/etc/nagios3/conf.d/server02.cfg`:

```
define host{
        use                     generic-host  ; Name of host template to use
        host_name               server02
        alias                   Server 02
        address                 172.18.100.101
}

# check DNS service.
define service {
        use                             generic-service
        host_name                       server02
        service_description             DNS
        check_command                   check_dns!172.18.100.101
}
```

3. Restart the nagios daemon to enable the new configuration:

```
sudo systemctl restart nagio3.service
```

- 1. Now add a service definition for the MySQL check by adding the following to `/etc/nagios3/conf.d/services_nagios2.cfg`:

```
# check MySQL servers.
define service {
        hostgroup_name        mysql-servers
        service_description   MySQL
        check_command         check_mysql_cmdlinecred!nagios!secret!$HOSTADDRESS
        use                   generic-service
        notification_interval 0 ; set > 0 if you want to be renotified
}
```

2. A *mysql-servers* hostgroup now needs to be defined. Edit `/etc/nagios3/conf.d/hostgroups_nagios2.cfg` adding:

```
# MySQL hostgroup.
define hostgroup {
        hostgroup_name  mysql-servers
                alias           MySQL servers
                members         localhost, server02
        }
```

3. The Nagios check needs to authenticate to MySQL. To add a *nagios* user to MySQL enter:

```
mysql -u root -p -e "create user nagios identified by 'secret';"
```

The *nagios* user will need to be added all hosts in the *mysql-servers* hostgroup.

4. Restart nagios to start checking the MySQL servers.

```
sudo systemctl restart nagios3.service
```

- 1. Lastly configure NRPE to check the disk space on *server02*.

On *server01* add the service check to `/etc/nagios3/conf.d/server02.cfg`:

```
# NRPE disk check.
define service {
        use                     generic-service
        host_name               server02
        service_description     nrpe-disk
        check_command           check_nrpe_1arg!check_all_disks!172.18.100.101
}
```

2. Now on *server02* edit `/etc/nagios/nrpe.cfg` changing:

```
allowed_hosts=172.18.100.100
```

And below in the command definition area add:

```
command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -e
```

3. Finally, restart nagios-nrpe-server:

```
sudo systemctl restart nagios-nrpe-server.service
```

4. Also, on *server01* restart nagios:

```
sudo systemctl restart nagios3.service
```

You should now be able to see the host and service checks in the Nagios CGI files. To access them point a browser to http://server01/nagios3. You will then be prompted for the *nagiosadmin* username and password.

2.4. References

This section has just scratched the surface of Nagios' features. The nagios-plugins-extra and nagios-snmp-plugins contain many more service checks.

- For more information see *Nagios*[1] website.
- Specifically the *Online Documentation*[2] site.
- There is also a list of *books*[3] related to Nagios and network monitoring:
- The *Nagios Ubuntu Wiki*[4] page also has more details.

[1] http://www.nagios.org/
[2] http://nagios.sourceforge.net/docs/3_0/
[3] http://www.nagios.org/propaganda/books/
[4] https://help.ubuntu.com/community/Nagios3

3. Munin

3.1. Installation

Before installing Munin on *server01* apache2 will need to be installed. The default configuration is fine for running a munin server. For more information see *Section 1, “HTTPD - Apache2 Web Server” [p. 211]*.

First, on *server01* install munin. In a terminal enter:

```
sudo apt install munin
```

Now on *server02* install the munin-node package:

```
sudo apt install munin-node
```

3.2. Configuration

On *server01* edit the `/etc/munin/munin.conf` adding the IP address for *server02*:

```
## First our "normal" host.
[server02]
       address 172.18.100.101
```

Replace *server02* and *172.18.100.101* with the actual hostname and IP address for your server.

Next, configure munin-node on *server02*. Edit `/etc/munin/munin-node.conf` to allow access by *server01*:

```
allow ^172\.18\.100\.100$
```

Replace *^172\.18\.100\.100$* with IP address for your munin server.

Now restart munin-node on *server02* for the changes to take effect:

```
sudo systemctl restart munini-node.service
```

Finally, in a browser go to *http://server01/munin*, and you should see links to nice graphs displaying information from the standard *munin-plugins* for disk, network, processes, and system.

Since this is a new install it may take some time for the graphs to display anything useful.

3.3. Additional Plugins

The munin-plugins-extra package contains performance checks additional services such as DNS, DHCP, Samba, etc. To install the package, from a terminal enter:

```
sudo apt install munin-plugins-extra
```

Be sure to install the package on both the server and node machines.

3.4. References

- See the *Munin*[5] website for more details.
- Specifically the *Munin Documentation*[6] page includes information on additional plugins, writing plugins, etc.

[5] http://munin-monitoring.org/

[6] https://munin.readthedocs.io/en/latest/

Chapter 11. 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, Chromium, or Internet Explorer.

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:

```
www.ubuntu.com
```

To view the *community*[2] sub-page, a user will enter the FQDN followed by a path:

```
www.ubuntu.com/community
```

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 install apache2
```

1.2. Configuration

Apache2 is configured by placing *directives* in plain text configuration files. These *directives* are separated between the following files and directories:

- *apache2.conf:* the main Apache2 configuration file. Contains settings that are *global* to Apache2.
- *httpd.conf:* historically the main Apache2 configuration file, named after the httpd daemon. Now the file does not exist. In older versions of Ubuntu the file might be present, but empty, as all configuration options have been moved to the below referenced directories.
- *conf-available:* this directory contains available configuration files. All files that were previously in `/etc/apache2/conf.d` should be moved to `/etc/apache2/conf-available`.

[1] http://www.ubuntu.com
[2] http://www.ubuntu.com/community

- *conf-enabled:* holds *symlinks* to the files in `/etc/apache2/conf-available`. When a configuration file is symlinked, it will be enabled the next time apache2 is restarted.
- *envvars:* file where Apache2 *environment* variables are set.
- *mods-available:* this directory contains configuration files to both load *modules* and configure them. Not all modules will have specific configuration files, however.
- *mods-enabled:* holds *symlinks* to the files in `/etc/apache2/mods-available`. When a module configuration file is symlinked it will be enabled the next time apache2 is restarted.
- *ports.conf:* houses the directives that determine which TCP ports Apache2 is listening on.
- *sites-available:* this directory has configuration files for Apache2 *Virtual Hosts*. Virtual Hosts allow Apache2 to be configured for multiple sites that have separate configurations.
- *sites-enabled:* like mods-enabled, `sites-enabled` contains symlinks to the `/etc/apache2/sites-available` directory. Similarly when a configuration file in sites-available is symlinked, the site configured by it will be active once Apache2 is restarted.
- *magic:* instructions for determining MIME type based on the first few bytes of a file.

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, typically via `/etc/apache2/mods-available/mime.conf`, which might also include additions and overrides, and is `/etc/mime.types` by default.

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/000-default.conf`.

  

  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.

  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:

[3] http://httpd.apache.org/docs/2.4/

```
sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/
mynewsite.conf
```

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.conf`).

  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, the following configuration will cause your site to respond to any domain request ending in *.ubunturocks.com*.

  ```
  ServerAlias *.ubunturocks.com
  ```

- The *DocumentRoot* directive specifies where Apache2 should look for the files that make up the site. The default value is /var/www/html, as specified in `/etc/apache2/sites-available/000-default.conf`. If desired, change this value in your site's virtual host file, and remember to create that directory if necessary!

Enable the new *VirtualHost* using the a2ensite utility and restart Apache2:

```
sudo a2ensite mynewsite
sudo systemctl restart apache2.service
```

Be sure to replace *mynewsite* with a more descriptive name for the VirtualHost. One method is to name the file after the *ServerName* directive of the VirtualHost.

Similarly, use the a2dissite utility to disable sites. This is can be useful when troubleshooting configuration problems with multiple VirtualHosts:

```
sudo a2dissite mynewsite
sudo systemctl restart apache2.service
```

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/mods-available/dir.conf` is "index.html index.cgi index.pl index.php index.xhtml index.htm". 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 Apache2 to use for specific error events. For example, if a user requests a resource that does not exist, a 404 error will occur. By default, Apache2 will simply return a HTTP 404 Return code. Read `/etc/apache2/conf-available/localized-error-pages.conf` for detailed instructions for using ErrorDocument, including locations of example files.
- 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/conf-available/other-vhosts-access-log.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. *Options* is one of these directives. A Directory stanza is enclosed in XML-like tags, like so:

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

  The *Options* directive within a Directory stanza accepts one or more of the following values (among others), separated by spaces:
  - **ExecCGI** - Allow execution of CGI scripts. CGI scripts are not executed if this option is not chosen.

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

- **Includes** - Allow server-side includes. Server-side includes allow an HTML file to *include* other files. See *Apache SSI documentation (Ubuntu community)*[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. httpd Settings

This section explains some basic httpd daemon configuration 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.

Group - 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".

[4] https://help.ubuntu.com/community/ServerSideIncludes
[5] http://httpd.apache.org/docs/2.4/mod/mod_negotiation.html#multiviews

1.2.4. Apache2 Modules

Apache2 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 Apache2. 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, Apache2 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. For example, run the following command at a terminal prompt to install the *MySQL Authentication* module:

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

See the `/etc/apache2/mods-available` directory, for additional modules.

Use the a2enmod utility to enable a module:

```
sudo a2enmod auth_mysql
sudo systemctl restart apache2.service
```

Similarly, a2dismod will disable a module:

```
sudo a2dismod auth_mysql
sudo systemctl restart apache2.service
```

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 at 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.conf`. In order for Apache2 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. 195]*

To configure Apache2 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 Apache2 now configured for HTTPS, restart the service to enable the new settings:

```
sudo systemctl restart apache2.service
```

Depending on how you obtained your certificate you may need to enter a passphrase when Apache2 starts.

You can access the secure server pages by typing https://your_hostname/url/ in your browser address bar.

1.4. Sharing Write Permission

For more than one user to be able to write to the same directory it will be necessary to grant write permission to a group they share in common. The following example grants shared write permission to `/var/www/html` to the group "webmasters".

```
sudo chgrp -R webmasters /var/www/html
sudo find /var/www/html -type d -exec chmod g=rwxs "{}" \;
sudo find /var/www/html -type f -exec chmod g=rw  "{}" \;
```

These commands recursively set the group permission on all files and directories in /var/www/html to read write and set user id. This has the effect of having the files and directories inherit their group and permission from their parrent. Many admins find this useful for allowing multiple users to edit files in a directory tree.

If access must be granted to more than one group per directory, enable Access Control Lists (ACLs).

1.5. References

- *Apache2 Documentation*[6] contains in depth information on Apache2 configuration directives. Also, see the apache2-doc package for the official Apache2 docs.
- See the *Mod SSL Documentation*[7] site for more SSL related information.
- O'Reilly's *Apache Cookbook*[8] is a good resource for accomplishing specific Apache2 configurations.
- For Ubuntu specific Apache2 questions, ask in the *#ubuntu-server* IRC channel on *freenode.net*[9].
- Usually integrated with PHP and MySQL the *Apache MySQL PHP Ubuntu Wiki* [10] page is a good resource.

[6] http://httpd.apache.org/docs/2.4/
[7] http://www.modssl.org/docs/
[8] http://oreilly.com/catalog/9780596001919/
[9] http://freenode.net/
[10] https://help.ubuntu.com/community/ApacheMySQLPHP

2. PHP - Scripting Language

PHP is a general-purpose scripting language suited for Web development. PHP scripts can be embedded into HTML. This section explains how to install and configure PHP in an Ubuntu System with Apache2 and MySQL.

This section assumes you have installed and configured Apache2 Web Server and MySQL Database Server. You can refer to the Apache2 and MySQL sections in this document to install and configure Apache2 and MySQL respectively.

2.1. Installation

PHP is available in Ubuntu Linux. Unlike python and perl, which are installed in the base system, PHP must be added.

- To install PHP and the Apache PHP module you can enter the following command at a terminal prompt:

  ```
  sudo apt install php libapache2-mod-php
  ```

  You can run PHP scripts at a terminal prompt. To run PHP scripts at a terminal prompt you should install the php-cli package. To install php-cli you can enter the following command at a terminal prompt:

  ```
  sudo apt install php-cli
  ```

  You can also execute PHP scripts without installing the Apache PHP module. To accomplish this, you should install the php-cgi package. You can run the following command at a terminal prompt to install the php-cgi package:

  ```
  sudo apt install php-cgi
  ```

  To use MySQL with PHP you should install the php-mysql package. To install php-mysql you can enter the following command at a terminal prompt:

  ```
  sudo apt install php-mysql
  ```

  Similarly, to use PostgreSQL with PHP you should install the php-pgsql package. To install php-pgsql you can enter the following command at a terminal prompt:

  ```
  sudo apt install php-pgsql
  ```

2.2. Configuration

If you have installed the libapache2-mod-php or php-cgi packages, you can run PHP scripts from your web browser. If you have installed the php-cli package, you can run PHP scripts at a terminal prompt.

By default, when libapache2-mod-php is installed, the Apache 2 Web server is configured to run PHP scripts. In other words, the PHP module is enabled in the Apache Web server when you install the module. Please verify if the files `/etc/apache2/mods-enabled/php7.0.conf` and `/etc/apache2/mods-enabled/php7.0.load` exist. If they do not exist, you can enable the module using the **a2enmod** command.

Once you have installed the PHP related packages and enabled the Apache PHP module, you should restart the Apache2 Web server to run PHP scripts. You can run the following command at a terminal prompt to restart your web server:

```
sudo systemctl restart apache2.service
```

2.3. Testing

To verify your installation, you can run the following PHP phpinfo script:

```
<?php
  phpinfo();
?>
```

You can save the content in a file `phpinfo.php` and place it under the **DocumentRoot** directory of the Apache2 Web server. Pointing your browser to `http://hostname/phpinfo.php` will display the values of various PHP configuration parameters.

2.4. References

- For more in depth information see the *php.net*[11] documentation.
- There are a plethora of books on PHP. A good book from O'Reilly is *Learning PHP*[12]. *PHP Cook Book*[13] is also good, but has no yet been updated for PHP7.
- Also, see the *Apache MySQL PHP Ubuntu Wiki*[14] page for more information.

[11] http://www.php.net/docs.php
[12] http://oreilly.com/catalog/0636920043034/
[13] http://oreilly.com/catalog/9781565926813/
[14] https://help.ubuntu.com/community/ApacheMySQLPHP

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 caching proxy server for many users ensure it 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 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. Make this copy and protect it from writing using the following commands:

```
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
```

- 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 systemctl restart squid.service
```

If formerly a customized squid3 was used that set up the spool at `/var/log/squid3` to be a mountpoint, but otherwise kept the default configuration the upgrade will fail. The upgrade tries to rename/move files as needed, but it can't do so for an active mountpoint. In that case please either adapt the mountpoint or the config in `/etc/squid/squid.conf` so that they match.

The same applies if the **include** config statement was used to pull in more files from the old path at `/etc/squid3/`. In those cases you should move and adapt your configuration accordingly.

3.3. References

Squid Website[15]

[15] http://www.squid-cache.org/

Ubuntu Wiki Squid[16] page.

[16] https://help.ubuntu.com/community/Squid

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. 211]*. For instructions on installing MySQL refer to *Section 1, “MySQL” [p. 230]*.

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 install rails
```

4.2. Configuration

Modify the `/etc/apache2/sites-available/000-default.conf` 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.

4.3. References

- See the *Ruby on Rails*[17] website for more information.
- Also *Agile Development with Rails*[18] is a great resource.
- Another place for more information is the *Ruby on Rails Ubuntu Wiki*[19] page.

[17] http://rubyonrails.org/

[18] http://pragprog.com/titles/rails3/agile-web-development-with-rails-third-edition

[19] https://help.ubuntu.com/community/RubyOnRails

5. Apache Tomcat

Apache Tomcat is a web container that allows you to serve Java Servlets and JSP (Java Server Pages) web applications.

Ubuntu has supported packages for both Tomcat 6 and 7. Tomcat 6 is the legacy version, and Tomcat 7 is the current version where new features are implemented. Both are considered stable. This guide will focus on Tomcat 7, but most configuration details are valid for both versions.

The Tomcat 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 will run as the tomcat7 (or 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 install tomcat7
```

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/tomcat7`. Only a few common configuration tweaks will be described here, please see *Tomcat 7.0 documentation*[20] for more.

5.2.1. Changing default ports

By default Tomcat 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 application on the system. This is done by changing the following lines in `/etc/tomcat7/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 JVMs, then try the Sun JVMs, then try some other JVMs. You can force Tomcat to use a specific JVM by setting JAVA_HOME in `/etc/default/tomcat7`:

[20] http://tomcat.apache.org/tomcat-7.0-doc/index.html

```
JAVA_HOME=/usr/lib/jvm/java-6-sun
```

5.2.3. Declaring users and roles

Usernames, passwords and roles (groups) can be defined centrally in a Servlet container. This is done in the `/etc/tomcat7/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 tomcat7-docs package contains Tomcat 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 install tomcat7-docs
```

5.3.2. Tomcat administration webapps

The tomcat7-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 install tomcat7-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-gui" in `/etc/tomcat7/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-gui" in `/etc/tomcat7/tomcat-users.xml` before you can access it.

For security reasons, the tomcat7 user cannot write to the `/etc/tomcat7` 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 tomcat7 group the necessary rights:

```
sudo chgrp -R tomcat7 /etc/tomcat7
```

```
sudo chmod -R g+w /etc/tomcat7
```

5.3.3. Tomcat examples webapps

The tomcat7-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 install tomcat7-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 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 install tomcat7-user
```

5.4.2. Creating a private instance

You can create a private instance directory by entering the following command in the terminal prompt:

```
tomcat7-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
```

5.5. References

- See the *Apache Tomcat*[21] website for more information.
- *Tomcat: The Definitive Guide*[22] is a good resource for building web applications with Tomcat.
- For additional books see the *Tomcat Books*[23] list page.

[21] http://tomcat.apache.org/
[22] http://shop.oreilly.com/product/9780596003180.do
[23] http://wiki.apache.org/tomcat/Tomcat/Books

Chapter 12. 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 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:mysql         *:*                     LISTEN      2556/mysqld
```

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

```
sudo systemctl restart mysql.service
```

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 systemctl restart mysql.service
```

If you would like to change the MySQL *root* password, in a terminal enter:

```
sudo dpkg-reconfigure mysql-server-5.5
```

The MySQL daemon will be stopped, and you will be prompted to enter a new password.

1.3. Database Engines

Whilst the default configuration of MySQL provided by the Ubuntu packages is perfectly functional and performs well there are things you may wish to consider before you proceed.

MySQL is designed to allow data to be stored in different ways. These methods are referred to as either database or storage engines. There are two main engines that you'll be interested in: InnoDB and MyISAM. Storage engines are transparent to the end user. MySQL will handle things differently under the surface, but regardless of which storage engine is in use, you will interact with the database in the same way.

Each engine has its own advantages and disadvantages.

While it is possible, and may be advantageous to mix and match database engines on a table level, doing so reduces the effectiveness of the performance tuning you can do as you'll be splitting the resources between two engines instead of dedicating them to one.

- MyISAM is the older of the two. It can be faster than InnoDB under certain circumstances and favours a read only workload. Some web applications have been tuned around MyISAM (though that's not to imply that they will slow under InnoDB). MyISAM also supports the FULLTEXT data type, which allows very fast searches of large quantities of text data. However MyISAM is only capable of locking an entire table for writing. This means only one process can update a table at a time. As any application that uses the table scales this may prove to be a hindrance. It also lacks journaling, which makes it harder for data to be recovered after a crash. The following link provides some points for consideration about using *MyISAM on a production database*[1].
- InnoDB is a more modern database engine, designed to be *ACID compliant*[2] which guarantees database transactions are processed reliably. Write locking can occur on a row level basis within a table. That means multiple updates can occur on a single table simultaneously. Data caching is also handled in memory within the database engine, allowing caching on a more efficient row level basis rather than file block. To meet ACID compliance all transactions are journaled independently of the main tables. This allows for much more reliable data recovery as data consistency can be checked.

As of MySQL 5.5 InnoDB is the default engine, and is highly recommended over MyISAM unless you have specific need for features unique to the engine.

1.4. Advanced configuration

1.4.1. Creating a tuned my.cnf file

There are a number of parameters that can be adjusted within MySQL's configuration file that will allow you to improve the performance of the server over time. For initial set-up you may find *Percona's my.cnf*

[1] http://www.mysqlperformanceblog.com/2006/06/17/using-myisam-in-production/
[2] http://en.wikipedia.org/wiki/ACID

generating tool[3] useful. This tool will help generate a my.cnf file that will be much more optimised for your specific server capabilities and your requirements.

Do not replace your existing my.cnf file with Percona's one if you have already loaded data into the database. Some of the changes that will be in the file will be incompatible as they alter how data is stored on the hard disk and you'll be unable to start MySQL. If you do wish to use it and you have existing data, you will need to carry out a mysqldump and reload:

```
mysqldump --all-databases --routines -u root -p > ~/fulldump.sql
```

This will then prompt you for the root password before creating a copy of the data. It is advisable to make sure there are no other users or processes using the database whilst this takes place. Depending on how much data you've got in your database, this may take a while. You won't see anything on the screen during this process.

Once the dump has been completed, shut down MySQL:

```
sudo systemctl stop mysql.service
```

Now backup the original my.cnf file and replace with the new one:

```
sudo cp /etc/mysql/my.cnf /etc/mysql/my.cnf.backup
sudo cp /path/to/new/my.cnf /etc/mysql/my.cnf
```

Then delete and re-initialise the database space and make sure ownership is correct before restarting MySQL:

```
sudo rm -rf /var/lib/mysql/*
sudo mysql_install_db
sudo chown -R mysql: /var/lib/mysql
sudo systemctl start mysql.service
```

Finally all that's left is to re-import your data. To give us an idea of how far the import process has got you may find the 'Pipe Viewer' utility, pv, useful. The following shows how to install and use pv for this case, but if you'd rather not use it just replace pv with cat in the following command. Ignore any ETA times produced by pv, they're based on the average time taken to handle each row of the file, but the speed of inserting can vary wildly from row to row with mysqldumps:

```
sudo apt install pv
pv ~/fulldump.sql | mysql
```

Once that is complete all is good to go!

This is not necessary for all my.cnf changes. Most of the variables you may wish to change to improve performance are adjustable even whilst the server is running. As with anything, make sure to have a good backup copy of config files and data before making changes.

[3] http://tools.percona.com/members/wizard

1.4.2. MySQL Tuner

MySQL Tuner is a useful tool that will connect to a running MySQL instance and offer suggestions for how it can be best configured for your workload. The longer the server has been running for, the better the advice mysqltuner can provide. In a production environment, consider waiting for at least 24 hours before running the tool. You can get install mysqltuner from the Ubuntu repositories:

```
sudo apt install mysqltuner
```

Then once its been installed, run it:

```
mysqltuner
```

and wait for its final report. The top section provides general information about the database server, and the bottom section provides tuning suggestions to alter in your my.cnf. Most of these can be altered live on the server without restarting, look through the official MySQL documentation (link in Resources section) for the relevant variables to change in production. The following is part of an example report from a production database which shows there may be some benefit from increasing the amount of query cache:

```
-------- Recommendations -----------------------------------------------------
General recommendations:
    Run OPTIMIZE TABLE to defragment tables for better performance
    Increase table_cache gradually to avoid file descriptor limits
Variables to adjust:
    key_buffer_size (> 1.4G)
    query_cache_size (> 32M)
    table_cache (> 64)
    innodb_buffer_pool_size (>= 22G)
```

One final comment on tuning databases: Whilst we can broadly say that certain settings are the best, performance can vary from application to application. For example, what works best for Wordpress might not be the best for Drupal, Joomla or proprietary applications. Performance is dependent on the types of queries, use of indexes, how efficient the database design is and so on. You may find it useful to spend some time searching for database tuning tips based on what applications you're using it for. Once you get past a certain point any adjustments you make will only result in minor improvements, and you'll be better off either improving the application, or looking at scaling up your database environment through either using more powerful hardware or by adding slave servers.

1.5. Resources

- See the *MySQL Home Page*[4] for more information.
- Full documentation is available in both online and offline formats from the *MySQL Developers portal*[5]
- For general SQL information see *Using SQL Special Edition*[6] by Rafe Colburn.

[4] http://www.mysql.com/
[5] http://dev.mysql.com/doc/
[6] http://www.informit.com/store/product.aspx?isbn=0768664128

- The *Apache MySQL PHP Ubuntu Wiki*[7] page also has useful information.

[7] https://help.ubuntu.com/community/ApacheMySQLPHP

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 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

PostgreSQL supports multiple client authentication methods. IDENT authentication method is used for postgres and local users, unless otherwise configured. Please refer to the *PostgreSQL Administrator's Guide*[8] if you would like to configure alternatives like Kerberos.

The following discussion assumes that you wish to enable TCP/IP connections and use the MD5 method for client authentication. PostgreSQLconfiguration files are stored in the `/etc/postgresql/<version>/main` directory. For example, if you install PostgreSQL 9.5, the configuration files are stored in the `/etc/postgresql/9.5/main` directory.

To configure *ident* authentication, add entries to the `/etc/postgresql/9.5/main/pg_ident.conf` file. There are detailed comments in the file to guide you.

To enable other computers to connect to your PostgreSQL server, edit the file `/etc/postgresql/9.5/main/postgresql.conf`

Locate the line *#listen_addresses = 'localhost'* and change it to:

```
listen_addresses = '*'
```

To allow both IPv4 and IPv6 connections replace 'localhost' with '::'

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:

[8] http://www.postgresql.org/docs/current/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/9.5/main/pg_hba.conf` to use *MD5* authentication with the *postgres* user:

```
local   all         postgres                          md5
```

Finally, you should restart the PostgreSQL service to initialize the new configuration. From a terminal prompt enter the following to restart PostgreSQL:

```
sudo systemctl restart postgresql.service
```

The above configuration is not complete by any means. Please refer to the *PostgreSQL Administrator's Guide*[9] to configure more parameters.

You can test server connections from other machines by using the PostgreSQL client.

```
sudo apt install postgresql-client
psql -h postgres.example.com -U postgres -W
```

Replace the domain name with your actual server domain name.

2.3. Backups

PostgreSQL databases should be backed up regularly. Refer to the *PostgreSQL Administrator's Guide*[10] for different approaches.

2.4. Resources

- As mentioned above the *PostgreSQL Administrator's Guide*[11] is an excellent resource. The guide is also available in the postgresql-doc-9.5 package. Execute the following in a terminal to install the package:

  ```
  sudo apt install postgresql-doc-9.5
  ```

  To view the guide enter **file:///usr/share/doc/postgresql-doc-9.5/html/index.html** into the address bar of your browser.

[9] http://www.postgresql.org/docs/current/static/admin.html
[10] http://www.postgresql.org/docs/current/static/backup.html
[11] http://www.postgresql.org/docs/current/static/admin.html

- For general SQL information see *Using SQL Special Edition*[12] by Rafe Colburn.
- Also, see the *PostgreSQL Ubuntu Wiki*[13] page for more information.

[12] http://www.informit.com/store/product.aspx?isbn=0768664128
[13] https://help.ubuntu.com/community/PostgreSQL

Chapter 13. LAMP Applications

1. Overview

LAMP installations (Linux + Apache + MySQL + PHP/Perl/Python) are a popular setup for Ubuntu servers. There is a plethora of Open Source applications written using the LAMP application stack. Some popular LAMP applications are Wiki's, Content Management Systems, and Management Software such as phpMyAdmin.

One advantage of LAMP is the substantial flexibility for different database, web server, and scripting languages. Popular substitutes for MySQL include PostgreSQL and SQLite. Python, Perl, and Ruby are also frequently used instead of PHP. While Nginx, Cherokee and Lighttpd can replace Apache.

The fastest way to get started is to install LAMP using tasksel. Tasksel is a Debian/Ubuntu tool that installs multiple related packages as a co-ordinated "task" onto your system. To install a LAMP server:

- At a terminal prompt enter the following command:

```
sudo tasksel install lamp-server
```

After installing it you'll be able to install most *LAMP* applications in this way:

- Download an archive containing the application source files.
- Unpack the archive, usually in a directory accessible to a web server.
- Depending on where the source was extracted, configure a web server to serve the files.
- Configure the application to connect to the database.
- Run a script, or browse to a page of the application, to install the database needed by the application.
- Once the steps above, or similar steps, are completed you are ready to begin using the application.

A disadvantage of using this approach is that the application files are not placed in the file system in a standard way, which can cause confusion as to where the application is installed. Another larger disadvantage is updating the application. When a new version is released, the same process used to install the application is needed to apply updates.

Fortunately, a number of *LAMP* applications are already packaged for Ubuntu, and are available for installation in the same way as non-LAMP applications. Depending on the application some extra configuration and setup steps may be needed, however.

This section covers how to install some *LAMP* applications.

2. Moin Moin

MoinMoin is a wiki engine implemented in Python, based on the PikiPiki Wiki engine, and licensed under the GNU GPL.

2.1. Installation

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

```
sudo apt install python-moinmoin
```

You should also install apache2 web server. For installing the apache2 web server, please refer to *Section 1.1, “Installation” [p. 211]* sub-section in *Section 1, “HTTPD - Apache2 Web Server” [p. 211]* section.

2.2. Configuration

To configure 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/mywiki/data'
```

to

```
data_dir = '/usr/share/moin/mywiki/data'
```

Also, below the *data_dir* option add the *data_underlay_dir*:

```
data_underlay_dir='/usr/share/moin/mywiki/underlay'
```

If the `/etc/moin/mywiki.py` file does not exist, you should copy `/usr/share/moin/config/wikifarm/mywiki.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.

You should add the following lines in `/etc/apache2/sites-available/000-default.conf` file inside the "<VirtualHost *>" tag:

```
### moin
  ScriptAlias /mywiki "/usr/share/moin/mywiki/moin.cgi"
  alias /moin_static<version> "/usr/share/moin/htdocs"
  <Directory /usr/share/moin/htdocs>
  Order allow,deny
  allow from all
  </Directory>
### end moin
```

The version in the above example is determined by running:

```
$ moin --version
```

If the output shows version 1.9.7, your second line should be:

```
alias /moin_static197 "/usr/share/moin/htdocs"
```

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 systemctl restart apache2.service
```

2.3. Verification

You can verify the Wiki application and see if it works by pointing your web browser to the following URL:

```
http://localhost/mywiki
```

For more details, please refer to the *MoinMoin*[1] web site.

2.4. References

- For more information see the *moinmoin Wiki*[2].
- Also, see the *Ubuntu Wiki MoinMoin*[3] page.

[1] http://moinmo.in/
[2] http://moinmo.in/
[3] https://help.ubuntu.com/community/MoinMoin

3. phpMyAdmin

phpMyAdmin is a LAMP application specifically written for administering MySQL servers. Written in PHP, and accessed through a web browser, phpMyAdmin provides a graphical interface for database administration tasks.

3.1. Installation

Before installing phpMyAdmin you will need access to a MySQL database either on the same host as that phpMyAdmin is installed on, or on a host accessible over the network. For more information see *Section 1, "MySQL" [p. 230]*. From a terminal prompt enter:

```
sudo apt install phpmyadmin
```

At the prompt choose which web server to be configured for phpMyAdmin. The rest of this section will use Apache2 for the web server.

In a browser go to *http://servername/phpmyadmin*, replacing *servername* with the server's actual hostname. At the login, page enter *root* for the *username*, or another MySQL user, if you have any setup, and enter the MySQL user's password.

Once logged in you can reset the *root* password if needed, create users, create/destroy databases and tables, etc.

3.2. Configuration

The configuration files for phpMyAdmin are located in `/etc/phpmyadmin`. The main configuration file is `/etc/phpmyadmin/config.inc.php`. This file contains configuration options that apply globally to phpMyAdmin.

To use phpMyAdmin to administer a MySQL database hosted on another server, adjust the following in `/etc/phpmyadmin/config.inc.php`:

```
$cfg['Servers'][$i]['host'] = 'db_server';
```

Replace *db_server* with the actual remote database server name or IP address. Also, be sure that the phpMyAdmin host has permissions to access the remote database.

Once configured, log out of phpMyAdmin and back in, and you should be accessing the new server.

The `config.header.inc.php` and `config.footer.inc.php` files are used to add a HTML header and footer to phpMyAdmin.

Another important configuration file is `/etc/phpmyadmin/apache.conf`, this file is symlinked to `/etc/apache2/conf-available/phpmyadmin.conf`, and, once enabled, is used to configure Apache2 to serve the

phpMyAdmin site. The file contains directives for loading PHP, directory permissions, etc. From a terminal type:

```
sudo ln -s /etc/phpmyadmin/apache.conf /etc/apache2/conf-available/phpmyadmin.conf
sudo a2enconf phpmyadmin.conf
sudo systemctl reload apache2.service
```

For more information on configuring Apache2 see *Section 1, "HTTPD - Apache2 Web Server" [p. 211]*.

3.3. References

- The phpMyAdmin documentation comes installed with the package and can be accessed from the *phpMyAdmin Documentation* link (a question mark with a box around it) under the phpMyAdmin logo. The official docs can also be access on the *phpMyAdmin*[4] site.
- Also, *Mastering phpMyAdmin*[5] is a great resource.
- A third resource is the *phpMyAdmin Ubuntu Wiki*[6] page.

[4] http://www.phpmyadmin.net/home_page/docs.php
[5] http://www.packtpub.com/phpmyadmin-3rd-edition/book
[6] https://help.ubuntu.com/community/phpMyAdmin

4. WordPress

Wordpress is a blog tool, publishing platform and CMS implemented in PHP and licensed under the GNU GPLv2.

4.1. Installation

To install WordPress, run the following comand in the command prompt:

```
sudo apt install wordpress
```

You should also install apache2 web server and mysql server. For installing apache2 web server, please refer to *Section 1.1, “Installation” [p. 211]* sub-section in *Section 1, “HTTPD - Apache2 Web Server” [p. 211]* section. For installing mysql server, please refer to *Section 1.1, “Installation” [p. 230]* sub-section in *Section 1, “MySQL” [p. 230]* section.

4.2. Configuration

For configuring your first WordPress application, configure an apache site. Open `/etc/apache2/sites-available/wordpress.conf` and write the following lines:

```
Alias /blog /usr/share/wordpress
<Directory /usr/share/wordpress>
    Options FollowSymLinks
    AllowOverride Limit Options FileInfo
    DirectoryIndex index.php
    Order allow,deny
    Allow from all
</Directory>
<Directory /usr/share/wordpress/wp-content>
    Options FollowSymLinks
    Order allow,deny
    Allow from all
</Directory>
```

Enable this new WordPress site

```
sudo a2ensite wordpress
```

Once you configure the apache2 web server and make it ready for your WordPress application, you should restart it. You can run the following command to restart the apache2 web server:

```
sudo systemctl restart apache2.service
```

To facilitate multiple WordPress installations, the name of this configuration file is based on the Host header of the HTTP request. This means that you can have a configuration per VirtualHost by simply

matching the hostname portion of this configuration with your Apache Virtual Host. e.g. /etc/wordpress/config-10.211.55.50.php, /etc/wordpress/config-hostalias1.php, etc. These instructions assume you can access Apache via the localhost hostname (perhaps by using an ssh tunnel) if not, replace /etc/wordpress/config-localhost.php with /etc/wordpress/config-NAME_OF_YOUR_VIRTUAL_HOST.php.

Once the configuration file is written, it is up to you to choose a convention for username and password to mysql for each WordPress database instance. This documentation shows only one, localhost, example.

Now configure WordPress to use a mysql database. Open `/etc/wordpress/config-localhost.php` file and write the following lines:

```
<?php
define('DB_NAME', 'wordpress');
define('DB_USER', 'wordpress');
define('DB_PASSWORD', 'yourpasswordhere');
define('DB_HOST', 'localhost');
define('WP_CONTENT_DIR', '/usr/share/wordpress/wp-content');
?>
```

Now create this mysql database. Open a temporary file with mysql commands `wordpress.sql` and write the following lines:

```
CREATE DATABASE wordpress;
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP,ALTER
ON wordpress.*
TO wordpress@localhost
IDENTIFIED BY 'yourpasswordhere';
FLUSH PRIVILEGES;
```

Execute these commands.

```
cat wordpress.sql | sudo mysql --defaults-extra-file=/etc/mysql/debian.cnf
```

Your new WordPress can now be configured by visiting *http://localhost/blog/wp-admin/install.php*. (Or *http://NAME_OF_YOUR_VIRTUAL_HOST/blog/wp-admin/install.php* if your server has no GUI and you are completing WordPress configuration via a web browser running on another computer.) Fill out the Site Title, username, password, and E-mail and click Install WordPress.

Note the generated password (if applicable) and click the login password. Your WordPress is now ready for use.

4.3. References

- *WordPress.org Codex*[7]
- *Ubuntu Wiki WordPress*[8]

[7] https://codex.wordpress.org/

[8] https://help.ubuntu.com/community/WordPress

Chapter 14. 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 downloading files between computers. In the past, it has also been used for uploading but, as that method does not use encryption, user credentials as well as data transferred in the clear and are easily intercepted. So if you are here looking for a way to upload and download files securely, see the section on OpenSSH in *Chapter 6, Remote Administration [p. 100]* instead.

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. This latter choice is very insecure and should not be used except in special circumstances. If you are looking to transfer files securely see SFTP in the section on OpenSSH-Server. 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 install vsftpd
```

1.2. Anonymous FTP Configuration

By default vsftpd is *not* configured to allow anonymous download. If you wish to enable anonymous download edit `/etc/vsftpd.conf` by changing:

```
anonymous_enable=Yes
```

During installation a *ftp* user is created with a home directory of `/srv/ftp`. This is the default FTP directory.

If you wish to change this location, to `/srv/files/ftp` for example, simply create a directory in another location and change the *ftp* user's home directory:

```
sudo mkdir /srv/files/ftp
sudo usermod -d /srv/files/ftp ftp
```

After making the change restart vsftpd:

```
sudo restart vsftpd
```

Finally, copy any files and directories you would like to make available through anonymous FTP to `/srv/files/ftp`, or `/srv/ftp` if you wish to use the default.

1.3. User Authenticated FTP Configuration

By default vsftpd is configured to authenticate system users and allow them to download files. If you want users to be able to upload files, edit `/etc/vsftpd.conf`:

```
write_enable=YES
```

Now restart vsftpd:

```
sudo restart vsftpd
```

Now when system users login to FTP they will start in their *home* directories where they can download, upload, create directories, etc.

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

```
anon_upload_enable=YES
```

Enabling anonymous FTP upload can be an extreme security risk. It is best to not enable anonymous upload on servers accessed directly from the Internet.

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.

1.4. Securing FTP

There are options in `/etc/vsftpd.conf` to help make vsftpd more secure. For example users can be limited to their home directories by uncommenting:

```
chroot_local_user=YES
```

You can also limit a specific list of users to just their home directories:

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
```

After uncommenting the above options, create a `/etc/vsftpd.chroot_list` containing a list of users one per line. Then restart vsftpd:

```
sudo restart vsftpd
```

Also, the `/etc/ftpusers` file is a list of users that are *disallowed* FTP access. The default list includes root, daemon, nobody, etc. To disable FTP access for additional users simply add them to the list.

FTP can also be encrypted using *FTPS*. Different from *SFTP*, *FTPS* is FTP over Secure Socket Layer (SSL). *SFTP* is a FTP like session over an encrypted *SSH* connection. A major difference is that users of SFTP need to have a *shell* account on the system, instead of a *nologin* shell. Providing all users with a shell may not be ideal for some environments, such as a shared web host. However, it is possible to restrict such accounts to only SFTP and disable shell interaction. See the section on OpenSSH-Server for more.

To configure *FTPS*, edit `/etc/vsftpd.conf` and at the bottom add:

```
ssl_enable=Yes
```

Also, notice the certificate and key related options:

```
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

By default these options are set to the certificate and key provided by the ssl-cert package. In a production environment these should be replaced with a certificate and key generated for the specific host. For more information on certificates see *Section 5, “Certificates” [p. 195]*.

Now restart vsftpd, and non-anonymous users will be forced to use *FTPS*:

```
sudo restart vsftpd
```

To allow users with a shell of `/usr/sbin/nologin` access to FTP, but have no shell access, edit `/etc/shells` adding the *nologin* shell:

```
# /etc/shells: valid login shells
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh
/usr/bin/rc
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
```

```
/bin/rbash
/usr/bin/screen
/usr/sbin/nologin
```

This is necessary because, by default vsftpd uses PAM for authentication, and the `/etc/pam.d/vsftpd` configuration file contains:

```
auth    required        pam_shells.so
```

The *shells* PAM module restricts access to shells listed in the `/etc/shells` file.

Most popular FTP clients can be configured to connect using FTPS. The lftp command line FTP client has the ability to use FTPS as well.

1.5. References

- See the *vsftpd website*[1] for more information.
- For detailed `/etc/vsftpd.conf` options see the *vsftpd.conf man page*[2].

[1] http://vsftpd.beasts.org/vsftpd_conf.html

[2] http://manpages.ubuntu.com/manpages/xenial/en/man5/vsftpd.conf.5.html

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 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 systemctl start nfs-kernel-server.service
```

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,wsize=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 install nfs-common
```

2.4. References

Linux NFS faq[3]

Ubuntu Wiki NFS Howto[4]

[3] http://nfs.sourceforge.net/

[4] https://help.ubuntu.com/community/NFSv4Howto

3. iSCSI Initiator

iSCSI (Internet Small Computer System Interface) is a protocol that allows SCSI commands to be transmitted over a network. Typically iSCSI is implemented in a SAN (Storage Area Network) to allow servers to access a large store of hard drive space. The iSCSI protocol refers to clients as *initiators* and iSCSI servers as *targets*.

Ubuntu Server can be configured as both an iSCSI initiator and a target. This guide provides commands and configuration options to setup an iSCSI initiator. It is assumed that you already have an iSCSI target on your local network and have the appropriate rights to connect to it. The instructions for setting up a target vary greatly between hardware providers, so consult your vendor documentation to configure your specific iSCSI target.

3.1. iSCSI Initiator Install

To configure Ubuntu Server as an iSCSI initiator install the open-iscsi package. In a terminal enter:

```
sudo apt install open-iscsi
```

3.2. iSCSI Initiator Configuration

Once the open-iscsi package is installed, edit `/etc/iscsi/iscsid.conf` changing the following:

```
node.startup = automatic
```

You can check which targets are available by using the iscsiadm utility. Enter the following in a terminal:

```
sudo iscsiadm -m discovery -t st -p 192.168.0.10
```

- *-m:* determines the mode that iscsiadm executes in.
- *-t:* specifies the type of discovery.
- *-p:* option indicates the target IP address.

Change example *192.168.0.10* to the target IP address on your network.

If the target is available you should see output similar to the following:

```
192.168.0.10:3260,1 iqn.1992-05.com.emc:sl7b920300005200000-2
```

The *iqn* number and IP address above will vary depending on your hardware.

You should now be able to connect to the iSCSI target, and depending on your target setup you may have to enter user credentials. Login to the iSCSI node:

```
sudo iscsiadm -m node --login
```

Check to make sure that the new disk has been detected using dmesg:

```
dmesg | grep sd
```

```
[    4.322384] sd 2:0:0:0: Attached scsi generic sg1 type 0
[    4.322797] sd 2:0:0:0: [sda] 41943040 512-byte logical blocks: (21.4 GB/20.0 GiB)
[    4.322843] sd 2:0:0:0: [sda] Write Protect is off
[    4.322846] sd 2:0:0:0: [sda] Mode Sense: 03 00 00 00
[    4.322896] sd 2:0:0:0: [sda] Cache data unavailable
[    4.322899] sd 2:0:0:0: [sda] Assuming drive cache: write through
[    4.323230] sd 2:0:0:0: [sda] Cache data unavailable
[    4.323233] sd 2:0:0:0: [sda] Assuming drive cache: write through
[    4.325312]  sda: sda1 sda2 < sda5 >
[    4.325729] sd 2:0:0:0: [sda] Cache data unavailable
[    4.325732] sd 2:0:0:0: [sda] Assuming drive cache: write through
[    4.325735] sd 2:0:0:0: [sda] Attached SCSI disk
[ 2486.941805] sd 4:0:0:3: Attached scsi generic sg3 type 0
[ 2486.952093] sd 4:0:0:3: [sdb] 1126400000 512-byte logical blocks: (576 GB/537 GiB)
[ 2486.954195] sd 4:0:0:3: [sdb] Write Protect is off
[ 2486.954200] sd 4:0:0:3: [sdb] Mode Sense: 8f 00 00 08
[ 2486.954692] sd 4:0:0:3: [sdb] Write cache: disabled, read cache: enabled, doesn't
 support DPO or FUA
[ 2486.960577]  sdb: sdb1
[ 2486.964862] sd 4:0:0:3: [sdb] Attached SCSI disk
```

In the output above *sdb* is the new iSCSI disk. Remember this is just an example; the output you see on your screen will vary.

Next, create a partition, format the file system, and mount the new iSCSI disk. In a terminal enter:

```
sudo fdisk /dev/sdb
n
p
enter
w
```

The above commands are from inside the fdisk utility; see **man fdisk** for more detailed instructions. Also, the cfdisk utility is sometimes more user friendly.

Now format the file system and mount it to `/srv` as an example:

```
sudo mkfs.ext4 /dev/sdb1
sudo mount /dev/sdb1 /srv
```

Finally, add an entry to `/etc/fstab` to mount the iSCSI drive during boot:

```
/dev/sdb1       /srv        ext4    defaults,auto,_netdev 0 0
```

It is a good idea to make sure everything is working as expected by rebooting the server.

3.3. References

Open-iSCSI Website[5]

Debian Open-iSCSI page[6]

[5] http://www.open-iscsi.com/

[6] http://wiki.debian.org/SAN/iSCSI/open-iscsi

4. 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.

4.1. Installation

To install CUPS on your Ubuntu computer, simply use sudo with the apt 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 install cups
```

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.

4.2. 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 add or 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
```

- **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
```

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 systemctl restart cups.service
```

4.3. Web Interface

CUPS can be configured and monitored using a web interface, which by default is available at *http://localhost:631/admin*. The web interface can be used to perform all printer management tasks.

In order to perform administrative tasks via the web interface, you must either have the root account enabled on your server, or authenticate as a user in the *lpadmin* group. For security reasons, CUPS won't authenticate a user that doesn't have a password.

To add a user to the *lpadmin* group, run at the terminal prompt:

```
sudo usermod -aG lpadmin username
```

Further documentation is available in the *Documentation/Help* tab of the web interface.

4.4. References

CUPS Website[7]

Debian Open-iSCSI page[8]

[7] http://www.cups.org/

[8] http://wiki.debian.org/SAN/iSCSI/open-iscsi

Chapter 15. 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).

This guide does not cover setting up Postfix *Virtual Domains*, for information on Virtual Domains and other advanced configurations see *Section 1.7.4, “References” [p. 266]*.

1.1. Installation

To install postfix run the following command:

```
sudo apt 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]/128 192.168.0.0/24
- 0
- +
- all

Replace mail.example.com with the domain for which you'll accept email, 192.168.0.0/24 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'
sudo postconf -e 'smtpd_sasl_local_domain ='
sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
sudo postconf -e 'broken_sasl_auth_clients = yes'
sudo postconf -e 'smtpd_sasl_auth_enable = yes'
sudo postconf -e 'smtpd_recipient_restrictions = \
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
```

The *smtpd_sasl_path* configuration is a path relative to the Postfix queue directory.

2. Next, generate or obtain a digital certificate for TLS. See *Section 5, “Certificates” [p. 195]* for details. This example also uses a Certificate Authority (CA). For information on generating a CA certificate see *Section 5.5, “Certification Authority” [p. 197]*.

MUAs connecting to your mail server via TLS will need to recognize the certificate used for TLS. This can either be done using a certificate from a commercial CA or with a self-signed certificate that users manually install/accept. For MTA to MTA TLS certficates are never validated without advance agreement from the affected organizations. For MTA to MTA TLS, unless local policy requires it, there is no reason not to use a self-signed certificate. Refer to *Section 5.3, “Creating a Self-Signed Certificate” [p. 197]* for more details.

3. Once you have a certificate, configure Postfix to provide TLS encryption for both incoming and outgoing mail:

```
sudo postconf -e 'smtp_tls_security_level = may'
sudo postconf -e 'smtpd_tls_security_level = may'
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
sudo postconf -e 'smtpd_tls_key_file = /etc/ssl/private/server.key'
sudo postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/server.crt'
sudo postconf -e 'smtpd_tls_loglevel = 1'
sudo postconf -e 'smtpd_tls_received_header = yes'
sudo postconf -e 'myhostname = mail.example.com'
```

4. If you are using your own *Certificate Authority* to sign the certificate enter:

   ```
   sudo postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'
   ```

   Again, for more details about certificates see *Section 5, “Certificates” [p. 195]*.

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:

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete
# version

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

myhostname = server1.example.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = server1.example.com, localhost.example.com, localhost
relayhost =
mynetworks = 127.0.0.0/8
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
smtpd_sasl_local_domain =
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject _unauth_destination
smtpd_tls_auth_only = no
smtp_tls_security_level = may
smtpd_tls_security_level = may
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/ssl/private/smtpd.key
smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt
smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
```

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

```
sudo systemctl restart postfix.service
```

Postfix supports SMTP-AUTH as defined in *RFC2554*[1]. It is based on *SASL*[2]. 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-core package will need to be installed. From a terminal prompt enter the following:

```
sudo apt install dovecot-core
```

Next you will need to edit `/etc/dovecot/conf.d/10-master.conf`. Change the following:

```
service auth {
  # auth_socket_path points to this userdb socket by default. It's typically
  # used by dovecot-lda, doveadm, possibly imap process, etc. Its default
  # permissions make it readable only by root, but you may need to relax these
  # permissions. Users that have access to this socket are able to get a list
  # of all usernames and get results of everyone's userdb lookups.
  unix_listener auth-userdb {
    #mode = 0600
    #user =
    #group =
  }

  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
  }
```

In order to let Outlook clients use SMTP-AUTH, in the *authentication mechanisms* section of /etc/dovecot/conf.d/10-auth.conf change this line:

```
auth_mechanisms = plain
```

To this:

```
auth_mechanisms = plain login
```

Once you have Dovecot configured restart it with:

[1] http://www.ietf.org/rfc/rfc2554.txt
[2] http://www.ietf.org/rfc/rfc2222.txt

```
sudo systemctl restart dovecot.service
```

1.5. Mail-Stack Delivery

Another option for configuring Postfix for SMTP-AUTH is using the mail-stack-delivery package (previously packaged as dovecot-postfix). This package will install Dovecot and configure Postfix to use it for both SASL authentication and as a Mail Delivery Agent (MDA). The package also configures Dovecot for IMAP, IMAPS, POP3, and POP3S.

You may or may not want to run IMAP, IMAPS, POP3, or POP3S on your mail server. For example, if you are configuring your server to be a mail gateway, spam/virus filter, etc. If this is the case it may be easier to use the above commands to configure Postfix for SMTP-AUTH.

To install the package, from a terminal prompt enter:

```
sudo apt install mail-stack-delivery
```

You should now have a working mail server, but there are a few options that you may wish to further customize. For example, the package uses the certificate and key from the ssl-cert package, and in a production environment you should use a certificate and key generated for the host. See *Section 5, “Certificates” [p. 195]* for more details.

Once you have a customized certificate and key for the host, change the following options in `/etc/postfix/main.cf`:

```
smtpd_tls_cert_file = /etc/ssl/certs/ssl-mail.pem
smtpd_tls_key_file = /etc/ssl/private/ssl-mail.key
```

Then restart Postfix:

```
sudo systemctl restart postfix.service
```

1.6. 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
```

1.7. Troubleshooting

This section introduces some common ways to determine the cause if problems arise.

1.7.1. 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 systemctl restart postfix.service
```

1.7.2. Smtps

If you need smtps, edit `/etc/postfix/master.cf` and uncomment the following line:

```
smtps     inet  n       -       -       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
```

1.7.3. 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 systemctl reload postfix.service**

- To increase the amount of information logged when troubleshooting *SASL* issues you can set the following options in `/etc/dovecot/conf.d/10-logging.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 systemctl reload dovecot.service**.

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.

1.7.4. 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*[3]. You can also post a message to one of the *Web Forums*[4].

For in depth Postfix information Ubuntu developers highly recommend: *The Book of Postfix*[5].

[3] http://freenode.net
[4] http://www.ubuntu.com/support/community/webforums
[5] http://www.postfix-book.com/

Finally, the *Postfix*[6] website also has great documentation on all the different configuration options available.

Also, the *Ubuntu Wiki Postfix*[7] page has more information.

[6] http://www.postfix.org/documentation.html

[7] https://help.ubuntu.com/community/Postfix

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 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 favorite 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 systemctl start exim4.service
```

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
```

Additionally, in order for outside mail client to be able to connect to new exim server, new user needs to be added into exim by using the following commands.

```
sudo /usr/share/doc/exim4-base/examples/exim-adduser
```

Users should protect the new exim password files with the following commands.

```
sudo chown root:Debian-exim /etc/exim4/passwd
sudo chmod 640 /etc/exim4/passwd
```

Finally, update the Exim4 configuration and restart the service:

```
sudo update-exim4.conf
sudo systemctl restart exim4.service
```

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 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 systemctl start saslauthd.service
```

Exim4 is now configured with SMTP-AUTH using TLS and SASL authentication.

2.5. References

- See *exim.org*[8] for more information.
- There is also an *Exim4 Book*[9] available.
- Another resource is the *Exim4 Ubuntu Wiki* [10] page.

[8] http://www.exim.org/
[9] http://www.uit.co.uk/content/exim-smtp-mail-server
[10] https://help.ubuntu.com/community/Exim4

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 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*[11] and *IMAP*[12].

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*[13].

Once you have chosen your mailbox type, edit the file `/etc/dovecot/conf.d/10-mail.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 systemctl restart dovecot.service
```

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:

[11] http://en.wikipedia.org/wiki/POP3
[12] http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol
[13] http://wiki2.dovecot.org/MailboxFormat

```
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/conf.d/10-ssl.conf` and amend following lines:

```
ssl = yes
ssl_cert = </etc/ssl/certs/dovecot.pem
ssl_key = </etc/ssl/private/dovecot.pem
```

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. 195]* 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/conf.d/10-ssl.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

3.5. References

- See the *Dovecot website*[14] for more information.
- Also, the *Dovecot Ubuntu Wiki*[15] page has more details.

[14] http://www.dovecot.org/

[15] https://help.ubuntu.com/community/Dovecot

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*[16]) 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, using 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 *Section 1.1, “Installation” [p. 211]* for details.

4.1.2. Postfix

For instructions on installing and configuring Postfix refer to *Section 1, “Postfix” [p. 260]*

4.1.3. Exim4

To install Exim4 refer to *Section 2, “Exim4” [p. 268]*.

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:

```
sudo apt install mailman
```

[16] http://lists.ubuntu.com

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 systemctl restart apache2.service
```

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 systemctl restart postfix.service
```

4.2.3. Exim4

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

```
sudo systemctl start exim4.service
```

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*[17] 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"
# 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
```

[17] http://www.exim.org

```
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 systemctl start mailman.service
```

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.

The Exim4 does not use the above aliases to forward mails to Mailman, as it uses a *discover* approach. To suppress the aliases while creating the list, you can add *MTA=None* line in Mailman configuration file, `/etc/mailman/mm_cfg.py`.

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[18]

HOWTO - Using Exim 4 and Mailman 2.1 together[19]

Also, see the *Mailman Ubuntu Wiki*[20] page.

[18] http://www.list.org/mailman-install/index.html
[19] http://www.exim.org/howto/mailman21.html
[20] https://help.ubuntu.com/community/Mailman

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 opendkim 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.
- opendkim 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 opendkim 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. 260]* for instructions on installing and configuring Postfix.

To install the rest of the applications enter the following from a terminal prompt:

```
sudo apt install amavisd-new spamassassin clamav-daemon
sudo apt install opendkim postfix-policyd-spf-python
```

There are some optional packages that integrate with Spamassassin for better spam detection:

```
sudo apt install pyzor razor
```

Along with the main filtering applications compression utilities are needed to process some email attachments:

```
sudo apt install arj cabextract cpio lha nomarch pax rar unrar unzip zip
```

If some packages are not found, check that the *multiverse* repository is enabled in `/etc/apt/sources.list`

If you make changes to the file, be sure to run **sudo apt update** before trying to install again.

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
sudo adduser amavis clamav
```

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 systemctl start spamassassin.service
```

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. The default behaviour is to instead discard. This is configured in `/etc/amavis/conf.d/20-debian_defaults` where *$final_spam_destiny* is set to D_DISCARD rather than D_BOUNCE.

Additionally, you may want to adjust the following options to flag more messages as spam:

```
$sa_tag_level_deflt = -999; # add spam info headers if at, or above that level
$sa_tag2_level_deflt = 6.0; # add 'spam detected' headers at that level
$sa_kill_level_deflt = 21.0; # triggers spam evasive actions
$sa_dsn_cutoff_level = 4; # spam level beyond which a DSN is not sent
```

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" );
```

If you want to cover multiple domains you can use the following in the`/etc/amavis/conf.d/50-user`

```
@local_domains_acl = qw(.);
```

After configuration Amavisd-new needs to be restarted:

```
sudo systemctl restart amavis.service
```

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 systemctl restart amavis.service
```

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,no_milters
```

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 systemctl restart postfix.service
```

Content filtering with spam and virus detection is now enabled.

5.2.5. Amavisd-new and Spamassassin

When integrating Amavisd-new with Spamassassin, if you choose to disable the bayes filtering by editing `/etc/spamassassin/local.cf` and use cron to update the nightly rules, the result can cause a situation where a large amount of error messages are sent to the *amavis* user via the amavisd-new cron job.

There are several ways to handle this situation:

- Configure your MDA to filter messages you do not wish to see.
- Change `/usr/sbin/amavisd-new-cronjob` to check for *use_bayes 0*. For example, edit `/usr/sbin/amavisd-new-cronjob` and add the following to the top before the *test* statements:

```
  egrep -q "^[ \t]*use_bayes[ \t]*0" /etc/spamassassin/local.cf && exit 0
```

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] ESMTP 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 1.7, “Troubleshooting” [p. 265]* 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*[21]
- *ClamAV Documentation*[22] and *ClamAV Wiki*[23]
- *Spamassassin Wiki*[24]
- *Pyzor Homepage*[25]
- *Razor Homepage*[26]

[21] http://www.ijs.si/software/amavisd/amavisd-new-docs.html
[22] http://www.clamav.net/doc/latest/html/
[23] http://wiki.clamav.net/Main/WebHome
[24] http://wiki.apache.org/spamassassin/
[25] http://sourceforge.net/apps/trac/pyzor/
[26] http://razor.sourceforge.net/

- *DKIM.org*[27]
- *Postfix Amavis New*[28]

Also, feel free to ask questions in the *#ubuntu-server* IRC channel on *freenode*[29].

[27] http://dkim.org/
[28] https://help.ubuntu.com/community/PostfixAmavisNew
[29] http://freenode.net

Chapter 16. Chat Applications

1. Overview

In this section, we will discuss how to install and configure a IRC server, ircd-irc2. We will also discuss how to install and configure Jabber, an instance messaging server.

2. IRC Server

The Ubuntu repository has many Internet Relay Chat servers. This section explains how to install and configure the original IRC server ircd-irc2.

2.1. Installation

To install ircd-irc2, run the following command in the command prompt:

```
sudo apt install ircd-irc2
```

The configuration files are stored in `/etc/ircd` directory. The documents are available in `/usr/share/doc/ircd-irc2` directory.

2.2. Configuration

The IRC settings can be done in the configuration file `/etc/ircd/ircd.conf`. You can set the IRC host name in this file by editing the following line:

```
M:irc.localhost::Debian ircd default configuration::000A
```

Please make sure you add DNS aliases for the IRC host name. For instance, if you set irc.livecipher.com as IRC host name, please make sure irc.livecipher.com is resolvable in your Domain Name Server. The IRC host name should not be same as the host name.

The IRC admin details can be configured by editing the following line:

```
A:Organization, IRC dept.:Daemon <ircd@example.irc.org>:Client Server::IRCnet:
```

You should add specific lines to configure the list of IRC ports to listen on, to configure Operator credentials, to configure client authentication, etc. For details, please refer to the example configuration file `/usr/share/doc/ircd-irc2/ircd.conf.example.gz`.

The IRC banner to be displayed in the IRC client, when the user connects to the server can be set in `/etc/ircd/ircd.motd` file.

After making necessary changes to the configuration file, you can restart the IRC server using following command:

```
sudo systemctl restart ircd-irc2.service
```

2.3. References

You may also be interested to take a look at other IRC servers available in Ubuntu Repository. It includes, ircd-ircu and ircd-hybrid.

- Refer to *IRCD FAQ*[1] for more details about the IRC Server.

[1] http://www.irc.org/tech_docs/ircnet/faq.html

3. Jabber Instant Messaging Server

Jabber a popular instant message protocol is based on XMPP, an open standard for instant messaging, and used by many popular applications. This section covers setting up a *Jabberd 2* server on a local LAN. This configuration can also be adapted to providing messaging services to users over the Internet.

3.1. Installation

To install jabberd2, in a terminal enter:

```
sudo apt install jabberd2
```

3.2. Configuration

A couple of XML configuration files will be used to configure jabberd2 for *Berkeley DB* user authentication. This is a very simple form of authentication. However, jabberd2 can be configured to use LDAP, MySQL, PostgreSQL, etc for for user authentication.

First, edit `/etc/jabberd2/sm.xml` changing:

```
<id>jabber.example.com</id>
```

Replace *jabber.example.com* with the hostname, or other id, of your server.

Now in the <storage> section change the <driver> to:

```
<driver>db</driver>
```

Next, edit `/etc/jabberd2/c2s.xml` in the <*local*> section change:

```
<id>jabber.example.com</id>
```

And in the <authreg> section adjust the <module> section to:

```
<module>db</module>
```

Finally, restart jabberd2 to enable the new settings:

```
sudo systemctl restart jabberd2.service
```

You should now be able to connect to the server using a Jabber client like Pidgin for example.

The advantage of using Berkeley DB for user data is that after being configured no additional maintenance is required. If you need more control over user accounts and credentials another authentication method is recommended.

3.3. References

- The *Jabberd2 Web Site*[2] contains more details on configuring Jabberd2.
- For more authentication options see the *Jabberd2 Install Guide*[3].
- Also, the *Setting Up Jabber Server Ubuntu Wiki*[4] page has more information.

[2] http://codex.xiaoka.com/wiki/jabberd2:start
[3] http://www.jabberdoc.org/
[4] https://help.ubuntu.com/community/SettingUpJabberServer

Chapter 17. 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 bzr:

```
sudo apt install bzr
```

1.2. Configuration

To introduce yourself to bzr, use the *whoami* command like this:

```
$ bzr whoami 'Joe Doe <joe.doe@gmail.com>'
```

1.3. Learning Bazaar

Bazaar comes with bundled documentation installed into /usr/share/doc/bzr/html by default. The tutorial is a good place to start. The bzr command also comes with built-in help:

```
$ bzr help
```

To learn more about the *foo* command:

```
$ bzr 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. Git

Git is an open source distributed version control system originally developped by Linus Torvalds to support the development of the linux kernel. Every Git working directory is a full-fledged repository with complete history and full version tracking capabilities, not dependent on network access or a central server.

2.1. Installation

The git version control system is installed with the following command

```
sudo apt install git
```

2.2. Configuration

Every git user should first introduce himself to git, by running these two commands:

```
git config --global user.email "you@example.com"
git config --global user.name "Your Name"
```

2.3. Basic usage

The above is already sufficient to use git in a distributed and secure way, provided users have access to the machine assuming the server role via SSH. On the server machine, creating a new repository can be done with:

```
git init --bare /path/to/repository
```

This creates a bare repository, that cannot be used to edit files directly. If you would rather have a working copy of the contents of the repository on the server, ommit the *--bare* option.

Any client with SSH access to the machine can then clone the repository with:

```
git clone username@hostname:/path/to/repository
```

Once cloned to the client's machine, the client can edit files, then commit and share them with:

```
cd /path/to/repository
#(edit some files
git commit -a # Commit all changes to the local version of the repository
git push origin master # Push changes to the server's version of the repository
```

2.4. Installing a gitolite server

While the above is sufficient to create, clone and edit repositories, users wanting to install git on a server will most likely want to have git work like a more traditional source control management server, with multiple users and access rights management. The suggested solution is to install gitolite with the following command:

```
sudo apt install gitolite
```

2.5. Gitolite configuration

Configuration of the gitolite server is a little different that most other servers on Unix-like systems. Instead of the traditional configuration files in /etc/, gitolite stores its configuration in a git repository. The first step to configuring a new installation is therefore to allow access to the configuration repository.

First of all, let's create a user for gitolite to be accessed as.

```
sudo adduser --system --shell /bin/bash --group --disabled-password --home /home/git git
```

Now we want to let gitolite know about the repository administrator's public SSH key. This assumes that the current user is the repository administrator. If you have not yet configured an SSH key, refer to *Section 1.4, “SSH Keys” [p. 102]*

```
cp ~/.ssh/id_rsa.pub /tmp/$(whoami).pub
```

Let's switch to the git user and import the administrator's key into gitolite.

```
sudo su - git
gl-setup /tmp/*.pub
```

Gitolite will allow you to make initial changes to its configuration file during the setup process. You can now clone and modify the gitolite configuration repository from your administrator user (the user whose public SSH key you imported). Switch back to that user, then clone the configuration repository:

```
exit
git clone git@$IP_ADDRESS:gitolite-admin.git
cd gitolite-admin
```

The gitolite-admin contains two subdirectories, "conf" and "keydir". The configuration files are in the conf dir, and the keydir directory contains the list of user's public SSH keys.

2.6. Managing gitolite users and repositories

Adding new users to gitolite is simple: just obtain their public SSH key and add it to the keydir directory as $DESIRED_USER_NAME.pub. Note that the gitolite usernames don't have to match the system usernames - they are only used in the gitolite configuration file to manage access control. Similarly, users are deleted by deleting their public key file. After each change, do not forget to commit the changes to git, and push the changes back to the server with

```
git commit -a
git push origin master
```

Repositories are managed by editing the conf/gitolite.conf file. The syntax is space separated, and simply specifies the list of repositories followed by some access rules. The following is a default example

```
repo    gitolite-admin
        RW+     =   admin
        R       =   alice

repo    project1
        RW+     =   alice
        RW      =   bob
        R       =   denise
```

2.7. Using your server

To use the newly created server, users have to have the gitolite admin import their public key into the gitolite configuration repository, they can then access any project they have access to with the following command:

```
git clone git@$SERVER_IP:$PROJECT_NAME.git
```

Or add the server's project as a remote for an existing git repository:

```
git remote add gitolite git@$SERVER_IP:$PROJECT_NAME.git
```

3. 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.

3.1. 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 install subversion apache2 libapache2-svn
```

3.2. 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.

3.2.1. Create Subversion Repository

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

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

3.2.2. 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
```

3.3. 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 17.1. 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].

3.3.1. 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.

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

To access the Subversion repository via WebDAV protocol, you must configure your Apache 2 web server. Add the following snippet between the <*VirtualHost*> and </*VirtualHost*> elements in `/etc/apache2/sites-available/000-default.conf`, or another VirtualHost file:

```
<Location /svn>
 DAV svn
 SVNParentPath /path/to/repos
 AuthType Basic
```

[3] http://svnbook.red-bean.com/

```
  AuthName "Your repository name"
  AuthUserFile /etc/subversion/passwd
  Require valid-user
</Location>
```

The above configuration snippet assumes that Subversion repositories are created under `/path/to/repos` directory using **svnadmin** command and that the HTTP user has sufficent access rights to the files (see below). They can be accessible using **http://hostname/svn/repos_name** url.

Changing the apache configuration like the above requires to reload the service with the following command

```
sudo systemctl reload apache2.service
```

To import or commit files to your Subversion repository over HTTP, the repository should be owned by the HTTP user. In Ubuntu systems, 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 that will contain user authentication details. To create a file issue the following command at a command prompt (which will create the file and add the first user):

```
sudo htpasswd -c /etc/subversion/passwd user_name
```

To add additional users omit the *"-c"* option as this option replaces the old file. Instead use this form:

```
sudo htpasswd /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.

3.3.3. 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. To use SSL with Subversion add the above Apache2 configuration to `/etc/apache2/sites-available/default-ssl.conf`. For more information on setting up Apache2 with SSL see *Section 1.3, "HTTPS Configuration" [p. 216]*.

You can install a digital certificate issued by a signing authority. 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.

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

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

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

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

```
username = password
```

For more details, please refer to the file.

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

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

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

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

```
svn co svn://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
```

3.3.5. Access via custom protocol with SSH encryption (svn+ssh://)

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

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

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

```
svn co svn+ssh://ssh_username@hostname/path/to/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.

4. References

- *Bazaar Home Page*[4]
- *Launchpad*[5]
- *Git homepage*[6]
- *Gitolite*[7]
- *Subversion Home Page*[8]
- *Subversion Book*[9]
- *Easy Bazaar Ubuntu Wiki page*[10]
- *Ubuntu Wiki Subversion page*[11]

[4] http://bazaar.canonical.com/en/
[5] https://launchpad.net/
[6] http://git-scm.com
[7] https://github.com/sitaramc/gitolite
[8] http://subversion.apache.org/
[9] http://svnbook.red-bean.com/
[10] https://help.ubuntu.com/community/EasyBazaar
[11] https://help.ubuntu.com/community/Subversion

Chapter 18. Samba

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. 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 File and Print Server” [p. 310]*.

2.1. Installation

The first step is to install the samba package. From a terminal prompt enter:

```
sudo apt 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 number 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.

[2] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

- *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:* determines if the share is read only or if write privileges are granted. Write privileges are allowed only when the value is *no*, as is seen in this example. If the value is *yes*, then access to the share is read only.
- *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.

4. Finally, restart the samba services to enable the new configuration:

```
sudo systemctl restart smbd.service nmbd.service
```

Once again, the above configuration gives all access to any client on the local network. For a more secure configuration see *Section 4, “Securing File and Print Server” [p. 310]*.

From a Windows client you should now be able to browse to the Ubuntu file server and see the shared directory. If your client doesn't show your share automatically, try to access your server by its IP address, e.g. \\192.168.1.1, in a Windows Explorer window. 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.

The file share named *"[share]"* and the path `/srv/samba/share` are just examples. Adjust the share and path names to fit your environment. It is a good idea to name a share after a directory on the file system. Another example would be a share name of *[qa]* with a path of `/srv/samba/qa`.

2.3. Resources

- For in depth Samba configurations see the *Samba HOWTO Collection*[4]

[3] http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM
[4] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

- The guide is also available in *printed format*[5].
- O'Reilly's *Using Samba*[6] is another good reference.
- The *Ubuntu Wiki Samba* [7] page.

[5] http://www.amazon.com/exec/obidos/tg/detail/-/0131882228
[6] http://www.oreilly.com/catalog/9780596007690/
[7] https://help.ubuntu.com/community/Samba

3. 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, “File Server” [p. 305]* 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 File and Print Server” [p. 310]*.

3.1. Installation

Before installing and configuring Samba it is best to already have a working CUPS installation. See *Section 4, “CUPS - Print Server” [p. 256]* for details.

To install the samba package, from a terminal enter:

```
sudo apt 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 *user*:

```
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 Samba:

```
sudo systemctl restart smbd.service nmbd.service
```

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*[8]
- The guide is also available in *printed format*[9].

[8] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/
[9] http://www.amazon.com/exec/obidos/tg/detail/-/0131882228

- O'Reilly's *Using Samba*[10] is another good reference.
- Also, see the *CUPS Website*[11] for more information on configuring CUPS.
- The *Ubuntu Wiki Samba* [12] page.

[10] http://www.oreilly.com/catalog/9780596007690/
[11] http://www.cups.org/
[12] https://help.ubuntu.com/community/Samba

4. Securing 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-winbind 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, “As a Domain Controller” [p. 315]* for further information.
- *security = ADS:* allows the Samba server to join an Active Directory domain as a native member. See *Section 6, “Active Directory Integration” [p. 319]* 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*[13] 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, “File Server” [p. 305]* and *Section 3, “Print Server” [p. 308]*, to require authentication.

First, install the libpam-winbind package which will sync the system users to the Samba user database:

```
sudo apt install libpam-winbind
```

If you chose the *Samba Server* task during installation libpam-winbind 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:

[13] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html#id349531

```
sudo systemctl restart smbd.service nmbd.service
```

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. 178]*.

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 systemctl restart smbd.service nmbd.service
```

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. 191]*.

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 install apparmor-profiles apparmor-utils
```

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*[14]
- The guide is also available in *printed format*[15].
- O'Reilly's *Using Samba*[16] is also a good reference.
- *Chapter 18*[17] of the Samba HOWTO Collection is devoted to security.
- For more information on Samba and ACLs see the *Samba ACLs page* [18].

[14] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/
[15] http://www.amazon.com/exec/obidos/tg/detail/-/0131882228
[16] http://www.oreilly.com/catalog/9780596007690/
[17] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/securing-samba.html
[18] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/AccessControls.html#id397568

- The *Ubuntu Wiki Samba* [19] page.

[19] https://help.ubuntu.com/community/Samba

5. 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-winbind to sync the user accounts, by entering the following in a terminal prompt:

   ```
   sudo apt install samba libpam-winbind
   ```

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 (the last line has been split to fit the format of this document):

   ```
   domain logons = yes
   logon path = \\%N\%U\profile
   logon drive = H:
   logon home = \\%N\%U
   logon script = logon.cmd
   add machine script = sudo /usr/sbin/useradd -N -g machines -c Machine -d
         /var/lib/samba -s /bin/false %u
   ```

   

   If you wish to not use *Roaming Profiles* leave the *logon home* and *logon path* options commented.

   - *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. 178]* for details.

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*[20] 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. Restart Samba to enable the new domain controller:

```
sudo systemctl restart smbd.service nmbd.service
```

8. Lastly, there are a few additional commands needed to setup the appropriate rights.

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:

[20] http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM

```
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.

If the user does not have Samba credentials yet, you can add them with the smbpasswd utility, change the *sysadmin* username appropriately:

```
sudo smbpasswd -a sysadmin
```

Also, rights need to be explicitly provided to the *Domain Admins* group to allow the *add machine script* (and other admin functions) to work. This is achieved by executing:

```
net rpc rights grant -U sysadmin "EXAMPLE\Domain Admins" SeMachineAccountPrivilege \
SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege \
SeRemoteShutdownPrivilege
```

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 *passdb 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. 137]* for details.

1. First, install samba and libpam-winbind. From a terminal enter:

```
sudo apt install samba libpam-winbind
```

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 systemctl restart smbd.service nmbd.service
```

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*[21]
- The guide is also available in *printed format*[22].
- O'Reilly's *Using Samba*[23] is also a good reference.
- *Chapter 4*[24] of the Samba HOWTO Collection explains setting up a Primary Domain Controller.
- *Chapter 5*[25] of the Samba HOWTO Collection explains setting up a Backup Domain Controller.
- The *Ubuntu Wiki Samba* [26] page.

[21] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/
[22] http://www.amazon.com/exec/obidos/tg/detail/-/0131882228
[23] http://www.oreilly.com/catalog/9780596007690/
[24] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-pdc.html
[25] http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-bdc.html
[26] https://help.ubuntu.com/community/Samba

6. 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 the *Likewise Open documentation*[27].

Once part of the Active Directory domain, enter the following command in the terminal prompt:

```
sudo apt install samba cifs-utils smbclient
```

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 systemctl restart smbd.service nmbd.service
```

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 File and Print Server" [p. 310]* 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:

[27] http://www.beyondtrust.com/Technical-Support/Downloads/files/pbiso/Manuals/ubuntu-active-directory.html

```
//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.

6.3. Resources

For more smbclient options see the man page: **man smbclient**, also available *online*[28].

The mount.cifs *man page*[29] is also useful for more detailed information.

The *Ubuntu Wiki Samba* [30] page.

[28] http://manpages.ubuntu.com/manpages/xenial/en/man1/smbclient.1.html
[29] http://manpages.ubuntu.com/manpages/xenial/en/man8/mount.cifs.8.html
[30] https://help.ubuntu.com/community/Samba

Chapter 19. Backups

There are many ways to backup an Ubuntu installation. The most important thing about backups is to develop a *backup plan* consisting of what to backup, where to back 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 pass those directories as arguments to the tar utility, which creates 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, thus 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/bash
####################################
#
# 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 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. 251]* for details of 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:* output to an 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; however there are many options that can be included in such a script. See *Section 1.4, "References" [p. 325]* 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. The file must be made executable:

```
chmod u+x backup.sh
```

Then from a terminal prompt:

```
sudo ./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. 325]*.

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 type:

```
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 snapshot utility used to create copies of an entire file system.
  - *rsync*[9]: a flexible utility used to create incremental copies of files.

[1] http://tldp.org/LDP/abs/html/
[2] http://safari.samspublishing.com/0672323583
[3] https://help.ubuntu.com/community/CronHowto
[4] http://www.gnu.org/software/tar/manual/index.html
[5] http://en.wikipedia.org/wiki/Backup_rotation_scheme
[6] http://www.gnu.org/software/cpio/
[7] http://www.gnu.org/software/coreutils/
[8] http://www.rsnapshot.org/
[9] http://www.samba.org/ftp/rsync/rsync.html

2. Archive Rotation

The shell script in *Section 1, “Shell Scripts” [p. 322]* 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 complex 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. 323]*.

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-effective 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 an NFS share. Using a tape drive simplifies archive rotation, and makes taking the media off-site easier as well.

When using a tape drive, the filename portions of the script aren't needed because the data 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 OS X - 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 backup locations:

- 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

If using MySQL or PostgreSQL as your database, you should already have the services available. Bacula will not install them for you.

There are multiple packages containing the different Bacula components. To install Bacula, from a terminal prompt enter:

```
sudo apt 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. 230]* 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 systemctl restart bacula-sd.service
```

- 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 = "Cv70F6pf1t6pBopT4vQOnigDrR0v3LT3Cgkiyjc"
  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 an 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 *Bacula's Documentation*[10].
- The *Bacula Home Page*[11] contains the latest Bacula news and developments.
- Also, see the *Bacula Ubuntu Wiki*[12] page.

[10] http://blog.bacula.org/documentation/documentation/
[11] http://www.bacula.org/
[12] https://help.ubuntu.com/community/Bacula

Chapter 20. 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. KVM requires virtualization extensions built into Intel and AMD hardware. Xen is also supported on Ubuntu. Xen can take advantage of virtualization extensions, when available, but can also be used on hardware without virtualization extensions. Qemu is another popular solution for hardware without virtualization extensions.

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:

```
kvm-ok
```

A message will be printed informing you if your CPU *does* or *does not* support hardware virtualization.

On many computers with processors supporting hardware assisted virtualization, it is necessary to activate an option in the BIOS to enable it.

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 includes *bridging* and *iptables* rules implementing *usermode* networking, which uses the SLIRP protocol. Traffic is NATed through the host interface to the outside network.

To enable external hosts to directly access services on virtual machines a different type of *bridge* than the default 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.

1.2. Installation

To install the necessary packages, from a terminal prompt enter:

```
sudo apt install qemu-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 $USER 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.

In more recent releases (>= Yakkety) the group was renamed to *libvirt*. Upgraded systems get a new *libvirt* group with the same gid as the *libvirtd* group to match that.

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. 340]* 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 uvtool. This application, available as of 14.04, allows you to set up specific VM options, execute custom post-install scripts, etc. For details see *Section 3, “Cloud images and uvtool” [p. 344]*.

Libvirt can also be configured work with Xen. For details, see the Xen Ubuntu community page referenced below.

1.3. virt-install

virt-install is part of the virtinst package. To install it, from a terminal prompt enter:

```
sudo apt install virtinst
```

There are several options available when using virt-install. For example:

```
sudo virt-install -n web_devel -r 256 \
--disk path=/var/lib/libvirt/images/web_devel.img,bus=virtio,size=4 -c \
ubuntu-16.04-server-i386.iso --network network=default,model=virtio \
--graphics vnc,listen=0.0.0.0 --noautoconsole -v
```

- *-n web_devel:* 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 in megabytes.
- *--disk path=/var/lib/libvirt/images/web_devel.img,size=4:* 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` in the /var/lib/libvirt/images/ directory, with a size of 4 gigabytes, and using *virtio* for the disk bus.
- *-c ubuntu-16.04-server-i386.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.
- *--network* provides details related to the VM's network interface. Here the *default* network is used, and the interface model is configured for *virtio*.
- *--graphics vnc,listen=0.0.0.0:* exports the guest's virtual console using VNC and on all host interfaces. Typically servers have no GUI, so another GUI based computer on the Local Area Network (LAN) can connect via VNC to complete the installation.
- *--noautoconsole:* will not automatically connect to the virtual machine's console.
- *-v:* creates a fully virtualized guest.

[1] https://help.ubuntu.com/16.04/installation-guide/

After launching virt-install you can connect to the virtual machine's console either locally using a GUI (if your server has a GUI), or via a remote VNC client from a GUI-based computer.

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
```

- *-o:* original virtual machine.
- *-n:* name of the new virtual machine.
- *-f:* path to the file, logical volume, or partition to be used by the new virtual machine.

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 list
  ```

- To start a virtual machine:

  ```
  virsh start web_devel
  ```

- Similarly, to start a virtual machine at boot:

  ```
  virsh autostart web_devel
  ```

- Reboot a virtual machine with:

  ```
  virsh 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 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 restore web_devel-022708.state
```

- To shutdown a virtual machine do:

```
virsh shutdown web_devel
```

- A CDROM device can be mounted in a virtual machine by entering:

```
virsh 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.

If virsh (or other vir* tools) shall connect to something else than the default qemu-kvm/system hipervisor one can find alternatives for the *connect* option in *man virsh* or *libvirt doc*[2]

1.5.2. migration

There are different types of migration available depending on the versions of libvirt and the hipervisor being used. In general those types are:

- *offline migration*[3]
- *live migration*[4]
- *postcopy migration*[5]

There are various options to those methods, but the entry point for all of them is *virsh migrate*. Read the integrated help for more detail.

```
virsh migrate --help
```

Some useful documentation on constraints and considerations about live migration can be found at the *Ubuntu Wiki*[6]

1.5.3. Device Passthrough / Hotplug

If instead of the here described hotplugging you want to always pass through a device add the xml content of the device to your static guest xml representation via e.g. **virsh edit <guestname>**. In that case you don't need to use *attach/detach*. There are different kinds of passthrough. Types available to you depend on your Hardware and software setup.

- USB hotplug/passthrough
- VF hotplug/Passthrough

[2] http://libvirt.org/uri.html
[3] https://libvirt.org/migration.html#offline
[4] https://libvirt.org/migration.html
[5] http://wiki.qemu.org/Features/PostCopyLiveMigration
[6] https://wiki.ubuntu.com/QemuKVMMigration

But both kinds are handled in a very similar way and while there are various way to do it (e.g. also via qemu monitor) driving such a change via libvirt is recommended. That way libvirt can try to manage all sorts of special cases for you and also somewhat masks version differences.

In general when driving hotplug via libvirt you create a xml snippet that describes the device just as you would do in a static *guest description.*[7] A usb device is usually identified by Vendor/Product id's:

```
<hostdev mode='subsystem' type='usb' managed='yes'>
  <source>
    <vendor id='0x0b6d'/>
    <product id='0x3880'/>
  </source>
</hostdev>
```

Virtual functions are usually assigned via their PCI-ID (domain, bus, slot, function).

```
<hostdev mode='subsystem' type='pci' managed='yes'>
  <source>
    <address domain='0x0000' bus='0x04' slot='0x10' function='0x0'/>
  </source>
</hostdev>
```

To get the Virtual function in the first place is very device dependent and can therefore not be fully covered here. But in general it involves setting up an iommu, registering via *VFIO*[8] and sometimes requesting a number of VFs. Here an example on ppc64el to get 4 VFs on a device:

```
$ sudo modprobe vfio-pci
# identify device
$ lspci -n -s 0005:01:01.3
0005:01:01.3 0200: 10df:e228 (rev 10)
# register and request VFs
$ echo 10df e228 | sudo tee /sys/bus/pci/drivers/vfio-pci/new_id
$ echo 4 | sudo tee /sys/bus/pci/devices/0005\:01\:00.0/sriov_numvfs
```

You then attach or detach the device via libvirt by relating the guest with the xml snippet.

```
virsh attach-device <guestname> <device-xml>
# Use the Device int the Guest
virsh detach-device <guestname> <device-xml>
```

There are several associated known issues in regard to apparmor proetction protecting "too much". You might need to tweak exceptions in the apparmor profiles until the bugs *1552241*[9] (for USB) and *https://bugs.launchpad.net/ubuntu/+source/apparmor/+bug/1679704* (For VF assignment) are resolved. To check if you are affected watch dmesg while you use the USB/VF passthrough/hotplug feature and verify if you see *apparmor denies*[10].

[7] https://libvirt.org/formatdomain.html
[8] https://www.kernel.org/doc/Documentation/vfio.txt
[9] https://bugs.launchpad.net/ubuntu/+source/libvirt/+bug/1552241
[10] http://wiki.apparmor.net/index.php/AppArmor_Failures#Messages_in_the_Log_files

1.5.4. Access Qemu Monitor via libvirt

The *Qemu Monitor*[11] is the way to interact with qemu/KVM while a guest is running. This interface has many and very powerful features for experienced users. When running under libvirt that monitor interface is bound by libvirt itself for management purposes, but a user can run qemu monitor commands via libvirt still. The general syntax is **virsh qemu-monitor-command [options] [guest] 'command'**

Libvirt covers most use cases needed, but if you every want/need to work around libvirt or want to tweak very special options you can e.g. add a device that way:

```
virsh qemu-monitor-command --hmp zesty-test-log 'drive_add 0 if=none,file=/var/lib/libvirt/
images/test.img,format=raw,id=disk1'
```

But since the monitor is so powerful, you can do a lot especially for debugging purposes like showing the guest registers:

```
virsh qemu-monitor-command --hmp y-ipns 'info registers'
RAX=00ffffc000000000 RBX=ffff8f0f5d5c7e48 RCX=0000000000000000 RDX=ffffea00007571c0
RSI=0000000000000000 RDI=ffff8f0fdd5c7e48 RBP=ffff8f0f5d5c7e18 RSP=ffff8f0f5d5c7df8
[...]
```

1.5.5. 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 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. 101]*

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.

[11] https://en.wikibooks.org/wiki/QEMU/Monitor

To install virt-viewer from a terminal enter:

```
sudo apt install virt-viewer
```

Once a virtual machine is installed and running you can connect to the virtual machine's console by using:

```
virt-viewer 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.

1.7. Resources

- See the *KVM*[12] home page for more details.
- For more information on libvirt see the *libvirt home page*[13]
- The *Virtual Machine Manager*[14] site has more information on virt-manager development.
- Also, stop by the *#ubuntu-virt* IRC channel on *freenode*[15] to discuss virtualization technology in Ubuntu.
- Another good resource is the *Ubuntu Wiki KVM*[16] page.
- For information on Xen, including using Xen with libvirt, please see the *Ubuntu Wiki Xen*[17] page.
- For basics how to assign VT-d devices to qemu/KVM, please see the *linux-kvm*[18] page.

[12] http://www.linux-kvm.org/
[13] http://libvirt.org/
[14] http://virt-manager.org/
[15] http://freenode.net/
[16] https://help.ubuntu.com/community/KVM
[17] https://help.ubuntu.com/community/Xen
[18] http://www.linux-kvm.org/page/How_to_assign_devices_with_VT-d_in_KVM#Assigning_the_device

2. Qemu

Qemu[19] is a machine emulator that can run operating systems and programs for one machine on a different machine. Mostly it is not used as emulator but as virtualizer in collaboration with KVM or XEN kernel components. In that case it utilizes the virtualization technology of the hardware to virtualize guests.

While qemu has a *command line interface*[20] and a *monitor*[21] to interact with running guests those is rarely used that way for other means than development purposes. *Libvirt* provides an abstraction from specific versions and hypervisors and encapsulates some workarounds and best practices.

2.1. Upgrading the machine type

This also is documented along some more constraints and considerations at the *Ubuntu Wiki*[22]

You might want to update your machine type of an existing defined guest to:

- to pick up latest security fixes and features
- continue using a guest created on a now unsupported release

In general it is recommended to update machine types when upgrading qemu/kvm to a new major version. But this can likely never be an automated task as this change is guest visible. The guest devices might change in appearance, new features will be announced to the guest and so on. Linux is usually very good at tolerating such changes, but it depends so much on the setup and workload of the guest that this has to be evaluated by the owner/admin of the system. Other operating systems where known to often have severe impacts by changing the hardware. Consider a machine type change similar to replacing all devices and firmware of a physical machine to the latest revision - all considerations that apply there apply to evaluating a machine type upgrade as well.

As usual with major configuration changes it is wise to back up your guest definition and disk state to be able to do a rollback just in case. There is no integrated single command to update the machine type via virsh or similar tools. It is a normal part of your machine definition. And therefore updated the same way as most others.

First shutdown your machine and wait until it has reached that state.

```
virsh shutdown <yourmachine>
# wait
virsh list --inactive
# should now list your machine as "shut off"
```

[19] http://wiki.qemu.org/Main_Page
[20] http://wiki.qemu.org/download/qemu-doc.html#sec_005finvocation
[21] http://wiki.qemu.org/download/qemu-doc.html#pcsys_005fmonitor
[22] https://wiki.ubuntu.com/QemuKVMMigration#Upgrade_machine_type

Then edit the machine definition and find the type in the type tag at the machine attribute.

```
virsh edit <yourmachine>
<type arch='x86_64' machine='pc-i440fx-xenial'>hvm</type>
```

Change this to the value you want. If you need to check what types are available via "-M ?" Note that while providing upstream types as convenience only Ubuntu types are supported. There you can also see what the current default would be. In general it is strongly recommended that you change to newer types if possible to exploit newer features, but also to benefit of bugfixes that only apply to the newer device virtualization.

```
kvm -M ?
# lists machine types, e.g.
pc-i440fx-xenial       Ubuntu 16.04 PC (i440FX + PIIX, 1996) (default)
...
```

After this you can start your guest again. You can check the current machine type from guest and host depending on your needs.

```
virsh start <yourmachine>
# check from host, via dumping the active xml definition
virsh dumpxml <yourmachine> | xmllint --xpath "string(//domain/os/type/@machine)" -
# or from the guest via dmidecode
sudo dmidecode | grep Product -A 1
        Product Name: Standard PC (i440FX + PIIX, 1996)
        Version: pc-i440fx-xenial
```

If you keep non-live definitions around like xml files remember to update those as well.

3. Cloud images and uvtool

3.1. Introduction

With Ubuntu being one of the most used operating systems on many cloud platforms, the availability of stable and secure cloud images has become very important. As of 12.04 the utilization of cloud images outside of a cloud infrastructure has been improved. It is now possible to use those images to create a virtual machine without the need of a complete installation.

3.2. Creating virtual machines using uvtool

Starting with 14.04 LTS, a tool called uvtool greatly facilitates the task of generating virtual machines (VM) using the cloud images. uvtool provides a simple mechanism to synchronize cloud-images locally and use them to create new VMs in minutes.

3.2.1. Uvtool packages

The following packages and their dependencies will be required in order to use uvtool:

- uvtool
- uvtool-libvirt

To install uvtool, run:

```
$ apt -y install uvtool
```

This will install uvtool's main commands:

- uvt-simplestreams-libvirt
- uvt-kvm

3.2.2. Get the Ubuntu Cloud Image with uvt-simplestreams-libvirt

This is one of the major simplifications that uvtool brings. It is aware of where to find the cloud images so only one command is required to get a new cloud image. For instance, if you want to synchronize all cloud images for the amd64 architecture, the uvtool command would be:

```
$ uvt-simplestreams-libvirt sync arch=amd64
```

After an amount of time required to download all the images from the Internet, you will have a complete set of cloud images stored locally. To see what has been downloaded use the following command:

```
$ uvt-simplestreams-libvirt query
release=oneiric arch=amd64 label=release (20130509)
release=precise arch=amd64 label=release (20160315)
release=quantal arch=amd64 label=release (20140409)
release=raring arch=amd64 label=release (20140111)
release=saucy arch=amd64 label=release (20140709)
```

```
release=trusty arch=amd64 label=release (20160314)
release=utopic arch=amd64 label=release (20150723)
release=vivid arch=amd64 label=release (20160203)
release=wily arch=amd64 label=release (20160315)
release=xenial arch=amd64 label=beta1 (20160223.1)
```

In the case where you want to synchronize only one specific cloud-image, you need to use the release= and arch= filters to identify which image needs to be synchronized.

```
$ uvt-simplestreams-libvirt sync release=xenial arch=amd64
```

3.2.3. Create the VM using uvt-kvm

In order to connect to the virtual machine once it has been created, you must have a valid SSH key available for the Ubuntu user. If your environment does not have an SSH key, you can easily create one using the following command:

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ubuntu/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ubuntu/.ssh/id_rsa.
Your public key has been saved in /home/ubuntu/.ssh/id_rsa.pub.
The key fingerprint is:
4d:ba:5d:57:c9:49:ef:b5:ab:71:14:56:6e:2b:ad:9b ubuntu@xenialS
The key's randomart image is:
+--[ RSA 2048]----+
|                ..|
|               o.=|
|           .    **|
|         +    o+=|
|        S . ...=.|
|         o . .+ .|
|        . .  o o |
|              *  |
|             E   |
+-----------------+
```

To create of a new virtual machine using uvtool, run the following in a terminal:

```
$ uvt-kvm create firsttest
```

This will create a VM named **firsttest** using the current LTS cloud image available locally. If you want to specify a release to be used to create the VM, you need to use the **release=** filter:

```
$ uvt-kvm create secondtest release=xenial
```

uvt-kvm wait can be used to wait until the creation of the VM has completed:

```
$ uvt-kvm wait secondttest --insecure
```

```
Warning: secure wait for boot-finished not yet implemented; use --insecure.
```

3.2.4. Connect to the running VM

Once the virtual machine creation is completed, you can connect to it using SSH:

```
$ uvt-kvm ssh secondtest --insecure
```

For the time being, the **--insecure** is required, so use this mechanism to connect to your VM only if you completely trust your network infrastructure.

You can also connect to your VM using a regular SSH session using the IP address of the VM. The address can be queried using the following command:

```
$ uvt-kvm ip secondtest
192.168.122.199
$ ssh -i ~/.ssh/id_rsa ubuntu@192.168.122.199
The authenticity of host '192.168.122.199 (192.168.122.199)' can't be established.
ECDSA key fingerprint is SHA256:8oxaztRWzTMtv8SC9LYyjuqBu79Z9JP8bUGh6G8R8cw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.122.199' (ECDSA) to the list of known hosts.
Welcome to Ubuntu Xenial Xerus (development branch) (GNU/Linux 4.4.0-X-generic ARCH)

 * Documentation:  https://help.ubuntu.com/

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@secondtest:~$
```

3.2.5. Get the list of running VMs

You can get the list of VMs running on your system with this command:

```
$ uvt-kvm list
secondtest
```

3.2.6. Destroy your VM

Once you are done with your VM, you can destroy it with:

```
$ uvt-kvm destroy secondtest
```

3.2.7. More uvt-kvm options

The following options can be used to change some of the characteristics of the VM that you are creating:

- --memory : Amount of RAM in megabytes. Default: 512.
- --disk : Size of the OS disk in gigabytes. Default: 8.
- --cpu : Number of CPU cores. Default: 1.

Some other parameters will have an impact on the cloud-init configuration:

- --password password : Allow login to the VM using the Ubuntu account and this provided password.
- --run-script-once script_file : Run script_file as root on the VM the first time it is booted, but never again.
- --packages package_list : Install the comma-separated packages specified in package_list on first boot.

A complete description of all available modifiers is available in the manpage of uvt-kvm.

3.3. 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*[23]

[23] https://lists.ubuntu.com/mailman/listinfo/ubuntu-server

4. Ubuntu Cloud

Cloud computing is a computing model that allows vast pools of resources to be allocated on-demand. These resources such as storage, computing power, network and software are abstracted and delivered as a service over the Internet anywhere, anytime. These services are billed per time consumed similar to the ones used by public services such as electricity, water and telephony. Ubuntu Cloud Infrastructure uses OpenStack open source software to help build highly scalable, cloud computing for both public and private clouds.

4.1. Installation and Configuration

Due to the current high rate of development of this complex technology we refer the reader to *upstream documentation*[24] for all matters concerning installation and configuration.

4.2. Support and Troubleshooting

Community Support

- *OpenStack Mailing list*[25]
- *The OpenStack Wiki search*[26]
- *Launchpad bugs area*[27]
- Join the IRC channel #openstack on freenode.

4.3. Resources

- *Cloud Computing - Service models*[28]
- *OpenStack Compute*[29]
- *OpenStack Image Service*[30]
- *OpenStack Object Storage Administration Guide*[31]
- *Installing OpenStack Object Storage on Ubuntu*[32]
- *http://cloudglossary.com/*

[24] http://docs.openstack.org/havana/install-guide/install/apt/content/
[25] https://launchpad.net/~openstack
[26] http://wiki.openstack.org
[27] https://bugs.launchpad.net/nova
[28] http://en.wikipedia.org/wiki/Cloud_computing#Service_Models
[29] http://www.openstack.org/software/openstack-compute/
[30] http://docs.openstack.org/diablo/openstack-compute/starter/content/GlanceMS-d2s21.html
[31] http://docs.openstack.org/trunk/openstack-object-storage/admin/content/index.html
[32] http://docs.openstack.org/trunk/openstack-object-storage/admin/content/installing-openstack-object-storage-on-ubuntu.html

5. LXD

LXD (pronounced lex-dee) is the lightervisor, or lightweight container hypervisor. While this claim has been controversial, it has been *quite well justified*[33] based on the original academic paper. It also nicely distinguishes LXD from *LXC*[34].

LXC (lex-see) is a program which creates and administers "containers" on a local system. It also provides an API to allow higher level managers, such as LXD, to administer containers. In a sense, one could compare LXC to QEMU, while comparing LXD to libvirt.

The LXC API deals with a 'container'. The LXD API deals with 'remotes', which serve images and containers. This extends the LXC functionality over the network, and allows concise management of tasks like container migration and container image publishing.

LXD uses LXC under the covers for some container management tasks. However, it keeps its own container configuration information and has its own conventions, so that it is best not to use classic LXC commands by hand with LXD containers. This document will focus on how to configure and administer LXD on Ubuntu systems.

5.1. Online Resources

There is excellent documentation for *getting started with LXD*[35] in the online LXD README. There is also an online server allowing you to *try out LXD remotely*[36]. Stephane Graber also has an *excellent blog series*[37] on LXD 2.0. Finally, there is great documentation on how to *drive lxd using juju*[38].

This document will offer an Ubuntu Server-specific view of LXD, focusing on administration.

5.2. Installation

LXD is pre-installed on Ubuntu Server cloud images. On other systems, the lxd package can be installed using:

```
sudo apt install lxd
```

This will install LXD as well as the recommended dependencies, including the LXC library and lxcfs.

[33] http://blog.dustinkirkland.com/2015/09/container-summit-presentation-and-live.html
[34] https://help.ubuntu.com/lts/serverguide/lxc.html
[35] http://github.com/lxc/lxd
[36] http://linuxcontainers.org/lxd/try-it
[37] https://www.stgraber.org/2016/03/11/lxd-2-0-blog-post-series-012/
[38] https://jujucharms.com/docs/devel/config-LXD

5.3. Kernel preparation

In general, Ubuntu 16.04 should have all the desired features enabled by default. One exception to this is that in order to enable swap accounting the boot argument **swapaccount=1** must be set. This can be done by appending it to the **GRUB_CMDLINE_LINUX_DEFAULT=**variable in /etc/default/grub, then running 'update-grub' as root and rebooting.

5.4. Configuration

By default, LXD is installed listening on a local UNIX socket, which members of group LXD can talk to. It has no trust password setup. And it uses the filesystem at `/var/lib/lxd` to store containers. To configure LXD with different settings, use **lxd init**. This will allow you to choose:

- Directory or *ZFS*[39] container backend. If you choose ZFS, you can choose which block devices to use, or the size of a file to use as backing store.
- Availability over the network
- A 'trust password' used by remote clients to vouch for their client certificate

You must run 'lxd init' as root. 'lxc' commands can be run as any user who is member of group lxd. If user joe is not a member of group 'lxd', you may run:

```
adduser joe lxd
```

as root to change it. The new membership will take effect on the next login, or after running 'newgrp lxd' from an existing login.

For more information on server, container, profile, and device configuration, please refer to the definitive configuration provided with the source code, which can be found *online*[40]

5.5. Creating your first container

This section will describe the simplest container tasks.

5.5.1. Creating a container

Every new container is created based on either an image, an existing container, or a container snapshot. At install time, LXD is configured with the following image servers:

- `ubuntu`: this serves official Ubuntu server cloud image releases.
- `ubuntu-daily`: this serves official Ubuntu server cloud images of the daily development releases.

[39] http://open-zfs.org
[40] https://github.com/lxc/lxd/blob/master/doc/configuration.md

- `images`: this is a default-installed alias for images.linuxcontainers.org. This is serves classical lxc images built using the same images which the LXC 'download' template uses. This includes various distributions and minimal custom-made Ubuntu images. This is not the recommended server for Ubuntu images.

The command to create and start a container is

```
lxc launch remote:image containername
```

Images are identified by their hash, but are also aliased. The 'ubuntu' server knows many aliases such as '16.04' and 'xenial'. A list of all images available from the Ubuntu Server can be seen using:

```
lxc image list ubuntu:
```

To see more information about a particular image, including all the aliases it is known by, you can use:

```
lxc image info ubuntu:xenial
```

You can generally refer to an Ubuntu image using the release name ('xenial') or the release number (16.04). In addition, 'lts' is an alias for the latest supported LTS release. To choose a different architecture, you can specify the desired architecture:

```
lxc image info ubuntu:lts/arm64
```

Now, let's start our first container:

```
lxc launch ubuntu:xenial x1
```

This will download the official current Xenial cloud image for your current architecture, then create a container using that image, and finally start it. Once the command returns, you can see it using:

```
lxc list
lxc info x1
```

and open a shell in it using:

```
lxc exec x1 bash
```

The try-it page gives a full synopsis of the commands you can use to administer containers.

Now that the 'xenial' image has been downloaded, it will be kept in sync until no new containers have been created based on it for (by default) 10 days. After that, it will be deleted.

5.6. LXD Server Configuration

By default, LXD is socket activated and configured to listen only on a local UNIX socket. While LXD may not be running when you first look at the process listing, any LXC command will start it up. For instance:

```
lxc list
```

This will create your client certificate and contact the LXD server for a list of containers. To make the server accessible over the network you can set the http port using:

```
lxc config set core.https_address :8443
```

This will tell LXD to listen to port 8843 on all addresses.

5.6.1. Authentication

By default, LXD will allow all members of group 'lxd' (which by default includes all members of group admin) to talk to it over the UNIX socket. Communication over the network is authorized using server and client certificates.

Before client c1 wishes to use remote r1, r1 must be registered using:

```
lxc remote add r1 r1.example.com:8443
```

The fingerprint of r1's certificate will be shown, to allow the user at c1 to reject a false certificate. The server in turn will verify that c1 may be trusted in one of two ways. The first is to register it in advance from any already-registered client, using:

```
lxc config trust add r1 certfile.crt
```

Now when the client adds r1 as a known remote, it will not need to provide a password as it is already trusted by the server.

The other is to configure a 'trust password' with r1, either at initial configuration using 'lxd init', or after the fact using

```
lxc config set core.trust_password PASSWORD
```

The password can then be provided when the client registers r1 as a known remote.

5.6.2. Backing store

LXD supports several backing stores. The recommended backing store is ZFS, however this is not available on all platforms. Supported backing stores include:

- ext4: this is the default, and easiest to use. With an ext4 backing store, containers and images are simply stored as directories on the host filesystem. Launching new containers requires copying a whole filesystem, and 10 containers will take up 10 times as much space as one container.
- ZFS: if ZFS is supported on your architecture (amd64, arm64, or ppc64le), you can set LXD up to use it using 'lxd init'. If you already have a ZFS pool configured, you can tell LXD to use it by setting the zfs_pool_name configuration key:

  ```
  lxc config set storage.zfs_pool_name lxd
  ```

  With ZFS, launching a new container is fast because the filesystem starts as a copy on write clone of the images' filesystem. Note that unless the container is privileged (see below) LXD will need to change ownership of all files before the container can start, however this is fast and change very little of the actual filesystem data.
- Btrfs: btrfs can be used with many of the same advantages as ZFS. To use BTRFS as a LXD backing store, simply mount a Btrfs filesystem under `/var/lib/lxd`. LXD will detect this and exploit the Btrfs subvolume feature whenever launching a new container or snapshotting a container.
- LVM: To use a LVM volume group called 'lxd', you may tell LXD to use that for containers and images using the command

  ```
  lxc config set storage.lvm_vg_name lxd
  ```

  When launching a new container, its rootfs will start as a lv clone. It is immediately mounted so that the file uids can be shifted, then unmounted. Container snapshots also are created as lv snapshots.

5.7. Container configuration

Containers are configured according to a set of profiles, described in the next section, and a set of container-specific configuration. Profiles are applied first, so that container specific configuration can override profile configuration.

Container configuration includes properties like the architecture, limits on resources such as CPU and RAM, security details including apparmor restriction overrides, and devices to apply to the container.

Devices can be of several types, including UNIX character, UNIX block, network interface, or 'disk'. In order to insert a host mount into a container, a 'disk' device type would be used. For instance, to mount /opt in container c1 at /opt, you could use:

```
lxc config device add c1 opt disk source=/opt path=opt
```

See:

```
lxc help config
```

for more information about editing container configurations. You may also use:

```
lxc config edit c1
```

to edit the whole of c1's configuration in your specified $EDITOR. Comments at the top of the configuration will show examples of correct syntax to help administrators hit the ground running. If the edited configuration is not valid when the $EDITOR is exited, then $EDITOR will be restarted.

5.8. Profiles

Profiles are named collections of configurations which may be applied to more than one container. For instance, all containers created with 'lxc launch', by default, include the 'default' profile, which provides a network interface 'eth0'.

To mask a device which would be inherited from a profile but which should not be in the final container, define a device by the same name but of type 'none':

```
lxc config device add c1 eth1 none
```

5.9. Nesting

Containers all share the same host kernel. This means that there is always an inherent trade-off between features exposed to the container and host security from malicious containers. Containers by default are therefore restricted from features needed to nest child containers. In order to run lxc or lxd containers under a lxd container, the 'security.nesting' feature must be set to true:

```
lxc config set container1 security.nesting true
```

Once this is done, container1 will be able to start sub-containers.

In order to run unprivileged (the default in LXD) containers nested under an unprivileged container, you will need to ensure a wide enough UID mapping. Please see the 'UID mapping' section below.

5.9.1. Docker

In order to facilitate running docker containers inside a LXD container, a 'docker' profile is provided. To launch a new container with the docker profile, you can run:

```
lxc launch xenial container1 -p default -p docker
```

Note that currently the docker package in Ubuntu 16.04 is patched to facilitate running in a container. This support is expected to land upstream soon.

Note that 'cgroup namespace' support is also required. This is available in the 16.04 kernel as well as in the 4.6 upstream source.

5.10. Limits

LXD supports flexible constraints on the resources which containers can consume. The limits come in the following categories:

- CPU: limit cpu available to the container in several ways.
- Disk: configure the priority of I/O requests under load
- RAM: configure memory and swap availability
- Network: configure the network priority under load
- Processes: limit the number of concurrent processes in the container.

For a full list of limits known to LXD, see *the configuration documentation*[41].

[41] https://github.com/lxc/lxd/blob/master/doc/configuration.md

5.11. UID mappings and Privileged containers

By default, LXD creates unprivileged containers. This means that root in the container is a non-root UID on the host. It is privileged against the resources owned by the container, but unprivileged with respect to the host, making root in a container roughly equivalent to an unprivileged user on the host. (The main exception is the increased attack surface exposed through the system call interface)

Briefly, in an unprivileged container, 65536 UIDs are 'shifted' into the container. For instance, UID 0 in the container may be 100000 on the host, UID 1 in the container is 100001, etc, up to 165535. The starting value for UIDs and GIDs, respectively, is determined by the 'root' entry the `/etc/subuid` and `/etc/subgid` files. (See the *subuid(5) manual page*[42].

It is possible to request a container to run without a UID mapping by setting the security.privileged flag to true:

```
lxc config set c1 security.privileged true
```

Note however that in this case the root user in the container is the root user on the host.

5.12. Apparmor

LXD confines containers by default with an apparmor profile which protects containers from each other and the host from containers. For instance this will prevent root in one container from signaling root in another container, even though they have the same uid mapping. It also prevents writing to dangerous, un-namespaced files such as many sysctls and `/proc/sysrq-trigger`.

If the apparmor policy for a container needs to be modified for a container c1, specific apparmor policy lines can be added in the 'raw.apparmor' configuration key.

5.13. Seccomp

All containers are confined by a default seccomp policy. This policy prevents some dangerous actions such as forced umounts, kernel module loading and unloading, kexec, and the open_by_handle_at system call. The seccomp configuration cannot be modified, however a completely different seccomp policy - or none - can be requested using raw.lxc (see below).

5.14. Raw LXC configuration

LXD configures containers for the best balance of host safety and container usability. Whenever possible it is highly recommended to use the defaults, and use the LXD configuration keys to request LXD to modify as needed. Sometimes, however, it may be necessary to talk to the underlying lxc driver itself. This can be done

[42] http://manpages.ubuntu.com/manpages/xenial/en/man5/subuid.5.html

by specifying LXC configuration items in the 'raw.lxc' LXD configuration key. These must be valid items as documented in *the lxc.container.conf(5) manual page*[43].

5.15. Images and containers

LXD is image based. When you create your first container, you will generally do so using an existing image. LXD comes pre-configured with three default image remotes:

- ubuntu: This is a *simplestreams-based*[44] remote serving released ubuntu cloud images.
- ubuntu-daily: This is another simplestreams based remote which serves 'daily' ubuntu cloud images. These provide quicker but potentially less stable images.
- images: This is a remote publishing best-effort container images for many distributions, created using community-provided build scripts.

To view the images available on one of these servers, you can use:

```
lxc image list ubuntu:
```

Most of the images are known by several aliases for easier reference. To see the full list of aliases, you can use

```
lxc image alias list images:
```

Any alias or image fingerprint can be used to specify how to create the new container. For instance, to create an amd64 Ubuntu 14.04 container, some options are:

```
lxc launch ubuntu:14.04 trusty1
lxc launch ubuntu:trusty trusty1
lxc launch ubuntu:trusty/amd64 trusty1
lxc launch ubuntu:lts trusty1
```

The 'lts' alias always refers to the latest released LTS image.

5.15.1. Snapshots

Containers can be renamed and live-migrated using the 'lxc move' command:

```
lxc move c1 final-beta
```

[43] http://manpages.ubuntu.com/manpages/xenial/en/man5/lxc.container.conf.5.html
[44] https://launchpad.net/simplestreams

They can also be snapshotted:

```
lxc snapshot c1 YYYY-MM-DD
```

Later changes to c1 can then be reverted by restoring the snapshot:

```
lxc restore u1 YYYY-MM-DD
```

New containers can also be created by copying a container or snapshot:

```
lxc copy u1/YYYY-MM-DD testcontainer
```

5.15.2. Publishing images

When a container or container snapshot is ready for consumption by others, it can be published as a new image using;

```
lxc publish u1/YYYY-MM-DD --alias foo-2.0
```

The published image will be private by default, meaning that LXD will not allow clients without a trusted certificate to see them. If the image is safe for public viewing (i.e. contains no private information), then the 'public' flag can be set, either at publish time using

```
lxc publish u1/YYYY-MM-DD --alias foo-2.0 public=true
```

or after the fact using

```
lxc image edit foo-2.0
```

and changing the value of the public field.

5.15.3. Image export and import

Image can be exported as, and imported from, tarballs:

```
lxc image export foo-2.0 foo-2.0.tar.gz
lxc image import foo-2.0.tar.gz --alias foo-2.0 --public
```

5.16. Troubleshooting

To view debug information about LXD itself, on a systemd based host use

```
journalctl -u LXD
```

On an Upstart-based system, you can find the log in `/var/log/upstart/lxd.log`. To make LXD provide much more information about requests it is serving, add '--debug' to LXD's arguments. In systemd, append '--debug' to the 'ExecStart=' line in `/lib/systemd/system/lxd.service`. In Upstart, append it to the **exec /usr/bin/lxd** line in `/etc/init/lxd.conf`.

Container logfiles for container c1 may be seen using:

```
lxc info c1 --show-log
```

The configuration file which was used may be found under `/var/log/lxd/c1/lxc.conf` while apparmor profiles can be found in `/var/lib/lxd/security/apparmor/profiles/c1` and seccomp profiles in `/var/lib/lxd/security/seccomp/c1`.

6. LXC

Containers are a lightweight virtualization technology. They are more akin to an enhanced chroot than to full virtualization like Qemu or VMware, both because they do not emulate hardware and because containers share the same operating system as the host. Containers are similar to Solaris zones or BSD jails. Linux-vserver and OpenVZ are two pre-existing, independently developed implementations of containers-like functionality for Linux. In fact, containers came about as a result of the work to upstream the vserver and OpenVZ functionality.

There are two user-space implementations of containers, each exploiting the same kernel features. Libvirt allows the use of containers through the LXC driver by connecting to 'lxc:///'. This can be very convenient as it supports the same usage as its other drivers. The other implementation, called simply 'LXC', is not compatible with libvirt, but is more flexible with more userspace tools. It is possible to switch between the two, though there are peculiarities which can cause confusion.

In this document we will mainly describe the lxc package. Use of libvirt-lxc is not generally recommended due to a lack of Apparmor protection for libvirt-lxc containers.

In this document, a container name will be shown as CN, C1, or C2.

6.1. Installation

The lxc package can be installed using

```
sudo apt install lxc
```

This will pull in the required and recommended dependencies, as well as set up a network bridge for containers to use. If you wish to use unprivileged containers, you will need to ensure that users have sufficient allocated subuids and subgids, and will likely want to allow users to connect containers to a bridge (see *Section 6.2.3, “Basic unprivileged usage” [p. 362]*).

6.2. Basic usage

LXC can be used in two distinct ways - privileged, by running the lxc commands as the root user; or unprivileged, by running the lxc commands as a non-root user. (The starting of unprivileged containers by the root user is possible, but not described here.) Unprivileged containers are more limited, for instance being unable to create device nodes or mount block-backed filesystems. However they are less dangerous to the host, as the root userid in the container is mapped to a non-root userid on the host.

6.2.1. Basic privileged usage

To create a privileged container, you can simply do:

```
sudo lxc-create --template download --name u1
```

or, abbreviated

```
sudo lxc-create -t download -n u1
```

This will interactively ask for a container root filesystem type to download - in particular the distribution, release, and architecture. To create the container non-interactively, you can specify these values on the command line:

```
sudo lxc-create -t download -n u1 -- --dist ubuntu --release xenial --arch amd64
```

or

```
sudo lxc-create -t download -n u1 -- -d ubuntu -r xenial -a amd64
```

You can now use **lxc-ls** to list containers, **lxc-info** to obtain detailed container information, **lxc-start** to start and **lxc-stop** to stop the container. **lxc-attach** and **lxc-console** allow you to enter a container, if ssh is not an option. **lxc-destroy** removes the container, including its rootfs. See the manual pages for more information on each command. An example session might look like:

```
sudo lxc-ls --fancy
sudo lxc-start --name u1 --daemon
sudo lxc-info --name u1
sudo lxc-stop --name u1
sudo lxc-destroy --name u1
```

6.2.2. User namespaces

Unprivileged containers allow users to create and administer containers without having any root privilege. The feature underpinning this is called user namespaces. User namespaces are hierarchical, with privileged tasks in a parent namespace being able to map its ids into child namespaces. By default every task on the host runs in the initial user namespace, where the full range of ids is mapped onto the full range. This can be seen by looking at /proc/self/uid_map and /proc/self/gid_map, which both will show "0 0 4294967295" when read from the initial user namespace. As of Ubuntu 14.04, when new users are created they are by default offered a range of userids. The list of assigned ids can be seen in the files `/etc/subuid` and `/etc/subgid` See their respective manpages for more information. Subuids and subgids are by convention started at id 100000 to avoid conflicting with system users.

If a user was created on an earlier release, it can be granted a range of ids using **usermod**, as follows:

```
sudo usermod -v 100000-200000 -w 100000-200000 user1
```

The programs **newuidmap** and **newgidmap** are setuid-root programs in the `uidmap` package, which are used internally by lxc to map subuids and subgids from the host into the unprivileged container. They ensure that the user only maps ids which are authorized by the host configuration.

6.2.3. Basic unprivileged usage

To create unprivileged containers, a few first steps are needed. You will need to create a default container configuration file, specifying your desired id mappings and network setup, as well as configure the host to allow the unprivileged user to hook into the host network. The example below assumes that your mapped user and group id ranges are 100000-165536. Check your actual user and group id ranges and modify the example accordingly:

```
grep $USER /etc/subuid
grep $USER /etc/subgid
```

```
mkdir -p ~/.config/lxc
echo "lxc.id_map = u 0 100000 65536" > ~/.config/lxc/default.conf
echo "lxc.id_map = g 0 100000 65536" >> ~/.config/lxc/default.conf
echo "lxc.network.type = veth" >> ~/.config/lxc/default.conf
echo "lxc.network.link = lxcbr0" >> ~/.config/lxc/default.conf
echo "$USER veth lxcbr0 2" | sudo tee -a /etc/lxc/lxc-usernet
```

After this, you can create unprivileged containers the same way as privileged ones, simply without using sudo.

```
lxc-create -t download -n u1 -- -d ubuntu -r xenial -a amd64
lxc-start -n u1 -d
lxc-attach -n u1
lxc-stop -n u1
lxc-destroy -n u1
```

6.2.4. Nesting

In order to run containers inside containers - referred to as nested containers - two lines must be present in the parent container configuration file:

```
lxc.mount.auto = cgroup
lxc.aa_profile = lxc-container-default-with-nesting
```

The first will cause the cgroup manager socket to be bound into the container, so that lxc inside the container is able to administer cgroups for its nested containers. The second causes the container to run in a looser Apparmor policy which allows the container to do the mounting required for starting containers. Note that this policy, when used with a privileged container, is much less safe than the regular policy or an unprivileged container. See *Section 6.9, “Apparmor” [p. 366]* for more information.

6.3. Global configuration

The following configuration files are consulted by LXC. For privileged use, they are found under `/etc/lxc`, while for unprivileged use they are under `~/.config/lxc`.

- `lxc.conf` may optionally specify alternate values for several lxc settings, including the lxcpath, the default configuration, cgroups to use, a cgroup creation pattern, and storage backend settings for lvm and zfs.
- `default.conf` specifies configuration which every newly created container should contain. This usually contains at least a network section, and, for unprivileged users, an id mapping section
- `lxc-usernet.conf` specifies how unprivileged users may connect their containers to the host-owned network.

`lxc.conf` and `default.conf` are both under `/etc/lxc` and `$HOME/.config/lxc`, while `lxc-usernet.conf` is only host-wide.

By default, containers are located under /var/lib/lxc for the root user, and $HOME/.local/share/lxc otherwise. The location can be specified for all lxc commands using the "-P|--lxcpath" argument.

6.4. Networking

By default LXC creates a private network namespace for each container, which includes a layer 2 networking stack. Containers usually connect to the outside world by either having a physical NIC or a veth tunnel endpoint passed into the container. LXC creates a NATed bridge, lxcbr0, at host startup. Containers created using the default configuration will have one veth NIC with the remote end plugged into the lxcbr0 bridge. A NIC can only exist in one namespace at a time, so a physical NIC passed into the container is not usable on the host.

It is possible to create a container without a private network namespace. In this case, the container will have access to the host networking like any other application. Note that this is particularly dangerous if the container is running a distribution with upstart, like Ubuntu, since programs which talk to init, like **shutdown**, will talk over the abstract Unix domain socket to the host's upstart, and shut down the host.

To give containers on lxcbr0 a persistent ip address based on domain name, you can write entries to `/etc/lxc/dnsmasq.conf` like:

```
dhcp-host=lxcmail,10.0.3.100
dhcp-host=ttrss,10.0.3.101
```

If it is desirable for the container to be publicly accessible, there are a few ways to go about it. One is to use **iptables** to forward host ports to the container, for instance

```
 iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 587 -j DNAT \
  --to-destination 10.0.3.100:587
```

Another is to bridge the host's network interfaces (see the Ubuntu Server Guide's Network Configuration chapter, *Section 1.4, “Bridging” [p. 44]*). Then, specify the host's bridge in the container configuration file in place of lxcbr0, for instance

```
lxc.network.type = veth
lxc.network.link = br0
```

Finally, you can ask LXC to use macvlan for the container's NIC. Note that this has limitations and depending on configuration may not allow the container to talk to the host itself. Therefore the other two options are preferred and more commonly used.

There are several ways to determine the ip address for a container. First, you can use **lxc-ls --fancy** which will print the ip addresses for all running containers, or **lxc-info -i -H -n C1** which will print C1's ip address. If dnsmasq is installed on the host, you can also add an entry to `/etc/dnsmasq.conf` as follows

```
server=/lxc/10.0.3.1
```

after which dnsmasq will resolve C1.lxc locally, so that you can do:

```
ping C1
ssh C1
```

For more information, see the lxc.conf manpage as well as the example network configurations under `/usr/share/doc/lxc/examples/`.

6.5. LXC startup

LXC does not have a long-running daemon. However it does have three upstart jobs.

- `/etc/init/lxc-net.conf`: is an optional job which only runs if `/etc/default/lxc-net` specifies USE_LXC_BRIDGE (true by default). It sets up a NATed bridge for containers to use.
- `/etc/init/lxc.conf` loads the lxc apparmor profiles and optionally starts any autostart containers. The autostart containers will be ignored if LXC_AUTO (true by default) is set to true in `/etc/default/lxc`. See the lxc-autostart manual page for more information on autostarted containers.
- `/etc/init/lxc-instance.conf` is used by `/etc/init/lxc.conf` to autostart a container.

6.6. Backing Stores

LXC supports several backing stores for container root filesystems. The default is a simple directory backing store, because it requires no prior host customization, so long as the underlying filesystem is large enough. It also requires no root privilege to create the backing store, so that it is seamless for unprivileged use. The rootfs for a privileged directory backed container is located (by default) under `/var/lib/lxc/C1/rootfs`, while the rootfs for an unprivileged container is under `~/.local/share/lxc/C1/rootfs`. If a custom lxcpath is specified in lxc.system.com, then the container rootfs will be under `$lxcpath/C1/rootfs`.

A snapshot clone C2 of a directory backed container C1 becomes an overlayfs backed container, with a rootfs called `overlayfs:/var/lib/lxc/C1/rootfs:/var/lib/lxc/C2/delta0`. Other backing store types include loop, btrfs, LVM and zfs.

A btrfs backed container mostly looks like a directory backed container, with its root filesystem in the same location. However, the root filesystem comprises a subvolume, so that a snapshot clone is created using a subvolume snapshot.

The root filesystem for an LVM backed container can be any separate LV. The default VG name can be specified in lxc.conf. The filesystem type and size are configurable per-container using lxc-create.

The rootfs for a zfs backed container is a separate zfs filesystem, mounted under the traditional `/var/lib/lxc/C1/rootfs` location. The zfsroot can be specified at lxc-create, and a default can be specified in lxc.system.conf.

More information on creating containers with the various backing stores can be found in the lxc-create manual page.

6.7. Templates

Creating a container generally involves creating a root filesystem for the container. **lxc-create** delegates this work to *templates*, which are generally per-distribution. The lxc templates shipped with lxc can be found under `/usr/share/lxc/templates`, and include templates to create Ubuntu, Debian, Fedora, Oracle, centos, and gentoo containers among others.

Creating distribution images in most cases requires the ability to create device nodes, often requires tools which are not available in other distributions, and usually is quite time-consuming. Therefore lxc comes with a special *download* template, which downloads pre-built container images from a central lxc server. The most important use case is to allow simple creation of unprivileged containers by non-root users, who could not for instance easily run the **debootstrap** command.

When running **lxc-create**, all options which come after -- are passed to the template. In the following command, *--name*, *--template* and *--bdev* are passed to **lxc-create**, while *--release* is passed to the template:

```
lxc-create --template ubuntu --name c1 --bdev loop -- --release xenial
```

You can obtain help for the options supported by any particular container by passing *--help* and the template name to **lxc-create**. For instance, for help with the download template,

```
lxc-create --template download --help
```

6.8. Autostart

LXC supports marking containers to be started at system boot. Prior to Ubuntu 14.04, this was done using symbolic links under the directory `/etc/lxc/auto`. Starting with Ubuntu 14.04, it is done through the container configuration files. An entry

```
lxc.start.auto = 1
lxc.start.delay = 5
```

would mean that the container should be started at boot, and the system should wait 5 seconds before starting the next container. LXC also supports ordering and grouping of containers, as well as reboot and shutdown by autostart groups. See the manual pages for lxc-autostart and lxc.container.conf for more information.

6.9. Apparmor

LXC ships with a default Apparmor profile intended to protect the host from accidental misuses of privilege inside the container. For instance, the container will not be able to write to `/proc/sysrq-trigger` or to most `/sys` files.

The `usr.bin.lxc-start` profile is entered by running **lxc-start**. This profile mainly prevents **lxc-start** from mounting new filesystems outside of the container's root filesystem. Before executing the container's **init**, **LXC** requests a switch to the container's profile. By default, this profile is the `lxc-container-default` policy which is defined in `/etc/apparmor.d/lxc/lxc-default`. This profile prevents the container from accessing many dangerous paths, and from mounting most filesystems.

Programs in a container cannot be further confined - for instance, MySQL runs under the container profile (protecting the host) but will not be able to enter the MySQL profile (to protect the container).

lxc-execute does not enter an Apparmor profile, but the container it spawns will be confined.

6.9.1. Customizing container policies

If you find that **lxc-start** is failing due to a legitimate access which is being denied by its Apparmor policy, you can disable the lxc-start profile by doing:

```
sudo apparmor_parser -R /etc/apparmor.d/usr.bin.lxc-start
sudo ln -s /etc/apparmor.d/usr.bin.lxc-start /etc/apparmor.d/disabled/
```

This will make **lxc-start** run unconfined, but continue to confine the container itself. If you also wish to disable confinement of the container, then in addition to disabling the `usr.bin.lxc-start` profile, you must add:

```
lxc.aa_profile = unconfined
```

to the container's configuration file.

LXC ships with a few alternate policies for containers. If you wish to run containers inside containers (nesting), then you can use the lxc-container-default-with-nesting profile by adding the following line to the container configuration file

```
lxc.aa_profile = lxc-container-default-with-nesting
```

If you wish to use libvirt inside containers, then you will need to edit that policy (which is defined in `/etc/apparmor.d/lxc/lxc-default-with-nesting`) by uncommenting the following line:

```
mount fstype=cgroup -> /sys/fs/cgroup/**,
```

and re-load the policy.

Note that the nesting policy with privileged containers is far less safe than the default policy, as it allows containers to re-mount `/sys` and `/proc` in nonstandard locations, bypassing apparmor protections. Unprivileged containers do not have this drawback since the container root cannot write to root-owned `proc` and `sys` files.

Another profile shipped with lxc allows containers to mount block filesystem types like ext4. This can be useful in some cases like maas provisioning, but is deemed generally unsafe since the superblock handlers in the kernel have not been audited for safe handling of untrusted input.

If you need to run a container in a custom profile, you can create a new profile under `/etc/apparmor.d/lxc/`. Its name must start with `lxc-` in order for **lxc-start** to be allowed to transition to that profile. The `lxc-default` profile includes the re-usable abstractions file `/etc/apparmor.d/abstractions/lxc/container-base`. An easy way to start a new profile therefore is to do the same, then add extra permissions at the bottom of your policy.

After creating the policy, load it using:

```
sudo apparmor_parser -r /etc/apparmor.d/lxc-containers
```

The profile will automatically be loaded after a reboot, because it is sourced by the file `/etc/apparmor.d/lxc-containers`. Finally, to make container `CN` use this new `lxc-CN-profile`, add the following line to its configuration file:

```
lxc.aa_profile = lxc-CN-profile
```

6.10. Control Groups

Control groups (cgroups) are a kernel feature providing hierarchical task grouping and per-cgroup resource accounting and limits. They are used in containers to limit block and character device access and to freeze (suspend) containers. They can be further used to limit memory use and block i/o, guarantee minimum cpu shares, and to lock containers to specific cpus.

By default, a privileged container CN will be assigned to a cgroup called `/lxc/CN`. In the case of name conflicts (which can occur when using custom lxcpaths) a suffix "-n", where n is an integer starting at 0, will be appended to the cgroup name.

By default, a privileged container CN will be assigned to a cgroup called `CN` under the cgroup of the task which started the container, for instance `/usr/1000.user/1.session/CN`. The container root will be given group ownership of the directory (but not all files) so that it is allowed to create new child cgroups.

As of Ubuntu 14.04, LXC uses the cgroup manager (cgmanager) to administer cgroups. The cgroup manager receives D-Bus requests over the Unix socket `/sys/fs/cgroup/cgmanager/sock`. To facilitate safe nested containers, the line

```
lxc.mount.auto = cgroup
```

can be added to the container configuration causing the `/sys/fs/cgroup/cgmanager` directory to be bind-mounted into the container. The container in turn should start the cgroup management proxy (done by default if the cgmanager package is installed in the container) which will move the `/sys/fs/cgroup/cgmanager` directory to `/sys/fs/cgroup/cgmanager.lower`, then start listening for requests to proxy on its own socket `/sys/fs/cgroup/cgmanager/sock`. The host cgmanager will ensure that nested containers cannot escape their assigned cgroups or make requests for which they are not authorized.

6.11. Cloning

For rapid provisioning, you may wish to customize a canonical container according to your needs and then make multiple copies of it. This can be done with the **lxc-clone** program.

Clones are either snapshots or copies of another container. A copy is a new container copied from the original, and takes as much space on the host as the original. A snapshot exploits the underlying backing store's snapshotting ability to make a copy-on-write container referencing the first. Snapshots can be created from btrfs, LVM, zfs, and directory backed containers. Each backing store has its own peculiarities - for instance, LVM containers which are not thinpool-provisioned cannot support snapshots of snapshots; zfs containers with snapshots cannot be removed until all snapshots are released; LVM containers must be more carefully planned as the underlying filesystem may not support growing; btrfs does not suffer any of these shortcomings, but suffers from reduced fsync performance causing dpkg and apt to be slower.

Snapshots of directory-packed containers are created using the overlay filesystem. For instance, a privileged directory-backed container C1 will have its root filesystem under `/var/lib/lxc/C1/rootfs`. A snapshot clone of C1 called C2 will be started with C1's rootfs mounted readonly under `/var/lib/lxc/C2/delta0`. Importantly, in this case C1 should not be allowed to run or be removed while C2 is running. It is advised instead to consider C1 a *canonical* base container, and to only use its snapshots.

Given an existing container called C1, a copy can be created using:

```
sudo lxc-clone -o C1 -n C2
```

A snapshot can be created using:

```
sudo lxc-clone -s -o C1 -n C2
```

See the lxc-clone manpage for more information.

6.11.1. Snapshots

To more easily support the use of snapshot clones for iterative container development, LXC supports *snapshots*. When working on a container C1, before making a potentially dangerous or hard-to-revert change, you can create a snapshot

```
sudo lxc-snapshot -n C1
```

which is a snapshot-clone called 'snap0' under /var/lib/lxcsnaps or $HOME/.local/share/lxcsnaps. The next snapshot will be called 'snap1', etc. Existing snapshots can be listed using **lxc-snapshot -L -n C1**, and a snapshot can be restored - erasing the current C1 container - using **lxc-snapshot -r snap1 -n C1**. After the restore command, the snap1 snapshot continues to exist, and the previous C1 is erased and replaced with the snap1 snapshot.

Snapshots are supported for btrfs, lvm, zfs, and overlayfs containers. If lxc-snapshot is called on a directory-backed container, an error will be logged and the snapshot will be created as a copy-clone. The reason for this is that if the user creates an overlayfs snapshot of a directory-backed container and then makes changes to the directory-backed container, then the original container changes will be partially reflected in the snapshot. If snapshots of a directory backed container C1 are desired, then an overlayfs clone of C1 should be created, C1 should not be touched again, and the overlayfs clone can be edited and snapshotted at will, as such

```
lxc-clone -s -o C1 -n C2
lxc-start -n C2 -d # make some changes
```

```
lxc-stop -n C2
lxc-snapshot -n C2
lxc-start -n C2 # etc
```

6.11.2. Ephemeral Containers

While snapshots are useful for longer-term incremental development of images, ephemeral containers utilize snapshots for quick, single-use throwaway containers. Given a base container C1, you can start an ephemeral container using

```
lxc-start-ephemeral -o C1
```

The container begins as a snapshot of C1. Instructions for logging into the container will be printed to the console. After shutdown, the ephemeral container will be destroyed. See the lxc-start-ephemeral manual page for more options.

6.12. Lifecycle management hooks

Beginning with Ubuntu 12.10, it is possible to define hooks to be executed at specific points in a container's lifetime:

- Pre-start hooks are run in the host's namespace before the container ttys, consoles, or mounts are up. If any mounts are done in this hook, they should be cleaned up in the post-stop hook.
- Pre-mount hooks are run in the container's namespaces, but before the root filesystem has been mounted. Mounts done in this hook will be automatically cleaned up when the container shuts down.
- Mount hooks are run after the container filesystems have been mounted, but before the container has called **pivot_root** to change its root filesystem.
- Start hooks are run immediately before executing the container's init. Since these are executed after pivoting into the container's filesystem, the command to be executed must be copied into the container's filesystem.
- Post-stop hooks are executed after the container has been shut down.

If any hook returns an error, the container's run will be aborted. Any *post-stop* hook will still be executed. Any output generated by the script will be logged at the debug priority.

Please see the lxc.container.conf manual page for the configuration file format with which to specify hooks. Some sample hooks are shipped with the lxc package to serve as an example of how to write and use such hooks.

6.13. Consoles

Containers have a configurable number of consoles. One always exists on the container's `/dev/console`. This is shown on the terminal from which you ran **lxc-start**, unless the *-d* option is specified. The output on `/dev/`

`console` can be redirected to a file using the *-c console-file* option to **lxc-start**. The number of extra consoles is specified by the **lxc.tty** variable, and is usually set to 4. Those consoles are shown on `/dev/ttyN` (for 1 <= N <= 4). To log into console 3 from the host, use:

```
sudo lxc-console -n container -t 3
```

or if the *-t N* option is not specified, an unused console will be automatically chosen. To exit the console, use the escape sequence Ctrl-a q. Note that the escape sequence does not work in the console resulting from **lxc-start** without the *-d* option.

Each container console is actually a Unix98 pty in the host's (not the guest's) pty mount, bind-mounted over the guest's `/dev/ttyN` and `/dev/console`. Therefore, if the guest unmounts those or otherwise tries to access the actual character device **4:N**, it will not be serving getty to the LXC consoles. (With the default settings, the container will not be able to access that character device and getty will therefore fail.) This can easily happen when a boot script blindly mounts a new `/dev`.

6.14. Troubleshooting

6.14.1. Logging

If something goes wrong when starting a container, the first step should be to get full logging from LXC:

```
sudo lxc-start -n C1 -l trace -o debug.out
```

This will cause lxc to log at the most verbose level, `trace`, and to output log information to a file called 'debug.out'. If the file `debug.out` already exists, the new log information will be appended.

6.14.2. Monitoring container status

Two commands are available to monitor container state changes. **lxc-monitor** monitors one or more containers for any state changes. It takes a container name as usual with the *-n* option, but in this case the container name can be a posix regular expression to allow monitoring desirable sets of containers. **lxc-monitor** continues running as it prints container changes. **lxc-wait** waits for a specific state change and then exits. For instance,

```
sudo lxc-monitor -n cont[0-5]*
```

would print all state changes to any containers matching the listed regular expression, whereas

```
sudo lxc-wait -n cont1 -s 'STOPPED|FROZEN'
```

will wait until container cont1 enters state STOPPED or state FROZEN and then exit.

6.14.3. Attach

As of Ubuntu 14.04, it is possible to attach to a container's namespaces. The simplest case is to simply do

```
sudo lxc-attach -n C1
```

which will start a shell attached to C1's namespaces, or, effectively inside the container. The attach functionality is very flexible, allowing attaching to a subset of the container's namespaces and security context. See the manual page for more information.

6.14.4. Container init verbosity

If LXC completes the container startup, but the container init fails to complete (for instance, no login prompt is shown), it can be useful to request additional verbosity from the init process. For an upstart container, this might be:

```
sudo lxc-start -n C1 /sbin/init loglevel=debug
```

You can also start an entirely different program in place of init, for instance

```
sudo lxc-start -n C1 /bin/bash
sudo lxc-start -n C1 /bin/sleep 100
sudo lxc-start -n C1 /bin/cat /proc/1/status
```

6.15. LXC API

Most of the LXC functionality can now be accessed through an API exported by `liblxc` for which bindings are available in several languages, including Python, lua, ruby, and go.

Below is an example using the python bindings (which are available in the python3-lxc package) which creates and starts a container, then waits until it has been shut down:

```
# sudo python3
Python 3.2.3 (default, Aug 28 2012, 08:26:03)
[GCC 4.7.1 20120814 (prerelease)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
```

```
>>> import lxc
__main__:1: Warning: The python-lxc API isn't yet stable and may change at any p
oint in the future.
>>> c=lxc.Container("C1")
>>> c.create("ubuntu")
True
>>> c.start()
True
>>> c.wait("STOPPED")
True
```

6.16. Security

A namespace maps ids to resources. By not providing a container any id with which to reference a resource, the resource can be protected. This is the basis of some of the security afforded to container users. For instance, IPC namespaces are completely isolated. Other namespaces, however, have various *leaks* which allow privilege to be inappropriately exerted from a container into another container or to the host.

By default, LXC containers are started under a Apparmor policy to restrict some actions. The details of AppArmor integration with lxc are in section *Section 6.9, “Apparmor” [p. 366]*. Unprivileged containers go further by mapping root in the container to an unprivileged host userid. This prevents access to `/proc` and `/sys` files representing host resources, as well as any other files owned by root on the host.

6.16.1. Exploitable system calls

It is a core container feature that containers share a kernel with the host. Therefore if the kernel contains any exploitable system calls the container can exploit these as well. Once the container controls the kernel it can fully control any resource known to the host.

Since Ubuntu 12.10 (Quantal) a container can also be constrained by a seccomp filter. Seccomp is a new kernel feature which filters the system calls which may be used by a task and its children. While improved and simplified policy management is expected in the near future, the current policy consists of a simple whitelist of system call numbers. The policy file begins with a version number (which must be 1) on the first line and a policy type (which must be 'whitelist') on the second line. It is followed by a list of numbers, one per line.

In general to run a full distribution container a large number of system calls will be needed. However for application containers it may be possible to reduce the number of available system calls to only a few. Even for system containers running a full distribution security gains may be had, for instance by removing the 32-bit compatibility system calls in a 64-bit container. See the lxc.container.conf manual page for details of how to configure a container to use seccomp. By default, no seccomp policy is loaded.

6.17. Resources

- The DeveloperWorks article *LXC: Linux container tools*[45] was an early introduction to the use of containers.

[45] https://www.ibm.com/developerworks/linux/library/l-lxc-containers/

- The *Secure Containers Cookbook*[46] demonstrated the use of security modules to make containers more secure.
- Manual pages referenced above can be found at:

  `capabilities`[47]
  `lxc.conf`[48]
- The upstream LXC project is hosted at *linuxcontainers.org*[49].
- LXC security issues are listed and discussed at *the LXC Security wiki page*[50]
- For more on namespaces in Linux, see: S. Bhattiprolu, E. W. Biederman, S. E. Hallyn, and D. Lezcano. Virtual Servers and Check- point/Restart in Mainstream Linux. SIGOPS Operating Systems Review, 42(5), 2008.

[46] http://www.ibm.com/developerworks/linux/library/l-lxc-security/index.html
[47] http://manpages.ubuntu.com/manpages/en/man7/capabilities.7.html
[48] http://manpages.ubuntu.com/manpages/en/man5/lxc.conf.5.html
[49] http://linuxcontainers.org
[50] http://wiki.ubuntu.com/LxcSecurity

Chapter 21. Control Groups

Control groups (cgroups) are a kernel mechanism for grouping, tracking, and limiting the resource usage of tasks. The kernel-provided administration interface is through a virtual filesystem. Higher level cgroup administration tools have been developed, including libcgroup and lmctfy. Additionally, there is guidance at freedesktop.org for how applications can best cooperate using the cgroup filesystem interface (see Resources).

As of Ubuntu 14.04, the cgroup manager (cgmanager) is available as another cgroup administion interface. It's goal is to respond to dbus requests from any user, allowing him to administer only those cgroups which have been delegated to him.

Section 1, “Overview” [p. 376] will describe cgroups in more detail. *Section 2, “Filesystem” [p. 377]* will describe the long-standing cgroups filesystem interface. *Section 4, “Manager” [p. 379]* will describe the cgroup manager.

1. Overview

Cgroups are the generalized feature for grouping tasks. The actual resource tracking and limits are implemented by subsystems. A hierarchy is a set of subsystems mounted together. For instance, if the memory and devices subsystems are mounted together under /sys/fs/cgroups/set1, then any task which is in "/child1" will be subject to the corresponding limits of both subsystems.

Each set of mounted subsystems consittutes a 'hierarchy'. With exceptions, cgroups which are children of "/child1" will be subject to all limits placed on "/child1", and their resource usage will be accounted to "/child1".

The existing subsystems include:

- *cpusets*: fascilitate assigning a set of CPUS and memory nodes to cgroups. Tasks in a cpuset cgroup may only be scheduled on CPUS assigned to that cpuset.
- *blkio* : limits per-cgroup block io.
- *cpuacct* : provides per-cgroup cpu usage accounting.
- *devices* : controls the ability of tasks to create or use devices nodes using either a blacklist or whitelist.
- *freezer* : provides a way to 'freeze' and 'thaw' whole cgroups. Tasks in the cgroup will not be scheduled while they are frozen.
- *hugetlb* : fascilitates limiting hugetlb usage per cgroup.
- *memory* : allows memory, kernel memory, and swap usage to be tracked and limited.
- *net_cls* : provides an interface for tagging packets based on the sender cgroup. These tags can then be used by tc (traffic controller) to assign priorities.
- *net_prio* : allows setting network traffic priority on a per-cgroup basis.
- *cpu* : enables setting of scheduling preferences on per-cgroup basis.
- *perf_event* : enables per-cpu mode to monitor only threads in certain cgroups.

In addition, named cgroups can be created with no bound subsystems for the sake of process tracking. As an example, systemd does this to track services and user sessions.

2. Filesystem

A hierarchy is created by mounting an instance of the cgroup filesystem with each of the desired subsystems listed as a mount option. For instance,

```
mount -t cgroup -o devices,memory,freezer cgroup /cgroup1
```

would instantiate a hierarchy with the devices and memory cgroups comounted. A child cgroup "child1" can be created using 'mkdir'

```
mkdir /cgroup1/child1
```

and tasks can be moved into the new child cgroup by writing their process IDs into the 'tasks' or 'cgroup.procs' file:

```
sleep 100 &
echo $! > /cgroup1/child1/cgroup.procs
```

Other administration is done through files in the cgroup directories. For instance, to freeze all tasks in child1,

```
echo FROZEN > /cgroup1/child1/freezer.state
```

A great deal of information about cgroups and its subsystems can be found under the cgroups documentation directory in the kernel source tree (see Resources).

3. Delegation

Cgroup files and directories can be owned by non-root users, enabling delegation of cgroup administration. In general, the kernel enforces the hierarchical constraints on limits, so that for instance if devices cgroup `/child1` cannot access a disk drive, then `/child1/child2` cannot give itself those rights.

As of Ubuntu 14.04, users are automatically placed in a set of cgroups which they own, safely allowing them to contrain their own jobs using child cgroups. This feature is relied upon, for instance, for unprivileged container creation in lxc.

4. Manager

The cgroup manager (cgmanager) provides a D-Bus service allowing programs and users to administer cgroups without needing direct knowledge of or access to the cgroup filesystem. For requests from tasks in the same namespaces as the manager, the manager can directly perform the needed security checks to ensure that requests are legitimate. For other requests - such as those from a task in a container - enhanced D-Bus requests must be made, where process-, user- and group-ids are passed as SCM_CREDENTIALS, so that the kernel maps the identifiers to their global host values.

To fascilitate the use of simple D-Bus calls from all users, a 'cgroup manager proxy' (cgproxy) is automatically started when in a container. The proxy accepts standard D-Bus requests from tasks in the same namespaces as itself, and converts them to SCM-enhanced D-Bus requests which it passes on to the cgmanager.

A simple example of creating a new cgroup in which to run a cpu-intensive compile would look like:

```
cgm create cpuset build1
cgm movepid cpuset build1 $$
cgm setvalue cpuset build1 cpuset.cpus 1
make
```

5. Resources

- Manual pages referenced above can be found at:

  `cgm`[1]
  `cgconfig.conf`[2]
  `cgmanager`[3]
  `cgproxy`[4]

- The upstream cgmanager project is hosted at *linuxcontainers.org*[5].
- The upstream kernel documentation page on cgroups can be seen *here* [6].
- The freedesktop.org control group usage guidelines can be seen *here*[7].

[1] http://manpages.ubuntu.com/manpages/en/man8/cgm.1.html
[2] http://manpages.ubuntu.com/manpages/en/man5/cgconfig.conf.5.html
[3] http://manpages.ubuntu.com/manpages/en/man8/cgmanager.8.html
[4] http://manpages.ubuntu.com/manpages/en/man8/cgproxy.8.html
[5] http://cgmanager.linuxcontainers.org
[6] https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/tree/Documentation/cgroups
[7] http://www.freedesktop.org/wiki/Software/systemd/PaxControlGroups/

Chapter 22. Clustering

1. DRBD

Distributed Replicated Block Device (DRBD) mirrors block devices between multiple hosts. The replication is transparent to other applications on the host systems. Any block device hard disks, partitions, RAID devices, logical volumes, etc can be mirrored.

To get started using drbd, first install the necessary packages. From a terminal enter:

```
sudo apt install drbd8-utils
```

If you are using the *virtual kernel* as part of a virtual machine you will need to manually compile the drbd module. It may be easier to install the linux-server package inside the virtual machine.

This section covers setting up a drbd to replicate a separate `/srv` partition, with an ext3 filesystem between two hosts. The partition size is not particularly relevant, but both partitions need to be the same size.

1.1. Configuration

The two hosts in this example will be called *drbd01* and *drbd02*. They will need to have name resolution configured either through DNS or the `/etc/hosts` file. See *Chapter 8, Domain Name Service (DNS) [p. 163]* for details.

- To configure drbd, on the first host edit `/etc/drbd.conf`:

```
global { usage-count no; }
common { syncer { rate 100M; } }
resource r0 {
        protocol C;
        startup {
                wfc-timeout  15;
                degr-wfc-timeout 60;
        }
        net {
                cram-hmac-alg sha1;
                shared-secret "secret";
        }
        on drbd01 {
                device /dev/drbd0;
                disk /dev/sdb1;
                address 192.168.0.1:7788;
                meta-disk internal;
        }
        on drbd02 {
                device /dev/drbd0;
                disk /dev/sdb1;
                address 192.168.0.2:7788;
                meta-disk internal;
        }
}
```

There are many other options in `/etc/drbd.conf`, but for this example their default values are fine.

- Now copy `/etc/drbd.conf` to the second host:

```
scp /etc/drbd.conf drbd02:~
```

- And, on *drbd02* move the file to `/etc`:

```
sudo mv drbd.conf /etc/
```

- Now using the drbdadm utility initialize the meta data storage. On each server execute:

```
sudo drbdadm create-md r0
```

- Next, on both hosts, start the drbd daemon:

```
sudo systemctl start drbd.service
```

- On the *drbd01*, or whichever host you wish to be the primary, enter the following:

```
sudo drbdadm -- --overwrite-data-of-peer primary all
```

- After executing the above command, the data will start syncing with the secondary host. To watch the progress, on *drbd02* enter the following:

```
watch -n1 cat /proc/drbd
```

To stop watching the output press *Ctrl+c*.

- Finally, add a filesystem to `/dev/drbd0` and mount it:

```
sudo mkfs.ext3 /dev/drbd0
sudo mount /dev/drbd0 /srv
```

1.2. Testing

To test that the data is actually syncing between the hosts copy some files on the *drbd01*, the primary, to `/srv`:

```
sudo cp -r /etc/default /srv
```

Next, unmount `/srv`:

```
sudo umount /srv
```

Demote the *primary* server to the *secondary* role:

```
sudo drbdadm secondary r0
```

Now on the *secondary* server *promote* it to the *primary* role:

```
sudo drbdadm primary r0
```

Lastly, mount the partition:

```
sudo mount /dev/drbd0 /srv
```

Using *ls* you should see `/srv/default` copied from the former *primary* host *drbd01*.

1.3. References

- For more information on DRBD see the *DRBD web site*[1].
- The *drbd.conf man page*[2] contains details on the options not covered in this guide.
- Also, see the *drbdadm man page*[3].
- The *DRBD Ubuntu Wiki*[4] page also has more information.

[1] http://www.drbd.org/
[2] http://manpages.ubuntu.com/manpages/xenial/en/man5/drbd.conf.5.html
[3] http://manpages.ubuntu.com/manpages/xenial/en/man8/drbdadm.8.html
[4] https://help.ubuntu.com/community/DRBD

Chapter 23. VPN

OpenVPN is a Virtual Private Networking (VPN) solution provided in the Ubuntu Repositories. It is flexible, reliable and secure. It belongs to the family of SSL/TLS VPN stacks (different from IPSec VPNs). This chapter will cover installing and configuring OpenVPN to create a VPN.

1. OpenVPN

If you want more than just pre-shared keys OpenVPN makes it easy to setup and use a Public Key Infrastructure (PKI) to use SSL/TLS certificates for authentication and key exchange between the VPN server and clients. OpenVPN can be used in a routed or bridged VPN mode and can be configured to use either UDP or TCP. The port number can be configured as well, but port 1194 is the official one. And it is only using that single port for all communication. VPN client implementations are available for almost anything including all Linux distributions, OS X, Windows and OpenWRT based WLAN routers.

1.1. Server Installation

To install openvpn in a terminal enter:

```
sudo apt install openvpn easy-rsa
```

1.2. Public Key Infrastructure Setup

The first step in building an OpenVPN configuration is to establish a PKI (public key infrastructure). The PKI consists of:

- a separate certificate (also known as a public key) and private key for the server and each client, and
- a master Certificate Authority (CA) certificate and key which is used to sign each of the server and client certificates.

OpenVPN supports bidirectional authentication based on certificates, meaning that the client must authenticate the server certificate and the server must authenticate the client certificate before mutual trust is established.

Both server and client will authenticate the other by first verifying that the presented certificate was signed by the master certificate authority (CA), and then by testing information in the now-authenticated certificate header, such as the certificate common name or certificate type (client or server).

1.2.1. Certificate Authority Setup

To setup your own Certificate Authority (CA) and generating certificates and keys for an OpenVPN server and multiple clients first copy the `easy-rsa` directory to `/etc/openvpn`. This will ensure that any changes to the scripts will not be lost when the package is updated. From a terminal change to user root and:

```
mkdir /etc/openvpn/easy-rsa/
cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

Next, edit `/etc/openvpn/easy-rsa/vars` adjusting the following to your environment:

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="NC"
```

```
export KEY_CITY="Winston-Salem"
export KEY_ORG="Example Company"
export KEY_EMAIL="steve@example.com"
export KEY_CN=MyVPN
export KEY_NAME=MyVPN
export KEY_OU=MyVPN
```

Enter the following to generate the master Certificate Authority (CA) certificate and key:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-ca
```

1.2.2. Server Certificates

Next, we will generate a certificate and private key for the server:

```
./build-key-server myservername
```

As in the previous step, most parameters can be defaulted. Two other queries require positive responses, "Sign the certificate? [y/n]" and "1 out of 1 certificate requests certified, commit? [y/n]".

Diffie Hellman parameters must be generated for the OpenVPN server:

```
./build-dh
```

All certificates and keys have been generated in the subdirectory keys/. Common practice is to copy them to /etc/openvpn/:

```
cd keys/
cp myservername.crt myservername.key ca.crt dh2048.pem /etc/openvpn/
```

1.2.3. Client Certificates

The VPN client will also need a certificate to authenticate itself to the server. Usually you create a different certificate for each client. To create the certificate, enter the following in a terminal while being user root:

```
cd /etc/openvpn/easy-rsa/
source vars
./build-key client1
```

Copy the following files to the client using a secure method:

- /etc/openvpn/ca.crt
- /etc/openvpn/easy-rsa/keys/client1.crt
- /etc/openvpn/easy-rsa/keys/client1.key

As the client certificates and keys are only required on the client machine, you should remove them from the server.

1.3. Simple Server Configuration

Along with your OpenVPN installation you got these sample config files (and many more if if you check):

```
root@server:/# ls -l /usr/share/doc/openvpn/examples/sample-config-files/
total 68
-rw-r--r-- 1 root root 3427 2011-07-04 15:09 client.conf
-rw-r--r-- 1 root root 4141 2011-07-04 15:09 server.conf.gz
```

Start with copying and unpacking server.conf.gz to /etc/openvpn/server.conf.

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/
sudo gzip -d /etc/openvpn/server.conf.gz
```

Edit `/etc/openvpn/server.conf` to make sure the following lines are pointing to the certificates and keys you created in the section above.

```
ca ca.crt
cert myservername.crt
key myservername.key
dh dh2048.pem
```

Edit `/etc/sysctl.conf` and uncomment the following line to enable IP forwarding.

```
#net.ipv4.ip_forward=1
```

Then reload sysctl.

```
sudo sysctl -p /etc/sysctl.conf
```

That is the minimum you have to configure to get a working OpenVPN server. You can use all the default settings in the sample server.conf file. Now start the server. You will find logging and error messages in your via journal. Dependin on what you look for:

```
sudo journalctl -xe
```

If you started a templatized service openvpn@server you can filter for this particular message source with:

```
sudo journalctl --identifier ovpn-server
```

Be aware that the "systemctl start openvpn" is not starting your openvpn you just defined. Openvpn uses templatized systemd jobs, openvpn@CONFIGFILENAME. So if for example your configuration file is

"server.conf" your service is called openvpn@server. You can run all kind of service and systemctl commands like start/stop/enable/disable/preset against a templatized service like openvpn@server.

```
ubuntu@testopenvpn-server:~$ sudo systemctl start openvpn@server

ubuntu@testopenvpn-server:~$ sudo systemctl status openvpn@server
. openvpn@server.service - OpenVPN connection to server
Loaded: loaded (/lib/systemd/system/openvpn@.service; enabled; vendor preset: enabled)
      Active: active (running) since Tue 2016-04-12 08:51:14 UTC; 1s ago
        Docs: man:openvpn(8)
              https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage
              https://community.openvpn.net/openvpn/wiki/HOWTO
     Process: 1573 ExecStart=/usr/sbin/openvpn --daemon ovpn-%i --status /run/openvpn/
%i.status 10 --cd /etc/openvpn --script-security 2 --config /etc/openvpn/%i.conf --writep
    Main PID: 1575 (openvpn)
       Tasks: 1 (limit: 512)
      CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
              |-1575 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/
server.status 10 --cd /etc/openvpn --script-security 2 --config /etc/openvpn/server.conf --
wr

Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: /sbin/ip route add 10.8.0.0/24 via
 10.8.0.2
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: UDPv4 link local (bound): [undef]
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: UDPv4 link remote: [undef]
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: MULTI: multi_init called, r=256 v=256
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: IFCONFIG POOL: base=10.8.0.4 size=62,
 ipv6=0
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: ifconfig_pool_read(),
 in='client1,10.8.0.4', TODO: IPv6
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: succeeded -> ifconfig_pool_set()
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: IFCONFIG POOL LIST
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: client1,10.8.0.4
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: Initialization Sequence Completed
```

You can enable/disable various openvpn services on one system, but you could also let Ubuntu do the heavy lifting. There is config for AUTOSTART in /etc/default/openvpn. Allowed values are "all", "none" or space separated list of names of the VPNs. If empty, "all" is assumed. The VPN name refers to the VPN configutation file name. i.e. "home" would be /etc/openvpn/home.conf If you're running systemd, changing this variable will require running "systemctl daemon-reload" followed by a restart of the openvpn service (if you removed entries you may have to stop those manually) After "systemctl daemon-reload" a restart of the "generic" openvon will restart all dependent services that the generator in /lib/systemd/system-generators/ openvpn-generator created for your conf files when you called daemon-reload.

That is the minimum you have to configure to get a working OpenVPN server. You can use all the default settings in the sample server.conf file. Now start the server. You will find logging and error messages in your journal.

Now check if OpenVPN created a tun0 interface:

```
root@server:/etc/openvpn# ifconfig tun0
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
[...]
```

1.4. Simple Client Configuration

There are various different OpenVPN client implementations with and without GUIs. You can read more about clients in a later section. For now we use the OpenVPN client for Ubuntu which is the same executable as the server. So you have to install the openvpn package again on the client machine:

```
sudo apt install openvpn
```

This time copy the client.conf sample config file to /etc/openvpn/.

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/
```

Copy the client keys and the certificate of the CA you created in the section above to e.g. /etc/openvpn/ and edit `/etc/openvpn/client.conf` to make sure the following lines are pointing to those files. If you have the files in /etc/openvpn/ you can omit the path.

```
ca ca.crt
cert client1.crt
key client1.key
```

And you have to at least specify the OpenVPN server name or address. Make sure the keyword client is in the config. That's what enables client mode.

```
client
remote vpnserver.example.com 1194
```

Also, make sure you specify the keyfile names you copied from the server

```
ca ca.crt
cert client1.crt
key client1.key
```

Now start the OpenVPN client:

```
ubuntu@testopenvpn-client:~$ sudo systemctl start openvpn@client
ubuntu@testopenvpn-client:~$ sudo systemctl status  openvpn@client
. openvpn@client.service - OpenVPN connection to client
   Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset: enabled)
   Active: active (running) since Tue 2016-04-12 08:50:50 UTC; 3s ago
     Docs: man:openvpn(8)
```

```
           https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
 Process: 1677 ExecStart=/usr/sbin/openvpn --daemon ovpn-%i --status /run/openvpn/%i.status
 10 --cd /etc/openvpn --script-security 2 --config /etc/openvpn/%i.conf --writep
Main PID: 1679 (openvpn)
   Tasks: 1 (limit: 512)
  CGroup: /system.slice/system-openvpn.slice/openvpn@client.service
          |-1679 /usr/sbin/openvpn --daemon ovpn-client --status /run/openvpn/client.status
 10 --cd /etc/openvpn --script-security 2 --config /etc/openvpn/client.conf --wr

Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: OPTIONS IMPORT: --ifconfig/up options
 modified
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: OPTIONS IMPORT: route options modified
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: ROUTE_GATEWAY
 192.168.122.1/255.255.255.0 IFACE=eth0 HWADDR=52:54:00:89:ca:89
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: TUN/TAP device tun0 opened
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: TUN/TAP TX queue length set to 100
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: do_ifconfig, tt->ipv6=0, tt-
>did_ifconfig_ipv6_setup=0
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: /sbin/ip link set dev tun0 up mtu 1500
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: /sbin/ip addr add dev tun0 local
 10.8.0.6 peer 10.8.0.5
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: /sbin/ip route add 10.8.0.1/32 via
 10.8.0.5
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: Initialization Sequence Completed
```

Check if it created a tun0 interface:

```
root@client:/etc/openvpn# ifconfig tun0
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.6  P-t-P:10.8.0.5  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
```

Check if you can ping the OpenVPN server:

```
root@client:/etc/openvpn# ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_req=1 ttl=64 time=0.920 ms
```

The OpenVPN server always uses the first usable IP address in the client network and only that IP is pingable. E.g. if you configured a /24 for the client network mask, the .1 address will be used. The P-t-P address you see in the ifconfig output above is usually not answering ping requests.

Check out your routes:

```
root@client:/etc/openvpn# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.8.0.5        0.0.0.0         255.255.255.255 UH        0 0          0 tun0
10.8.0.1        10.8.0.5        255.255.255.255 UGH       0 0          0 tun0
```

```
192.168.42.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.42.1    0.0.0.0         UG        0 0          0 eth0
```

1.5. First trouble shooting

If the above didn't work for you, check this:

- Check your journal, e.g. journalctl --identifier ovpn-server (for server.conf)
- Check that you have specified the keyfile names correctly in client.conf and server.conf.
- Can the client connect to the server machine? Maybe a firewall is blocking access? Check journal on server.
- Client and server must use same protocol and port, e.g. UDP port 1194, see port and proto config option
- Client and server must use same config regarding compression, see comp-lzo config option
- Client and server must use same config regarding bridged vs routed mode, see server vs server-bridge config option

1.6. Advanced configuration

1.6.1. Advanced routed VPN configuration on server

The above is a very simple working VPN. The client can access services on the VPN server machine through an encrypted tunnel. If you want to reach more servers or anything in other networks, push some routes to the clients. E.g. if your company's network can be summarized to the network 192.168.0.0/16, you could push this route to the clients. But you will also have to change the routing for the way back - your servers need to know a route to the VPN client-network.

Or you might push a default gateway to all the clients to send all their internet traffic to the VPN gateway first and from there via the company firewall into the internet. This section shows you some possible options.

Push routes to the client to allow it to reach other private subnets behind the server. Remember that these private subnets will also need to know to route the OpenVPN client address pool (10.8.0.0/24) back to the OpenVPN server.

```
push "route 10.0.0.0 255.0.0.0"
```

If enabled, this directive will configure all clients to redirect their default network gateway through the VPN, causing all IP traffic such as web browsing and DNS lookups to go through the VPN (the OpenVPN server machine or your central firewall may need to NAT the TUN/TAP interface to the internet in order for this to work properly).

```
push "redirect-gateway def1 bypass-dhcp"
```

Configure server mode and supply a VPN subnet for OpenVPN to draw client addresses from. The server will take 10.8.0.1 for itself, the rest will be made available to clients. Each client will be able to reach the server on 10.8.0.1. Comment this line out if you are ethernet bridging.

```
server 10.8.0.0 255.255.255.0
```

Maintain a record of client to virtual IP address associations in this file. If OpenVPN goes down or is restarted, reconnecting clients can be assigned the same virtual IP address from the pool that was previously assigned.

```
ifconfig-pool-persist ipp.txt
```

Push DNS servers to the client.

```
push "dhcp-option DNS 10.0.0.2"
push "dhcp-option DNS 10.1.0.2"
```

Allow client to client communication.

```
client-to-client
```

Enable compression on the VPN link.

```
comp-lzo
```

The *keepalive* directive causes ping-like messages to be sent back and forth over the link so that each side knows when the other side has gone down. Ping every 1 second, assume that remote peer is down if no ping received during a 3 second time period.

```
keepalive 1 3
```

It's a good idea to reduce the OpenVPN daemon's privileges after initialization.

```
user nobody
group nogroup
```

OpenVPN 2.0 includes a feature that allows the OpenVPN server to securely obtain a username and password from a connecting client, and to use that information as a basis for authenticating the client. To use this authentication method, first add the auth-user-pass directive to the client configuration. It will direct the OpenVPN client to query the user for a username/password, passing it on to the server over the secure TLS channel.

```
# client config!
auth-user-pass
```

This will tell the OpenVPN server to validate the username/password entered by clients using the login PAM module. Useful if you have centralized authentication with e.g. Kerberos.

```
plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so login
```

Please read the OpenVPN *hardening security guide*[1] for further security advice.

1.6.2. Advanced bridged VPN configuration on server

OpenVPN can be setup for either a routed or a bridged VPN mode. Sometimes this is also referred to as OSI layer-2 versus layer-3 VPN. In a bridged VPN all layer-2 frames - e.g. all ethernet frames - are sent to the VPN partners and in a routed VPN only layer-3 packets are sent to VPN partners. In bridged mode all traffic including traffic which was traditionally LAN-local like local network broadcasts, DHCP requests, ARP requests etc. are sent to VPN partners whereas in routed mode this would be filtered.

1.6.2.1. Prepare interface config for bridging on server

Make sure you have the bridge-utils package installed:

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

Before you setup OpenVPN in bridged mode you need to change your interface configuration. Let's assume your server has an interface eth0 connected to the internet and an interface eth1 connected to the LAN you want to bridge. Your /etc/network/interfaces would like this:

```
auto eth0
iface eth0 inet static
  address 1.2.3.4
  netmask 255.255.255.248
  default 1.2.3.1

auto eth1
iface eth1 inet static
  address 10.0.0.4
  netmask 255.255.255.0
```

This straight forward interface config needs to be changed into a bridged mode like where the config of interface eth1 moves to the new br0 interface. Plus we configure that br0 should bridge interface eth1. We also need to make sure that interface eth1 is always in promiscuous mode - this tells the interface to forward all ethernet frames to the IP stack.

```
auto eth0
iface eth0 inet static
  address 1.2.3.4
  netmask 255.255.255.248
  default 1.2.3.1

auto eth1
iface eth1 inet manual
  up ip link set $IFACE up promisc on
```

[1] http://openvpn.net/index.php/open-source/documentation/howto.html#security

```
auto br0
iface br0 inet static
  address 10.0.0.4
  netmask 255.255.255.0
  bridge_ports eth1
```

At this point you need to bring up the bridge. Be prepared that this might not work as expected and that you will lose remote connectivity. Make sure you can solve problems having local access.

```
sudo ifdown eth1 && sudo ifup -a
```

1.6.2.2. Prepare server config for bridging

Edit `/etc/openvpn/server.conf` changing the following options to:

```
;dev tun
dev tap
up "/etc/openvpn/up.sh br0 eth1"
;server 10.8.0.0 255.255.255.0
server-bridge 10.0.0.4 255.255.255.0 10.0.0.128 10.0.0.254
```

Next, create a helper script to add the *tap* interface to the bridge and to ensure that eth1 is promiscuous mode. Create `/etc/openvpn/up.sh`:

```
#!/bin/sh

BR=$1
ETHDEV=$2
TAPDEV=$3

/sbin/ip link set "$TAPDEV" up
/sbin/ip link set "$ETHDEV" promisc on
/sbin/brctl addif $BR $TAPDEV
```

Then make it executable:

```
sudo chmod 755 /etc/openvpn/up.sh
```

After configuring the server, restart openvpn by entering:

```
sudo systemctl restart openvpn@server
```

1.6.2.3. Client Configuration

First, install openvpn on the client:

```
sudo apt install openvpn
```

Then with the server configured and the client certificates copied to the `/etc/openvpn/` directory, create a client configuration file by copying the example. In a terminal on the client machine enter:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn
```

Now edit `/etc/openvpn/client.conf` changing the following options:

```
dev tap
;dev tun
ca ca.crt
cert client1.crt
key client1.key
```

Finally, restart openvpn:

```
sudo systemctl restart openvpn@client
```

You should now be able to connect to the remote LAN through the VPN.

1.7. Client software implementations

1.7.1. Linux Network-Manager GUI for OpenVPN

Many Linux distributions including Ubuntu desktop variants come with Network Manager, a nice GUI to configure your network settings. It also can manage your VPN connections. Make sure you have package network-manager-openvpn installed. Here you see that the installation installs all other required packages as well:

```
root@client:~# apt install network-manager-openvpn
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  liblzo2-2 libpkcs11-helper1 network-manager-openvpn-gnome openvpn
Suggested packages:
  resolvconf
The following NEW packages will be installed:
  liblzo2-2 libpkcs11-helper1 network-manager-openvpn
  network-manager-openvpn-gnome openvpn
0 upgraded, 5 newly installed, 0 to remove and 631 not upgraded.
Need to get 700 kB of archives.
After this operation, 3,031 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

To inform network-manager about the new installed packages you will have to restart it:

```
root@client:~# restart network-manager
network-manager start/running, process 3078
```

Open the Network Manager GUI, select the VPN tab and then the 'Add' button. Select OpenVPN as the VPN type in the opening requester and press 'Create'. In the next window add the OpenVPN's server name as the 'Gateway', set 'Type' to 'Certificates (TLS)', point 'User Certificate' to your user certificate, 'CA Certificate' to your CA certificate and 'Private Key' to your private key file. Use the advanced button to enable compression (e.g. comp-lzo), dev tap, or other special settings you set on the server. Now try to establish your VPN.

1.7.2. OpenVPN with GUI for Mac OS X: Tunnelblick

Tunnelblick is an excellent free, open source implementation of a GUI for OpenVPN for OS X. The project's homepage is at *http://code.google.com/p/tunnelblick/*. Download the latest OS X installer from there and install it. Then put your client.ovpn config file together with the certificates and keys in /Users/username/Library/Application Support/Tunnelblick/Configurations/ and lauch Tunnelblick from your Application folder.

```
# sample client.ovpn for Tunnelblick
client
remote blue.example.com
port 1194
proto udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 86400
auth-user-pass
auth-nocache
auth-retry interact
comp-lzo yes
verb 3
ca ca.crt
cert client.crt
key client.key
```

1.7.3. OpenVPN with GUI for Win 7

First download and install the latest *OpenVPN Windows Installer*[2]. OpenVPN 2.3.2 was the latest when this was written. As of this writing, the management GUI is included with the Windows binary installer.

You need to start the OpenVPN service. Goto Start > Computer > Manage > Services and Applications > Services. Find the OpenVPN service and start it. Set it's startup type to automatic. When you start the OpenVPN MI GUI the first time you need to run it as an administrator. You have to right click on it and you will see that option.

You will have to write your OpenVPN config in a textfile and place it in C:\Program Files\OpenVPN\config \client.ovpn along with the CA certificate. You could put the user certificate in the user's home directory like in the follwing example.

[2] http://www.openvpn.net/index.php/open-source/downloads.html

```
# C:\Program Files\OpenVPN\config\client.ovpn
client
remote server.example.com
port 1194
proto udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 86400
auth-user-pass
auth-retry interact
comp-lzo yes
verb 3
ca ca.crt
cert "C:\\Users\\username\\My Documents\\openvpn\\client.crt"
key "C:\\Users\\username\\My Documents\\openvpn\\client.key"
management 127.0.0.1 1194
management-hold
management-query-passwords
auth-retry interact
; Set the name of the Windows TAP network interface device here
dev-node MyTAP
```

Note: If you are not using user authentication and/or you want to run the service without user interaction, comment out the following options:

```
auth-user-pass
auth-retry interact
management 127.0.0.1 1194
management-hold
management-query-passwords
```

You may want to set the Windows service to "automatic".

1.7.4. OpenVPN for OpenWRT

OpenWRT is described as a Linux distribution for embedded devices like WLAN router. There are certain types of WLAN routers who can be flashed to run OpenWRT. Depending on the available memory on your OpenWRT router you can run software like OpenVPN and you could for example build a small inexpensive branch office router with VPN connectivity to the central office. More info on OpenVPN on OpenWRT is *here*[3]. And here is the OpenWRT project's homepage: *http://openwrt.org*

Log into your OpenWRT router and install OpenVPN:

```
opkg update
opkg install openvpn
```

[3] http://wiki.openwrt.org/doc/howto/vpn.overview

Check out /etc/config/openvpn and put your client config in there. Copy certificates and keys to /etc/openvpn/

```
config openvpn client1
        option enable 1
        option client 1
#       option dev tap
        option dev tun
        option proto udp
        option ca /etc/openvpn/ca.crt
        option cert /etc/openvpn/client.crt
        option key /etc/openvpn/client.key
        option comp_lzo 1
```

Restart OpenVPN on OpenWRT router to pick up the config

You will have to see if you need to adjust your router's routing and firewall rules.

1.8. References

- See the *OpenVPN*[4] website for additional information.
- *OpenVPN hardening security guide*[5]
- Also, Pakt's *OpenVPN: Building and Integrating Virtual Private Networks*[6] is a good resource.

[4] http://openvpn.net/

[5] http://openvpn.net/index.php/open-source/documentation/howto.html#security

[6] http://www.packtpub.com/openvpn/book

Chapter 24. Other Useful Applications

There are many very useful applications developed by the Ubuntu Server Team, and others that are well integrated with Ubuntu Server Edition, that might not be well known. This chapter will showcase some useful applications that can make administering an Ubuntu server, or many Ubuntu servers, that much easier.

1. pam_motd

When logging into an Ubuntu server you may have noticed the informative Message Of The Day (MOTD). This information is obtained and displayed using a couple of packages:

- *landscape-common:* provides the core libraries of landscape-client, which is needed to manage systems with *Landscape*[1] (proprietary). Yet the package also includes the landscape-sysinfo utility which is responsible for displaying core system data involving cpu, memory, disk space, etc. For instance:

```
System load:  0.0               Processes:           76
Usage of /:   30.2% of 3.11GB   Users logged in:     1
Memory usage: 20%               IP address for eth0: 10.153.107.115
Swap usage:   0%

Graph this data and manage this system at https://landscape.canonical.com/
```

You can run landscape-sysinfo manually at any time.

- *update-notifier-common:* provides information on available package updates, impending filesystem checks (fsck), and required reboots (e.g.: after a kernel upgrade).

pam_motd executes the scripts in `/etc/update-motd.d` in order based on the number prepended to the script. The output of the scripts is written to `/var/run/motd`, keeping the numerical order, then concatenated with `/etc/motd.tail`.

You can add your own dynamic information to the MOTD. For example, to add local weather information:

- First, install the weather-util package:

```
sudo apt install weather-util
```

- The weather utility uses METAR data from the National Oceanic and Atmospheric Administration and forecasts from the National Weather Service. In order to find local information you will need the 4-character ICAO location indicator. This can be determined by browsing to the *National Weather Service*[2] site.

  Although the National Weather Service is a United States government agency there are weather stations available world wide. However, local weather information for all locations outside the U.S. may not be available.

- Create `/usr/local/bin/local-weather`, a simple shell script to use weather with your local ICAO indicator:

[1] http://landscape.canonical.com/

[2] http://www.weather.gov/tg/siteloc.shtml

```
#!/bin/sh
#
#
# Prints the local weather information for the MOTD.
#
#

# Replace KINT with your local weather station.
# Local stations can be found here: http://www.weather.gov/tg/siteloc.shtml

echo
weather -i KINT
echo
```

- Make the script executable:

```
sudo chmod 755 /usr/local/bin/local-weather
```

- Next, create a symlink to `/etc/update-motd.d/98-local-weather`:

```
sudo ln -s /usr/local/bin/local-weather /etc/update-motd.d/98-local-weather
```

- Finally, exit the server and re-login to view the new MOTD.

You should now be greeted with some useful information, and some information about the local weather that may not be quite so useful. Hopefully the local-weather example demonstrates the flexibility of pam_motd.

1.1. Resources

- See the *update-motd man page*[3] for more options available to update-motd.
- The Debian Package of the Day *weather*[4] article has more details about using the weatherutility.

[3] http://manpages.ubuntu.com/manpages/xenial/en/man5/update-motd.5.html

[4] http://debaday.debian.net/2007/10/04/weather-check-weather-conditions-and-forecasts-on-the-command-line/

2. etckeeper

etckeeper allows the contents of `/etc` to be stored in a Version Control System (VCS) repository. It integrates with APT and automatically commits changes to `/etc` when packages are installed or upgraded. Placing `/etc` under version control is considered an industry best practice, and the goal of etckeeper is to make this process as painless as possible.

Install etckeeper by entering the following in a terminal:

```
sudo apt install etckeeper
```

The main configuration file, `/etc/etckeeper/etckeeper.conf`, is fairly simple. The main option is which VCS to use and by default etckeeper is configured to use Bazaar. The repository is automatically initialized (and committed for the first time) during package installation. It is possible to undo this by entering the following command:

```
sudo etckeeper uninit
```

By default, etckeeper will commit uncommitted changes made to /etc daily. This can be disabled using the AVOID_DAILY_AUTOCOMMITS configuration option. It will also automatically commit changes before and after package installation. For a more precise tracking of changes, it is recommended to commit your changes manually, together with a commit message, using:

```
sudo etckeeper commit "..Reason for configuration change.."
```

Using bzr's VCS commands you can view log information:

```
sudo bzr log /etc/passwd
```

To demonstrate the integration with the package management system (APT), install postfix:

```
sudo apt install postfix
```

When the installation is finished, all the postfix configuration files should be committed to the repository:

```
Committing to: /etc/
added aliases.db
modified group
modified group-
modified gshadow
modified gshadow-
modified passwd
modified passwd-
added postfix
added resolvconf
```

```
added rsyslog.d
modified shadow
modified shadow-
added init.d/postfix
added network/if-down.d/postfix
added network/if-up.d/postfix
added postfix/dynamicmaps.cf
added postfix/main.cf
added postfix/master.cf
added postfix/post-install
added postfix/postfix-files
added postfix/postfix-script
added postfix/sasl
added ppp/ip-down.d
added ppp/ip-down.d/postfix
added ppp/ip-up.d/postfix
added rc0.d/K20postfix
added rc1.d/K20postfix
added rc2.d/S20postfix
added rc3.d/S20postfix
added rc4.d/S20postfix
added rc5.d/S20postfix
added rc6.d/K20postfix
added resolvconf/update-libc.d
added resolvconf/update-libc.d/postfix
added rsyslog.d/postfix.conf
added ufw/applications.d/postfix
Committed revision 2.
```

For an example of how etckeeper tracks manual changes, add new a host to `/etc/hosts`. Using bzr you can see which files have been modified:

```
sudo bzr status /etc/
modified:
  hosts
```

Now commit the changes:

```
sudo etckeeper commit "added new host"
```

For more information on bzr see *Section 1, “Bazaar” [p. 293]*.

2.1. Resources

- See the *etckeeper*[5] site for more details on using etckeeper.
- For the latest news and information about bzr see the *bzr*[6] web site.

[5] http://etckeeper.branchable.com/
[6] http://bazaar-vcs.org/

3. Byobu

One of the most useful applications for any system administrator is an xterm multiplexor such as screen or tmux. It allows for the execution of multiple shells in one terminal. To make some of the advanced multiplexor features more user-friendly and provide some useful information about the system, the byobu package was created. It acts as a wrapper to these programs. By default Byobu uses tmux (if installed) but this can be changed by the user.

Invoke it simply with:

byobu

Now bring up the configuration menu. By default this is done by pressing the *F9* key. This will allow you to:

- View the Help menu
- Change Byobu's background color
- Change Byobu's foreground color
- Toggle status notifications
- Change the key binding set
- Change the escape sequence
- Create new windows
- Manage the default windows
- Byobu currently does not launch at login (toggle on)

The *key bindings* determine such things as the escape sequence, new window, change window, etc. There are two key binding sets to choose from *f-keys* and *screen-escape-keys*. If you wish to use the original key bindings choose the *none* set.

byobu provides a menu which displays the Ubuntu release, processor information, memory information, and the time and date. The effect is similar to a desktop menu.

Using the *"Byobu currently does not launch at login (toggle on)"* option will cause byobu to be executed any time a terminal is opened. Changes made to byobu are on a per user basis, and will not affect other users on the system.

One difference when using byobu is the *scrollback* mode. Press the *F7* key to enter scrollback mode. Scrollback mode allows you to navigate past output using *vi* like commands. Here is a quick list of movement commands:

- *h* - Move the cursor left by one character
- *j* - Move the cursor down by one line
- *k* - Move the cursor up by one line
- *l* - Move the cursor right by one character

- *0* - Move to the beginning of the current line
- *$* - Move to the end of the current line
- *G* - Moves to the specified line (defaults to the end of the buffer)
- */* - Search forward
- *?* - Search backward
- *n* - Moves to the next match, either forward or backward

3.1. Resources

- For more information on screen see the *screen web site*[7].
- And the *Ubuntu Wiki screen*[8] page.
- Also, see the byobu *project page*[9] for more information.

[7] http://www.gnu.org/software/screen/
[8] https://help.ubuntu.com/community/Screen
[9] https://launchpad.net/byobu

Appendix A. Appendix

1. Reporting Bugs in Ubuntu Server Edition

The Ubuntu Project, and thus Ubuntu Server, uses *Launchpad*[1] as its bugtracker. In order to file a bug, you will need a Launchpad account. *Create one here*[2] if necessary.

1.1. Reporting Bugs With apport-cli

The preferred way to report a bug is with the apport-cli command. It must be invoked on the machine affected by the bug because it collects information from the system on which it is being run and publishes it to the bug report on Launchpad. Getting that information to Launchpad can therefore be a challenge if the system is not running a desktop environment in order to use a browser (common with servers) or if it does not have Internet access. The steps to take in these situations are described below.

The commands apport-cli and ubuntu-bug should give the same results on a CLI server. The latter is actually a symlink to apport-bug which is intelligent enough to know whether a desktop environment is in use and will choose apport-cli if not. Since server systems tend to be CLI-only apport-cli was chosen from the outset in this guide.

Bug reports in Ubuntu need to be filed against a specific software package, so the name of the package (source package or program name/path) affected by the bug needs to be supplied to apport-cli:

```
apport-cli PACKAGENAME
```

See *Chapter 3, Package Management [p. 25]* for more information about packages in Ubuntu.

Once apport-cli has finished gathering information you will be asked what to do with it. For instance, to report a bug in vim:

```
apport-cli vim

*** Collecting problem information

The collected information can be sent to the developers to improve the
application. This might take a few minutes.
...

*** Send problem report to the developers?

After the problem report has been sent, please fill out the form in the
automatically opened web browser.

What would you like to do? Your options are:
  S: Send report (2.8 KB)
```

[1] https://launchpad.net/

[2] https://help.launchpad.net/YourAccount/NewAccount

```
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  I: Cancel and ignore future crashes of this program version
  C: Cancel
Please choose (S/V/K/I/C):
```

The first three options are described below:

- **Send:** submits the collected information to Launchpad as part of the process of filing a new bug report. You will be given the opportunity to describe the bug in your own words.

```
*** Uploading problem information

The collected information is being sent to the bug tracking system.
This might take a few minutes.
94%

*** To continue, you must visit the following URL:

  https://bugs.launchpad.net/ubuntu/+source/vim/+filebug/09b2495a-
e2ab-11e3-879b-68b5996a96c8?

You can launch a browser now, or copy this URL into a browser on another computer.


Choices:
  1: Launch a browser now
  C: Cancel
Please choose (1/C):  1
```

  The browser that will be used when choosing '1' will be the one known on the system as www-browser via the *Debian alternatives system*[3]. Examples of text-based browsers to install include links, elinks, lynx, and w3m. You can also manually point an existing browser at the given URL.

- **View:** displays the collected information on the screen for review. This can be a lot of information. Press 'Enter' to scroll by screenful. Press 'q' to quit and return to the choice menu.
- **Keep:** writes the collected information to disk. The resulting file can be later used to file the bug report, typically after transferring it to another Ubuntu system.

```
What would you like to do? Your options are:
  S: Send report (2.8 KB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  I: Cancel and ignore future crashes of this program version
  C: Cancel
Please choose (S/V/K/I/C): k
Problem report file: /tmp/apport.vim.1pg92p02.apport
```

[3] http://manpages.ubuntu.com/manpages/en/man8/update-alternatives.8.html

To report the bug, get the file onto an internet-enabled Ubuntu system and apply apport-cli to it. This will cause the menu to appear immediately (the information is already collected). You should then press 's' to send:

```
apport-cli apport.vim.1pg92p02.apport
```

To directly save a report to disk (without menus) you can do:

```
apport-cli vim --save apport.vim.test.apport
```

Report names should end in *.apport* .

If this internet-enabled system is non-Ubuntu/Debian, apport-cli is not available so the bug will need to be created manually. An apport report is also not to be included as an attachment to a bug either so it is completely useless in this scenario.

1.2. Reporting Application Crashes

The software package that provides the apport-cli utility, apport, can be configured to automatically capture the state of a crashed application. This is enabled by default (in `/etc/default/apport`).

After an application crashes, if enabled, apport will store a crash report under `/var/crash`:

```
-rw-r----- 1 peter    whoopsie 150K Jul 24 16:17 _usr_lib_x86_64-linux-gnu_libmenu-
cache2_libexec_menu-cached.1000.crash
```

Use the apport-cli command without arguments to process any pending crash reports. It will offer to report them one by one.

```
apport-cli

*** Send problem report to the developers?

After the problem report has been sent, please fill out the form in the
automatically opened web browser.

What would you like to do? Your options are:
  S: Send report (153.0 KB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  I: Cancel and ignore future crashes of this program version
  C: Cancel
Please choose (S/V/K/I/C): s
```

If you send the report, as was done above, the prompt will be returned immediately and the `/var/crash` directory will then contain 2 extra files:

```
-rw-r----- 1 peter    whoopsie 150K Jul 24 16:17 _usr_lib_x86_64-linux-gnu_libmenu-
cache2_libexec_menu-cached.1000.crash
-rw-rw-r-- 1 peter    whoopsie    0 Jul 24 16:37 _usr_lib_x86_64-linux-gnu_libmenu-
cache2_libexec_menu-cached.1000.upload
-rw------- 1 whoopsie whoopsie    0 Jul 24 16:37 _usr_lib_x86_64-linux-gnu_libmenu-
cache2_libexec_menu-cached.1000.uploaded
```

Sending in a crash report like this will not immediately result in the creation of a new public bug. The report will be made private on Launchpad, meaning that it will be visible to only a limited set of bug triagers. These triagers will then scan the report for possible private data before creating a public bug.

1.3. Resources

- See the *Reporting Bugs*[4] Ubuntu wiki page.
- Also, the *Apport*[5] page has some useful information. Though some of it pertains to using a GUI.

[4] https://help.ubuntu.com/community/ReportingBugs

[5] https://wiki.ubuntu.com/Apport