

Οδηγός Διακομιστή Ubuntu

Οδηγός Διακομιστή Ubuntu

Πνευματικά Δικαιώματα © 2012 Contributors to the document

Περίληψη

Καλώς ήρθατε στον *Οδηγό Διακομιστή Ubuntu*! Περιέχει πληροφορίες για το πως να εγκαταστήσετε και να διαμορφώσετε προηγούμενες εφαρμογές διακομιστή στο σύστημα Ubuntu σας για να ταιριάζει στις ανάγκες σας. Είναι ένας βήμα-προς-βήμα, προσανατολισμένος σε διεργασίες οδηγός για να διαμορφώσετε και να προσαρμόσετε το σύστημά σας.

Συντελεστές και Άδεια Χρήσης

This document is maintained by the Ubuntu documentation team (<https://wiki.ubuntu.com/DocumentationTeam>). A list of contributors is below.

This document is made available under the Creative Commons ShareAlike 3.0 License (CC-BY-SA).

Είστε ελεύθεροι να τροποποιήσετε, να επεκτείνετε, και να βελτιώσετε τον πηγαίο κώδικα του Ubuntu υπό τους όρους της παρούσας άδειας. Όλα τα παραγόμενα έργα πρέπει να δημοσιεύονται με αυτή την άδεια.

Αυτή η τεκμηρίωση διανέμεται με την ελπίδα ότι θα είναι χρήσιμη, αλλά ΧΩΡΙΣ ΚΑΜΙΑ ΕΓΓΥΗΣΗ, χωρίς ακόμη και την έμμεση εγγύηση ΕΜΠΟΡΕΥΣΙΜΟΤΗΤΑΣ ή ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ ΓΙΑ ΕΝΑ ΣΥΓΓΕΚΡΙΜΕΝΟ ΣΚΟΠΟ ΟΠΩΣ ΠΕΡΙΓΡΑΦΕΤΑΙ ΣΤΗΝ ΑΠΟΠΟΙΗΣΗ.

A copy of the license is available here: *Creative Commons ShareAlike License*¹.

Contributors to this document are:

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

¹ <http://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://code.launchpad.net/serverguide>

⁶ <https://code.launchpad.net/ubuntu-docs>

Πίνακας Περιεχομένων

1. Εισαγωγή	1
1. Υποστήριξη	2
2. Εγκατάσταση	3
1. Προετοιμασία εγκατάστασης	4
2. Εγκατάσταση από CD	6
3. Αναβάθμιση	9
4. Εγκατάσταση για προχωρημένους	10
5. Kernel Crash Dump	19
3. Διαχείριση Πακέτων	22
1. Εισαγωγή	23
2. dpkg	24
3. Apt-Get	26
4. Aptitude	28
5. Αυτόματες Ενημερώσεις	30
6. Ρυθμίσεις	32
7. Αναφορές	34
4. Δικτύωση	35
1. Διαμόρφωση Δικτύου	36
2. TCP/IP	45
3. Πρωτόκολλο Δυναμικής Διαμόρφωσης Κεντρικού Υπολογιστή (Dynamic Host Configuration Protocol (DHCP))	50
4. Συγχρονισμός Ώρας με NTP	53
5. DM-Multipath	55
1. Device Mapper Multipathing	56
2. Multipath Devices	59
3. Setting up DM-Multipath Overview	62
4. The DM-Multipath Configuration File	66
5. DM-Multipath Administration and Troubleshooting	79
6. Απομακρυσμένη Διαχείριση	84
1. OpenSSH Server	85
2. Puppet	89
3. Zentyal	92
7. Πιστοποίηση δικτύου	96
1. Εξυπηρετητής OpenLDAP	97
2. Samba και LDAP	123
3. Kerberos	130
4. Kerberos και LDAP	138
8. Υπηρεσία ονομάτων τομέα (DNS)	145
1. Εγκατάσταση	146
2. Ρυθμίσεις	147

3. Επίλυση Προβλημάτων	153
4. Αναφορές	157
9. Ασφάλεια	159
1. Διαχείριση Χρηστών	160
2. Ασφάλεια Κονσόλας	167
3. Τείχος Προστασίας	168
4. AppArmor	176
5. Πιστοποιητικά	181
6. eCryptfs	187
10. Παρακολούθηση	190
1. Επισκόπηση	191
2. Nagios	192
3. Munin	197
11. Διακομιστές Ιστού	199
1. HTTPD - Apache2 Διακομιστής Ιστού	200
2. PHP5 - Γλώσσα Σεναρίου	209
3. Squid - Διακομιστής Διαμεσολαβητή	212
4. Ruby on Rails	215
5. Apache Tomcat	217
12. Βάσεις δεδομένων	221
1. MySQL	222
2. PostgreSQL	227
13. Εφαρμογές LAMP	230
1. Επισκόπηση	231
2. Moin Moin	233
3. MediaWiki	235
4. phpMyAdmin	237
5. WordPress	239
14. Εξυπηρετητές αρχείων	242
1. Εξυπηρετητής FTP	243
2. Σύστημα Αρχείων Δικτύου (NFS)	247
3. Αρχικοποιητής iSCSI	249
4. CUPS - Εξυπηρετητής εκτυπώσεων	252
15. Υπηρεσίες Ηλ. Αλληλογραφίας	255
1. Postfix	256
2. Exim4	265
3. Εξυπηρετητής Dovecot	268
4. Mailman	270
5. Φίλτρα ηλ. αλληλογραφίας	277
16. Εφαρμογές συζήτησης	284
1. Επισκόπηση	285
2. Εξυπηρετητής IRC	286

3. Εξυπηρετητής άμεσης ανταλλαγής μηνυμάτων Jabber	288
17. Σύστημα Ελέγχου Έκδοσης	290
1. Bazaar	291
2. Subversion	292
3. Διακομιστής CVS	298
4. Αναφορές	300
18. Samba	301
1. Εισαγωγή	302
2. File Server	303
3. Διακομιστής Εκτύπωσης	306
4. Securing File and Print Server	308
5. As a Domain Controller	313
6. Active Directory Integration	318
19. Αντίγραφα ασφαλείας	321
1. Σενάρια εντολών κελύφους	322
2. Archive Rotation	327
3. Bacula	331
20. Εικονικοποίηση	337
1. libvirt	338
2. JeOS και vmbuilder	344
3. Ubuntu Cloud	354
4. LXC	361
21. Συστοίχιση	385
1. DRBD	386
22. VPN	389
1. OpenVPN	390
23. Άλλες Χρήσιμες Εφαρμογές	403
1. pam_motd	404
2. etckeeper	406
3. Byobu	408
4. Αναφορές	410
A. Appendix	411
1. Reporting Bugs in Ubuntu Server Edition	412

Κατάλογος Πινάκων

2.1. Προτεινόμενες ελάχιστες απαιτήσεις	4
5.1. Priority Checker Conversion	56
5.2. DM-Multipath Components	57
5.3. Multipath Configuration Defaults	70
5.4. Multipath Attributes	74
5.5. Device Attributes	76
5.6. Useful multipath Command Options	82
17.1. Μέθοδοι Πρόσβασης	293
20.1. Container commands	374

Κεφάλαιο 1. Εισαγωγή

Καλωσορίσατε στον *Οδηγό εξυπηρετητή Ubuntu*!

Εδώ μπορείτε να βρείτε πληροφορίες για το πώς θα εγκαταστήσετε και θα ρυθμίσετε διάφορες εφαρμογές εξυπηρετητών. Είναι ένας εργοστροφής οδηγός, που βήμα-βήμα θα σας βοηθήσει να ρυθμίσετε και να προσαρμόσετε το σύστημά σας.

This guide assumes you have a basic understanding of your Ubuntu system. Some installation details are covered in *Κεφάλαιο 2, Εγκατάσταση [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/13.04/installation-guide/>

² <https://help.ubuntu.com>

1. Υποστήριξη

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

Παρέχεται επίσης υποστήριξη κοινότητας από ξεχωριστά άτομα και εταιρίες, που επιθυμούν να κάνουν το Ubuntu την καλύτερη δυνατή διανομή. Η υποστήριξη παρέχεται μέσω πολλών λιστών αλληλογραφίας, καναλιών IRC, φόρουμ, ιστολογίων, wiki, κτλ. Το μεγάλο ποσό διαθέσιμης πληροφορίας μπορεί να γίνει αφόρητο, αλλά ένα καλό ερώτημα σε κάποια μηχανή αναζήτησης μπορεί συνήθως να απαντήσει στις ερωτήσεις σας. Δείτε την *ελληνική σελίδα υποστήριξης του Ubuntu*⁴ ή την *αγγλική σελίδα Ubuntu Support*⁵ για περισσότερες πληροφορίες.

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

⁴ <http://wiki.ubuntu-gr.org/Support>

⁵ <http://www.ubuntu.com/support>

Κεφάλαιο 2. Εγκατάσταση

This chapter provides a quick overview of installing Ubuntu 13.04 Server Edition. For more detailed instructions, please refer to the *Ubuntu Installation Guide*¹.

¹ <https://help.ubuntu.com/13.04/installation-guide/>

1. Προετοιμασία εγκατάστασης

Αυτή η ενότητα εξηγεί διάφορες πτυχές που θα πρέπει να σκεφτείτε πριν ξεκινήσετε την εγκατάσταση.

1.1. Απαιτήσεις συστήματος

Ubuntu 13.04 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.

Πίνακας 2.1. Προτεινόμενες ελάχιστες απαιτήσεις

Τύπος εγκατάστασης	Κεντρική μονάδα επεξεργασίας (CPU)	RAM	Χώρος σκληρού δίσκου	
			Βασικό σύστημα	Με εγκατεστημένες όλες τις λειτουργίες
Server (Standard)	1 gigahertz	512 megabytes	1 gigabyte	1.75 gigabytes
Server (Minimal)	300 megahertz	256 megabytes	700 megabytes	1.4 gigabytes

Η Server Edition παρέχει μια κοινή βάση για όλων των ειδών τις εφαρμογές εξυπηρευτών. Είναι ένας μινιμαλιστικός σχεδιασμός που παρέχει μια πλατφόρμα για τις επιθυμητές υπηρεσίες, όπως υπηρεσίες αρχείων/εκτυπώσεων, φιλοξενία ιστοσελίδων, φιλοξενία ηλεκτρονικής αλληλογραφίας, κτλ.

1.2. Διαφορές μεταξύ Server και Desktop

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. Διαφορές στον πυρήνα:

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.



Όταν εκτελείτε μια έκδοση 64-bit του Ubuntu σε επεξεργαστές 64-bit δεν περιορίζετε από τον χώρο διευθυνσιοδότησης μνήμης (memory addressing).

To see all kernel configuration options you can look through `/boot/config-3.8.0-server`. Also, *Linux Kernel in a Nutshell*² is a great resource on the options available.

1.3. Αντίγραφο ασφαλείας

- Πριν εγκαταστήσετε το Ubuntu Server Edition, θα πρέπει να σιγουρευτείτε πως έχετε κρατήσει αντίγραφο ασφαλείας από όλα τα δεδομένα στο σύστημα. Δείτε το *Κεφάλαιο 19, Αντίγραφο ασφαλείας [321]* για επιλογές διατήρησης αντιγράφων ασφαλείας.

Αν αυτή δεν είναι η πρώτη φορά που εγκαθίσταται ένα λειτουργικό σύστημα στον υπολογιστή σας, είναι πιθανό πως θα χρειαστεί να επανα-κατατμήσετε τον δίσκο σας για να δημιουργήσετε χώρο για το Ubuntu.

Κάθε φορά που δημιουργείτε κατατμήσεις στον δίσκο σας, θα πρέπει να είστε προετοιμασμένοι να χάσετε τα πάντα στον δίσκο αν κάνετε κάποιο λάθος ή κάτι πάει στραβά κατά την κατάτμηση. Τα προγράμματα που χρησιμοποιούνται στην εγκατάσταση είναι αρκετά αξιόπιστα και τα περισσότερα χρησιμοποιούνται για χρόνια, αλλά εκτελούν επίσης και καταστρεπτικές ενέργειες.

² <http://www.kroah.com/lkn/>

2. Εγκατάσταση από CD

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

- First, download and burn the appropriate ISO file from the *Ubuntu web site*³.
- Εκκινήστε το σύστημα από τον οδηγό CD-ROM.
- 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 for 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.
- Το πρόγραμμα εγκατάστασης μετά εξερευνεί τις ρυθμίσεις του υλικού σας και ρυθμίζει τις επιλογές δικτύου χρησιμοποιώντας DHCP. Αν δεν επιθυμείτε να χρησιμοποιήσετε DHCP, στην επόμενη οθόνη επιλέξτε "Πίσω" και θα έχετε την επιλογή να ρυθμίσετε το δίκτυο χειροκίνητα.
- Μετά, το πρόγραμμα εγκατάστασης ζητάει το όνομα του συστήματος και τη ζώνη ώρας.
- You can then choose from several options to configure the hard drive layout. Afterwards you are asked for 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 *Τμήμα 4, Εγκατάσταση για προχωρημένους*; [10].
- Το βασικό σύστημα του Ubuntu είναι τότε εγκατεστημένο.
- 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 to encrypt your home directory.
- Το επόμενο βήμα στην διαδικασία εγκατάστασης είναι να αποφασίσετε πώς θέλετε να ενημερώνεται το σύστημα. Υπάρχουν τρεις επιλογές:
 - *Χωρίς αυτόματες ενημερώσεις*: αυτό χρειάζεται έναν διαχειριστή να συνδέεται στο μηχάνημα και να εγκαθιστά τις ενημερώσεις χειροκίνητα.
 - *Install security updates automatically*: this will install the unattended-upgrades package, which will install security updates without the intervention

³ <http://www.ubuntu.com/download/server/download>

of an administrator. For more details see *Τμήμα 5, “Αυτόματες Ενημερώσεις” [30]*.

- *Διαχείριση του συστήματος με το Landscape*: Το Landscape είναι μια υπηρεσία επί πληρωμή που παρέχεται από την Canonical για να βοηθήσει στη διαχείριση των μηχανημάτων Ubuntu σας. Δείτε τον ιστότοπο του *Landscape*⁴ για λεπτομέρειες.
- Τώρα έχετε την επιλογή να εγκαταστήσετε, ή να μην εγκαταστήσετε, αρκετές εργασίες πακέτων. Δείτε το *Τμήμα 2.1, “Εργασίες πακέτων” [7]* για λεπτομέρειες. Επίσης, υπάρχει μια επιλογή που εκκινεί το aptitude ώστε να επιλέξετε συγκεκριμένα πακέτα για εγκατάσταση. Για περισσότερες πληροφορίες δείτε το *Τμήμα 4, “Aptitude” [28]*.
- Τέλος, το τελευταίο βήμα πριν την επανεκκίνηση, είναι να ρυθμιστεί το ρολόι σε UTC.



Αν σε οποιοδήποτε σημείο κατά την εγκατάσταση δεν είσαστε ικανοποιημένοι από τις προεπιλεγμένες ρυθμίσεις, χρησιμοποιήστε τη λειτουργία "Πίσω", σε οποιοδήποτε σημείο, για να μεταβείτε σε ένα λεπτομερές μενού εγκατάστασης που θα σας επιτρέψει να τροποποιήσετε τις προεπιλεγμένες ρυθμίσεις.

Σε κάποιο σημείο κατά την διαδικασία εγκατάστασης, μπορεί να θέλετε να διαβάσετε την οθόνη βοήθειας που παρέχεται από το σύστημα εγκατάστασης. Για να το κάνετε αυτό, πιέστε F1.

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

2.1. Εργασίες πακέτων

Κατά την εγκατάσταση της Server Edition, έχετε την επιλογή να εγκαταστήσετε επιπλέον πακέτα από το CD. Τα πακέτα ομαδοποιούνται σύμφωνα με το είδος των υπηρεσιών που προσφέρουν.

- Εξυπηρετητής DNS: Επιλέγει τον εξυπηρετητή BIND DNS και την τεκμηρίωσή του.
- Εξυπηρετητής LAMP: Επιλέγει έναν έτοιμο εξυπηρετητή Linux/Apache/MySQL/PHP.
- Mail server: This task selects a variety of packages useful for a general purpose mail server system.
- Εξυπηρετητής OpenSSH: Επιλέγει πακέτα που χρειάζονται για έναν εξυπηρετητή OpenSSH.
- Βάση δεδομένων PostgreSQL: Αυτή η εργασία επιλέγει πακέτα πελάτη και εξυπηρετητή για τη βάση δεδομένων PostgreSQL.
- Εξυπηρετητής εκτυπώσεων: Αυτή η εργασία ρυθμίζει το σύστημά σας ώστε να είναι ένας εξυπηρετητής εκτυπώσεων.

⁴ <http://www.canonical.com/projects/landscape>

⁵ <https://help.ubuntu.com/13.04/installation-guide/>

- Εξυπηρετητής αρχείων Samba: Αυτή η εργασία ρυθμίζει το σύστημά σας ώστε να είναι ένας εξυπηρετητής αρχείων Samba, που είναι ειδικά κατάλληλος σε δίκτυα με συστήματα Windows και Linux.
- 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.

Μόλις η διαδικασία εγκατάστασης ολοκληρωθεί μπορείτε να εμφανίσετε μια λίστα με διαθέσιμες εργασίες πληκτρολογώντας το ακόλουθο σε ένα τερματικό:

`tasksel --list-tasks`



Το αποτέλεσμα θα εμφανίσει εργασίες από άλλες διανομές βασισμένες στο Ubuntu όπως το Kubuntu και το Edubuntu. Σημειώστε πως μπορείτε επίσης να καλέσετε την εντολή **`tasksel`** χωρίς παραμέτρους, πράγμα που θα εμφανίσει ένα μενού με τις διάφορες διαθέσιμες εργασίες.

Μπορείτε να δείτε μία λίστα των πακέτων που έχουν εγκατασταθεί με κάθε εργασία χρησιμοποιώντας την επιλογή *`--task-packages`*. Για παράδειγμα, για να δείτε τα πακέτα που εγκαταστάθηκαν με τον *εξυπηρετητή DNS* πληκτρολογήστε το ακόλουθο:

`tasksel --task-packages dns-server`

Το αποτέλεσμα της εντολής πρέπει να εμφανίσει:

```
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 CD and from a terminal:

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

3. Αναβάθμιση

Υπάρχουν αρκετοί τρόποι για να αναβαθμίσετε μια έκδοση του Ubuntu σε μία άλλη. Αυτή η ενότητα δίνει μια γενική εικόνα της προτεινόμενης μεθόδου αναβάθμισης.

3.1. `do-release-upgrade`

Ο προτεινόμενος τρόπος αναβάθμισης μιας εγκατάστασης Server Edition είναι να χρησιμοποιήσετε το εργαλείο `do-release-upgrade`. Μέρος του πακέτου *update-manager-core*, δεν έχει καμία εξάρτηση με γραφικό περιβάλλον και είναι εγκατεστημένο από προεπιλογή.

Τα συστήματα που βασίζονται στο Debian μπορούν επίσης να αναβαθμιστούν με τη χρήση του **`apt-get dist-upgrade`**. Ωστόσο, η χρήση του `do-release-upgrade` προτείνεται επειδή έχει τη δυνατότητα να χειριστεί αλλαγές στις ρυθμίσεις του συστήματος που κάποιες φορές χρειάζονται κατά την αλλαγή εκδόσεων.

Για να κάνετε αναβάθμιση σε μια νεότερη έκδοση, σε ένα τερματικό πληκτρολογήστε:

`do-release-upgrade`

Είναι επίσης εφικτή η χρήση του `do-release-upgrade` για την αναβάθμιση σε κάποια έκδοση του Ubuntu που βρίσκεται υπό ανάπτυξη. Για να επιτευχθεί αυτό, χρησιμοποιήστε την επιλογή `-d`:

`do-release-upgrade -d`



Η αναβάθμιση σε έκδοση που βρίσκεται υπό ανάπτυξη δεν συνιστάται για περιβάλλοντα παραγωγής.

4. Εγκατάσταση για προχωρημένους

4.1. RAID λογισμικού

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').

Το λογισμικό RAID που περιέχεται στις τρέχουσες εκδόσεις του Linux (και του Ubuntu) βασίζεται στον οδηγό 'mdadm' και δουλεύει πολύ καλά, καλύτερα ακόμη από πολλούς ξακουστούς ελεγκτές RAID υλικού. Αυτή η ενότητα θα σας καθοδηγήσει στην εγκατάσταση του Ubuntu Server Edition χρησιμοποιώντας δύο κατατμήσεις RAID1 σε δύο φυσικούς σκληρούς δίσκους, έναν για το / και τον άλλον για το *swap*.

4.1.1. Διαμερισμός

Ακολουθήστε τα βήματα εγκατάστασης μέχρι να φτάσετε στο βήμα *Διαμέριση δίσκων*, μετά:

1. Επιλέξτε *Χειροκίνητα* ως την μέθοδο διαμέρισης.
2. Επιλέξτε τον πρώτο σκληρό δίσκο, και συμφωνήστε στη "*δημιουργία νέου πίνακα διαμέρισης στη συσκευή αυτή*".

Επαναλάβετε αυτό το βήμα για κάθε συσκευή που επιθυμείτε να είναι μέρος της διάταξης RAID.

3. Επιλέξτε το "*ΕΛΕΥΘΕΡΟΣ ΧΩΡΟΣ*" στην πρώτη συσκευή και μετά επιλέξτε "*Δημιουργία νέας κατάτμησης*".
4. Μετά επιλέξτε το *Μέγεθος* της κατάτμησης. Αυτή η κατάτμηση θα είναι η κατάτμηση του *swap* και ένας γενικός κανόνας για το μέγεθος του *swap* είναι το διπλάσιο εκείνου της RAM. Εισαγάγετε το μέγεθος της κατάτμησης, μετά επιλέξτε *Πρωτεύουσα* και μετά *Αρχή*.



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. Επιλέξτε τη γραμμή "*Χρήση ως:*" στην κορυφή. Από προεπιλογή αυτό είναι "*σύστημα αρχείων ext4 με journal*", αλλάξτε το σε "*φυσικός τόμος για RAID*" και μετά επιλέξτε "*Ολοκλήρωση της ρύθμισης της κατάτμησης*".

6. Για την κατάτμηση /για μία ακόμη φορά, επιλέξτε *"Ελεύθερος χώρος"* στην πρώτη συσκευή και μετά *"Δημιουργία νέας κατάτμησης"*.
7. Χρησιμοποιήστε τον υπόλοιπο ελεύθερο χώρο της συσκευής και επιλέξτε *Συνέχεια* και μετά *Πρωτεύουσα*.
8. Όπως με την κατάτμηση του *swar*, επιλέξτε τη γραμμή *"Χρήση ως:"* στην κορυφή, αλλάζοντάς την σε *"φυσικός τόμος για RAID"*. Επίσης επιλέξτε τη γραμμή *"Εκκινήσιμη:"* για να αλλάξετε την τιμή σε *"ναι"*. Μετά επιλέξτε *"Ολοκλήρωση της ρύθμισης της κατάτμησης"*.
9. Επαναλάβετε τα βήματα τρία έως οκτώ για τους άλλους δίσκους και κατατμήσεις.

4.1.2. Ρύθμιση του RAID

Με τις κατατμήσεις να έχουν δημιουργηθεί, οι διατάξεις είναι έτοιμες να ρυθμιστούν:

1. Πίσω στην κύρια σελίδα *"Διαμέριση δίσκων"*, επιλέξτε *"Ρύθμιση RAID λογισμικού"* στην κορυφή.
2. Επιλέξτε *"ναι"* για να εγγραφούν οι αλλαγές στον δίσκο.
3. Επιλέξτε *"Δημιουργία μονάδας MD"*.
4. Για αυτό το παράδειγμα, επιλέξτε *"RAID1"*, αλλά αν χρησιμοποιείτε διαφορετική εγκατάσταση, επιλέξτε τον κατάλληλο τύπο (RAID0 RAID1 RAID5).



Για να χρησιμοποιήσετε *RAID5* χρειάζεστε τουλάχιστον *τρεις* συσκευές. Χρησιμοποιώντας RAID0 ή RAID1, απαιτούνται μόνο *δύο* συσκευές.

5. Πληκτρολογήστε τον αριθμό των ενεργών συσκευών - *"2"*, ή τον αριθμό των σκληρών δίσκων που έχετε - για τη συστοιχία. Μετά επιλέξτε *"Συνέχεια"*.
6. Μετά, πληκτρολογήστε τον αριθμό των εφεδρικών συσκευών - *"0"* από προεπιλογή - και επιλέξτε *"Συνέχεια"*.
7. Επιλέξτε ποιες κατατμήσεις θα χρησιμοποιηθούν. Γενικά, αυτές θα είναι *sda1*, *sdb1*, *sdc1*, κτλ. Οι αριθμοί συνήθως θα ταιριάζουν, και τα διαφορετικά γράμματα αντιστοιχούν σε διαφορετικούς σκληρούς δίσκους.

Για την κατάτμηση του *swar* επιλέξτε τα *sda1* και *sdb1*. Επιλέξτε *"Συνέχεια"* για να προχωρήσετε στο επόμενο βήμα.

8. Επαναλάβετε τα βήματα *τρία* έως *επτά* για την κατάτμηση /επιλέγοντας τα *sda2* και *sdb2*.
9. Μόλις τελειώσετε, επιλέξτε *"Ολοκλήρωση"*.

4.1.3. Διαμόρφωση

Τώρα θα πρέπει να υπάρχει μια λίστα σκληρών δίσκων και συσκευών RAID. Το επόμενο βήμα είναι να διαμορφώσετε και να ορίσετε το σημείο προσάρτησης για τις συσκευές

RAID. Αντιμετωπίστε τη συσκευή RAID ως έναν τοπικό σκληρό δίσκο, διαμορφώστε και προσαρτήστε αναλόγως.

1. Επιλέξτε "#1" κάτω από την κατάτμηση "RAID1 device #0"
2. Επιλέξτε "Χρήση ως:". Μετά επιλέξτε "χώρος εικονικής μνήμης", μετά "Ολοκλήρωση της ρύθμισης της κατάτμησης".
3. Μετά επιλέξτε "#1" κάτω από την κατάτμηση "RAID1 device #1".
4. Επιλέξτε "Χρήση ως:". Μετά επιλέξτε "σύστημα αρχείων ext4 με journal".
5. Μετά επιλέξτε το "Σημείο προσάρτησης" και επιλέξτε "/" - το βασικό σύστημα αρχείων". Αλλάξτε οποιαδήποτε άλλη επιλογή καταλλήλως και μετά επιλέξτε "Ολοκλήρωση της ρύθμισης της κατάτμησης".
6. Τέλος, επιλέξτε "Ολοκλήρωση διαμέρισης και εγγραφή αλλαγών στον δίσκο".

Αν επιλέξετε να τοποθετήσετε την κατάτμηση του βασικού συστήματος (root) σε μία συστοιχία RAID, το πρόγραμμα εγκατάστασης θα ρωτήσει αν θέλετε να γίνεται εκκίνηση σε υποβαθμισμένη κατάσταση. Δείτε το *Τμήμα 4.1.4, “Υποβαθμισμένο RAID” [12]* για περισσότερες λεπτομέρειες.

Η διαδικασία εγκατάστασης θα συνεχιστεί τότε κανονικά.

4.1.4. Υποβαθμισμένο RAID

Σε κάποιο σημείο της ζωής του υπολογιστή, μπορεί να προκύψει κάποια βλάβη στον δίσκο. Όταν συμβαίνει αυτό, ενώ χρησιμοποιείτε RAID λογισμικού, το λειτουργικό σύστημα θα τοποθετήσει τη συστοιχία σε αυτό που είναι γνωστό ως *υποβαθμισμένη κατάσταση*.

Αν η διάταξη έχει γίνει υποβαθμισμένη, λόγω της πιθανότητας απώλειας δεδομένων, από προεπιλογή το Ubuntu Server Edition θα εκκινήσει σε *initramfs* μετά από τριάντα δευτερόλεπτα. Μόλις εκκινηθεί το *initramfs*, υπάρχει μια ερώτηση για πενήντα δευτερόλεπτα που σας δίνει τη δυνατότητα να προχωρήσετε και να εκκινήσετε το σύστημα, ή να επιχειρήσετε χειροκίνητη ανάκτηση. Η εκκίνηση στο *initramfs* μπορεί να είναι ή όχι η επιθυμητή συμπεριφορά, ειδικά αν το μηχάνημα είναι σε απομακρυσμένη τοποθεσία. Η εκκίνηση σε μια υποβαθμισμένη διάταξη μπορεί να ρυθμιστεί με πολλούς τρόπους:

- Το εργαλείο `dpkg-reconfigure` μπορεί να χρησιμοποιηθεί για να ρυθμιστεί η προεπιλεγμένη συμπεριφορά και κατά τη διαδικασία θα ερωτηθείτε για επιπλέον ρυθμίσεις σχετικές με τη συστοιχία. Όπως παρακολούθηση, ειδοποιήσεις μέσω email, κτλ. Για να επαναρυθμίσετε το `mdadm`, πληκτρολογήστε το ακόλουθο:

```
sudo dpkg-reconfigure mdadm
```

- Η διαδικασία **`dpkg-reconfigure mdadm`** θα αλλάξει το αρχείο ρυθμίσεων `/etc/initramfs-tools/conf.d/mdadm`. Το αρχείο έχει το πλεονέκτημα πως έχει τη δυνατότητα να προ-

ρυθμίσει τη συμπεριφορά του συστήματος και μπορείτε επίσης να το επεξεργαστείτε χειροκίνητα:

```
BOOT_DEGRADED=true
```



Το αρχείο ρυθμίσεων μπορεί να παρακαμφθεί χρησιμοποιώντας κάποια παράμετρο με τον πυρήνα.

- Η χρήση μιας παραμέτρου πυρήνα θα επιτρέψει στο σύστημα να εκκινήσει σε μία υποβαθμισμένη διάταξη επίσης:
 - 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.
 - Προσθέστε *"bootdegraded=true"* (χωρίς τα εισαγωγικά) στο τέλος της γραμμής.
 - Press **Ctrl+x** to boot the system.

Μόλις το σύστημα εκκινηθεί, μπορείτε είτε να επισκευάσετε τη συστοιχία - δείτε το *Τμήμα 4.1.5, “Συντήρηση του RAID” [13]* για λεπτομέρειες -, ή να αντιγράψετε σημαντικά δεδομένα σε ένα άλλο μηχανήμα λόγω σημαντικής βλάβης υλικού.

4.1.5. Συντήρηση του RAID

Το εργαλείο mdadm μπορεί να χρησιμοποιηθεί για να προβάλλετε την κατάσταση μιας συστοιχίας, για να προσθέσετε δίσκους σε μία συστοιχία, να αφαιρέσετε δίσκους, κτλ:

- Για να προβάλλετε την κατάσταση μιας συστοιχίας, σε ένα τερματικό πληκτρολογήστε:

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

Η επιλογή *-D* λέει στο mdadm να εμφανίσει αναλυτικές πληροφορίες για την συσκευή /dev/md0. Αντικαταστήστε το /dev/md0 με την κατάλληλη συσκευή RAID.

- Για να προβάλλετε την κατάσταση ενός δίσκου σε μια συστοιχία:

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

Το αποτέλεσμα είναι παρόμοιο με αυτό της εντολής **mdadm -D**, προσαρμόστε το /dev/sda1 για κάθε δίσκο.

- Αν κάποιος δίσκος παρουσιάσει βλάβη και πρέπει να αφαιρεθεί από μία συστοιχία, πληκτρολογήστε:

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

Αλλάξτε τα /dev/md0 και /dev/sda1 με την κατάλληλη συσκευή RAID και δίσκο.

- Παρομοίως, για να προσθέσετε έναν νέο δίσκο:

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

Κάποιες φορές ένας δίσκος μπορεί να μεταβεί σε κατάσταση *ελαττωματικότητας* ακόμη και αν δεν υπάρχει κάποιο φυσικό πρόβλημα με τη συσκευή. Συνήθως αξίζει τον κόπο να αφαιρέσετε τη συσκευή από τη διάταξη και μετά να την επανατοποθετήσετε. Αυτό θα κάνει τη συσκευή να επανασυγχρονιστεί με τη διάταξη. Αν η συσκευή δεν συγχρονιστεί με τη διάταξη, είναι μια καλή ένδειξη ελαττωματικού υλικού.

Το αρχείο `/proc/mdstat` περιέχει επίσης χρήσιμες πληροφορίες για τις συσκευές RAID του συστήματος:

```
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>
```

Η ακόλουθη εντολή είναι πολύ καλή για την παρακολούθηση της κατάστασης μιας συσκευής που συγχρονίζεται:

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

Πιέστε `Ctrl+c` για να τερματίσετε την εντολή `watch`.

Εάν χρειάζεται να αντικαταστήσετε μία προβληματική συσκευή, αφού η συσκευή έχει αντικατασταθεί και συγχρονιστεί, θα χρειαστεί να είναι εγκατεστημένο το `grub`. Για να εγκαταστήσετε το `grub` στη νέα συσκευή, πληκτρολογήστε το ακόλουθο:

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

Αντικαταστήστε το `/dev/md0` με το κατάλληλο όνομα της συσκευής συστοιχίας.

4.1.6. Πόροι

Το θέμα των συστοιχιών RAID είναι πολύπλοκο λόγω της πληθώρας των τρόπων που μπορεί να ρυθμιστεί το RAID. Παρακαλούμε δείτε τους ακόλουθους συνδέσμους για περισσότερες πληροφορίες:

- *Ubuntu Wiki Articles on RAID*⁶.
- *Software RAID HOWTO*⁷
- *Διαχείριση του RAID σε Linux*⁸

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/>

4.2. Διαχειριστής λογικών τόμων (LVM)

Ο διαχειριστής λογικών τόμων, ή *LVM*, επιτρέπει στους διαχειριστές να δημιουργήσουν λογικούς τόμους από έναν ή πολλούς φυσικούς σκληρούς δίσκους. Οι τόμοι LVM μπορούν να δημιουργηθούν και σε κατατμήσεις RAID λογισμικού και σε τυπικές κατατμήσεις που βρίσκονται σε έναν δίσκο. Οι τόμοι μπορούν επίσης να επεκταθούν, δίνοντας μεγαλύτερη ευελιξία στα συστήματα καθώς οι απαιτήσεις αλλάζουν.

4.2.1. Επισκόπηση

Μία παρενέργεια της δύναμης και της ευελιξίας του LVM είναι ο μεγαλύτερος βαθμός πολυπλοκότητας. Πριν ξεκινήσετε με τη διαδικασία εγκατάστασης του LVM, είναι καλύτερα να εξοικειωθείτε με κάποιους όρους.

- *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 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. Εγκατάσταση

Σαν παράδειγμα, αυτή η ενότητα καλύπτει την εγκατάσταση του Ubuntu Server Edition με το */srv* να είναι προσαρτημένο σε έναν τόμο LVM. Κατά την αρχική εγκατάσταση, μόνο ένας φυσικός τόμος (PV) θα είναι μέρος της ομάδας τόμων (VG). Ένα άλλο PV θα προστεθεί μετά την εγκατάσταση ώστε να δειχθεί πώς μπορεί να επεκταθεί ένα VG.

Υπάρχουν αρκετές επιλογές εγκατάστασης για το LVM: "*Καθοδηγούμενη διαμέριση - χρήση ολόκληρου του δίσκου και ρύθμιση λογικών τόμων LVM*" που θα σας επιτρέψει επίσης να αποδώσετε ένα μέρος του διαθέσιμου χώρου σε LVM, "*Καθοδηγούμενη διαμέριση - χρήση ολόκληρου του δίσκου και ρύθμιση κρυπτογραφημένων τόμων LVM*", ή *Χειροκίνητη ρύθμιση των κατατμήσεων και του LVM*. Αυτή τη στιγμή, ο μοναδικός τρόπος για να ρυθμίσετε ένα σύστημα και με LVM και με τυπικές κατατμήσεις, κατά την εγκατάσταση, είναι να χρησιμοποιήσετε την χειροκίνητη διαμέριση.

1. Ακολουθήστε τα βήματα εγκατάστασης μέχρι να φτάσετε στο βήμα *Διαμέριση δίσκων*, μετά:
2. Στην οθόνη "*Διαμέριση δίσκων*" επιλέξτε "*Χειροκίνητη*".
3. Επιλέξτε τον σκληρό δίσκο και στην επόμενη οθόνη επιλέξτε "ναι" στο "*Δημιουργία νέου κενού πίνακα διαμέρισης σε αυτή τη συσκευή*".
4. Στη συνέχεια, δημιουργήστε τις τυπικές κατατμήσεις */boot*, *swap* και /με οποιοδήποτε σύστημα αρχείων προτιμάτε.

5. Για το LVM */srv*, δημιουργήστε μία νέα λογική κατάτμηση. Μετά αλλάξτε το "Χρήση ως" σε "φυσικός τόμος για το LVM" και μετά επιλέξτε "Ολοκλήρωση της ρύθμισης της κατάτμησης".
6. Τώρα επιλέξτε "Ρύθμιση του Διαχειριστή Λογικών Τόμων" στην κορυφή και επιλέξτε "Ναι" για να εγγραφούν οι αλλαγές στον δίσκο.
7. Για "Εργασία ρύθμισης του LVM" στην επόμενη οθόνη, επιλέξτε "Δημιουργία ομάδας τόμων". Πληκτρολογήστε ένα όνομα για το VG όπως *vg01*, ή κάτι πιο περιγραφικό. Αφού πληκτρολογήσετε ένα όνομα, επιλέξτε την κατάτμηση που ρυθμίστηκε για LVM και επιλέξτε "Συνέχεια".
8. Πίσω στην οθόνη "Εργασία ρύθμισης του LVM", επιλέξτε "Δημιουργία λογικού τόμου". Επιλέξτε την νέα ομάδα τόμου που δημιουργήσατε, και πληκτρολογήστε ένα όνομα για το νέο LV, για παράδειγμα *srv* μιας και αυτό είναι το προοριζόμενο σημείο προσάρτησης. Μετά επιλέξτε ένα μέγεθος, που μπορεί να είναι ολόκληρη η κατάτμηση καθώς μπορεί πάντα να επεκταθεί αργότερα. Επιλέξτε "Τέλος" και θα πρέπει να μεταφερθείτε πίσω στην κύρια οθόνη "Διαμέριση δίσκων".
9. Τώρα προσθέστε ένα σύστημα αρχείων στο νέο LVM. Επιλέξτε την κατάτμηση κάτω από το "LVM VG *vg01*, LV *srv*", ή όποιο όνομα έχετε διαλέξει, μετά επιλέξτε το *Χρήση ως*. Ρυθμίστε ένα σύστημα αρχείων ως συνήθως επιλέγοντας */srv* ως το σημείο προσάρτησης. Μόλις τελειώσετε, επιλέξτε "Ολοκλήρωση της ρύθμισης της κατάτμησης".
10. Τέλος, επιλέξτε "Ολοκλήρωση της διαμέρισης και αποθήκευση των αλλαγών στον δίσκο". Μετά επιβεβαιώστε τις αλλαγές και συνεχίστε με την υπόλοιπη εγκατάσταση.

Υπάρχουν κάποια χρήσιμα εργαλεία για να προβάλλετε πληροφορίες για το LVM:

- *pvdisplay*: shows information about Physical Volumes.
- *vgdisplay*: εμφανίζει πληροφορίες για τις ομάδες τόμων.
- *lvdisplay*: shows information about Logical Volumes.

4.2.3. Επέκταση ομάδων τόμων

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. Πρώτα, δημιουργήστε τον φυσικό τόμο, σε ένα τερματικό εκτελέστε:

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

2. Τώρα επεκτείνετε την ομάδα τόμων (VG):

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

3. Χρησιμοποιήστε το `vgdisplay` για να βρείτε τις ελεύθερες φυσικές εκτάσεις - Ελεύθερο PE / μέγεθος (το μέγεθος που μπορείτε να προσδώσετε). Θα υποθέσουμε πως υπάρχει ελεύθερο μέγεθος 511 PE (ισούται με 2GB με μέγεθος PE 4MB) και θα χρησιμοποιήσουμε ολόκληρο τον διαθέσιμο ελεύθερο χώρο. Χρησιμοποιήστε το δικό σας μέγεθος PE και/ή ελεύθερο χώρο.

Ο λογικός τόμος (LV) μπορεί τώρα να επεκταθεί με διαφορετικές μεθόδους, εμείς θα δούμε μόνο πώς να χρησιμοποιήσετε το PE για να επεκτείνετε το LV:

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

Η επιλογή `-l` επιτρέπει στο LV να επεκταθεί με τη χρήση του PE. Η επιλογή `-L` επιτρέπει στο LV να επεκταθεί χρησιμοποιώντας Meg, Gig, Tera, κτλ 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).

Οι ακόλουθες εντολές είναι για συστήματα αρχείων *EXT3* ή *EXT4*. Αν χρησιμοποιείτε άλλο σύστημα αρχείων, μπορεί να υπάρχουν άλλα εργαλεία διαθέσιμα.

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

Η επιλογή `-f` του `e2fsck` κάνει εξαναγκαστικό έλεγχο, ακόμη και αν το σύστημα φαίνεται καθαρό.

5. Τέλος, αλλάξτε το μέγεθος του συστήματος αρχείων:

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

6. Τώρα προσαρτήστε την κατάτμηση και ελέγξτε το μέγεθός της.

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

4.2.4. Πόροι

- See the *Ubuntu Wiki LVM Articles*⁹.

⁹ <https://help.ubuntu.com/community/Installation#lvm>

- Δείτε το *HOWTO του LVM*¹⁰ για περισσότερες πληροφορίες.
- Ένα άλλο καλό άρθρο είναι το *Managing Disk Space with LVM*¹¹ στον ιστότοπο του O'Reilly linuxdevcenter.com.
- For more information on fdisk see the *fdisk man page*¹².

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/raring/en/man8/fdisk.8.html>

5. Kernel Crash Dump

5.1. Εισαγωγή

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. Εγκατάσταση

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

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

A reboot is then needed.

5.4. Ρυθμίσεις

No further configuration is required in order to have the kernel dump mechanism enabled.

5.5. Έλεγχος

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)
```

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. Πόροι

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>

Κεφάλαιο 3. Διαχείριση Πακέτων

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 35,000 software packages for your Ubuntu computer, the package management facilities also feature dependency resolution capabilities and software update checking.

Υπάρχουν πολλά διαθέσιμα εργαλεία για που αλληλεπιδρούν με το σύστημα διαχείρισης πακέτων, από απλές λειτουργίες γραμμής-εντολών που μπορούν να αυτοματοποιηθούν εύκολα από τους διαχειριστές συστήματος, σε απλές γραφικές διεπαφές με εύκολη χρήση για τους νέους στο Ubuntu.

1. Εισαγωγή

Το σύστημα διαχείρισης πακέτων Ubuntu προέρχεται από το ίδιο σύστημα που χρησιμοποιείται από την έκδοση Debian GNU/Linux. Τα αρχεία πακέτων περιέχουν όλα τα κατάλληλα αρχεία, μετα-δεδομένα, και πληροφορίες για την εφαρμογή μια συγκεκριμένης λειτουργίας ή εφαρμογής λογισμικού στον υπολογιστή Ubuntu σας.

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

2. dpkg

dpkg is a package manager for *Debian*-based systems. It can install, remove, and build packages, but unlike other package management 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

- Ανάλογα με τον όγκο των πακέτων στο σύστημά σας, αυτό μπορεί να παράγει ένα μεγάλο όγκο εξόδου. Διοχετεύστε την έξοδο μέσω `grep` για να δείτε εάν ένα συγκεκριμένο πακέτο έχει εγκατασταθεί:

dpkg -l | grep apache2

Αντικαταστήστε το *apache2* με οποιοδήποτε όνομα πακέτου, ή άλλες κανονικές επεκτάσεις.

- Για να καταγράψετε τα αρχεία που έχουν εγκατασταθεί από ένα πακέτο, σε αυτή την περίπτωση το πακέτο `ufw`, πληκτρολογήστε:

dpkg -L ufw

- Εάν δεν είστε σίγουροι ποιο πακέτο εγκατέστησε ένα αρχείο, η `dpkg -S` μπορεί να είναι ικανό να σας πει. Για παράδειγμα:

dpkg -S /etc/host.conf

base-files: /etc/host.conf

Η έξοδος δείχνει ότι το `/etc/host.conf` ανήκει στο πακέτο `base-files`.



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.

- Μπορείτε να εγκαταστήσετε ένα τοπικό αρχείο *.deb* πληκτρολογώντας:

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.

- Η απεγκατάσταση ενός πακέτου μπορεί να επιτευχθεί:

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.

Για περισσότερες επιλογές `dpkg` δείτε τη σελίδα: **`man dpkg`**.

3. Apt-Get

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

Μερικά παραδείγματα δημοφιλών χρήσεων της λειτουργίας apt-get:

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

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

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

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



Πολλαπλά Πακέτα: Μπορείτε να προσδιορίσετε πολλαπλά πακέτα να εγκατασταθούν ή να αφαιρεθούν, χωρισμένα με κενά.

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

- **Update the Package Index:** The APT package index is essentially a database of available packages from the repositories defined in the `/etc/apt/sources.list` file 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-get update
```

- **Αναβάθμιση Πακέτων:** Σε πάροδο χρόνου, αναβαθμισμένες εκδόσεις πακέτων που είναι εγκαταστημένα στον υπολογιστή σας μπορεί να γίνουν διαθέσιμες από το πακέτο αποθετηρίων (για παράδειγμα ενημερώσεις ασφαλείας). Για να αναβαθμίσετε το σύστημά σας, πρώτα ενημερώστε το ευρετήριο πακέτου όπως περιγράφεται παραπάνω, και μετά πληκτρολογήστε:

```
sudo apt-get upgrade
```


Για πληροφορίες με το πως να αναβαθμίσετε μία καινούρια έκδοση Ubuntu δείτε *Τμήμα 3, Αναβάθμιση* [9].

Ενέργειες της εντολής `apt-get`, όπως εγκατάσταση και αφαίρεση πακέτων, καταγράφονται στο `/var/log/dpkg.log` αρχείο ιστορικού.

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

`apt-get help`

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

4. Aptitude

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.

Η χρήση του Aptitude για διαχείριση πακέτων είναι σχετικά απλή, και η διεπαφή του χρήστη κάνει απλές διεργασίες εύκολες να εκτελεστούν. Τα ακόλουθα είναι παραδείγματα κοινών λειτουργιών διαχείρισης πακέτων όπως εκτελέστηκαν στο 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 you will be prompted to become root to complete the installation. Press **ENTER** which will result in a *Password:* prompt. Enter your user password to become root. Finally, press **g** once more and you'll be prompted to download the package. Press **ENTER** on the *Continue* prompt, and downloading and installation of the package will commence.
- **Remove Packages:** To remove a package, locate the package via the *Installed Packages* package category, 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 you will be prompted to become root to complete the removal. Press **ENTER** which will result in a *Password:* prompt. Enter your user password to become root. Finally, press **g** once more, then press **ENTER** on the *Continue* prompt, and removal of the package will commence.
- **Update Package Index:** To update the package index, simply press the **u** key and you will be prompted to become root to complete the update. Press **ENTER** which will result in a *Password:* prompt. Enter your user password to become root. Updating of the package index will commence. Press **ENTER** on the *OK* prompt when the download dialog is presented to complete the process.

- **Upgrade Packages:** To upgrade packages, perform the update of the package index as detailed above, and then press the **U** key to mark all packages with updates. Now press **g** whereby you'll be presented with a summary of package actions. Press **g** again, and you will be prompted to become root to complete the installation. Press **ENTER** which will result in a *Password:* prompt. Enter your user password to become root. Finally, press **g** once more, and you'll be prompted to download the packages. Press **ENTER** on the *Continue* prompt, and upgrade of the packages will commence.

Η πρώτη στήλη πληροφοριών που προβάλλεται στη λίστα πακέτων στο πρώτο παράθυρο, όταν προβάλλετε πακέτα καταγράφει την τρέχουσα κατάσταση των πακέτων, και χρησιμοποιεί το ακόλουθο κλειδί για να περιγράψει την κατάσταση του πακέτου:

- **i:** Εγκαταστημένο πακέτο
- **c:** Πακέτο μη εγκαταστημένο, αλλά η διαμόρφωση πακέτου παραμένει στο σύστημα.
- **p:** Καθαρισμένο από το σύστημα
- **v:** Εικονικό πακέτο
- **B:** Σπασμένο πακέτο
- **u:** Ασυσκεύαστα αρχεία, αλλά χωρίς να έχει διαμορφωθεί το πακέτο ακόμα
- **C:** Μισο-διαμορφωμένα - Η διαμόρφωση απέτυχε και απαιτεί διόρθωση
- **H:** Μισο-εγκαταστημένα - Η αφαίρεση απέτυχε και απαιτεί διόρθωση

Για να εξέλθετε από το Aptitude, απλά πατήστε το πλήκτρο **q** και επιβεβαιώστε ότι θέλετε να εξέλθετε. Πολλές άλλες λειτουργίες είναι διαθέσιμες στο μενού Aptitude πατώντας το πλήκτρο **F10**.

4.1. Command Line Aptitude

You can also use Aptitude as a command-line tool, similar to apt-get. To install the nmap package with all necessary dependencies, as in the apt-get 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. Αυτόματες Ενημερώσεις

Το πακέτο `unattended-upgrades` μπορεί να χρησιμοποιηθεί για να εγκαθιστώνται αυτόματα οι ενημερώσεις πακέτων, και μπορεί να διαμορφωθεί να ενημερώνει όλα τα πακέτα ή απλά να εγκαθιστά ενημερώσεις ασφαλείας. Πρώτον, εγκαταστήστε το πακέτο πληκτρολογώντας τα ακόλουθα σε ένα τερματικό:

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

Για να διαμορφώσετε το `unattended-upgrades`, επεξεργαστείτε το `/etc/apt/apt.conf.d/50unattended-upgrades` και προσαρμόστε τα ακόλουθα ώστε να ταιριάζουν στις ανάγκες σας:

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

Ορισμένα πακέτα μπορούν να *μποουν στη μαύρη λίστα* και έτσι να μην ενημερωθούν αυτόματα. Για να βάλετε ένα πακέτο στη μαύρη λίστα, προσθέστε το στη λίστα:

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



Η γραμμές με διπλή `/*` λειτουργούν σα σχόλια, έτσι ότι ακολουθεί μετά από `/*` δε θα αξιολογηθεί.

To enable automatic updates, edit `/etc/apt/apt.conf.d/10periodic` 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.



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

Τα αποτελέσματα του `unattended-upgrades` θα καταγραφούν στο `/var/log/unattended-upgrades`.

5.1. Κοινοποιήσεις

Η διαμόρφωση του *Unattended-Upgrade::Mail* στο `/etc/apt/apt.conf.d/50unattended-upgrades` θα ενεργοποιήσει το `unattended-upgrades` να στείλει email σε ένα διαχειριστή δίνοντας λεπτομέρειες για κάθε πακέτο που χρειάζεται αναβάθμιση ή έχει προβλήματα.

Ένα άλλο χρήσιμο πακέτο είναι το `apticron`. Το `apticron` θα διαμορφώσει μια δουλειά `cron` να στείλει email σε ένα διαχειριστή πληροφορίες για πακέτα στο σύστημα που έχουν διαθέσιμες ενημερώσεις, καθώς και μια περίληψη αλλαγών σε κάθε πακέτο.

Για να εγκαταστήσετε το πακέτο `apticron`, σε ένα τερματικό πληκτρολογήστε:

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

Όταν το πακέτο εγκατασταθεί επεξεργαστείτε το `/etc/apticron/apticron.conf`, για να δείτε τη διεύθυνση ηλεκτρονικού ταχυδρομείου και άλλες επιλογές:

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

6. Ρυθμίσεις

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.

Μπορείτε να επεξεργαστείτε το αρχείο για να ενεργοποιήσετε ή να απενεργοποιήσετε αποθετήρια. Για παράδειγμα, για να απενεργοποιήσετε τη απαίτηση εισαγωγής του Ubuntu CD-ROM όποτε προκύπτουν λειτουργίες πακέτου, απλώς αποσχολιάστε την κατάλληλη γραμμή για το CD-ROM, η οποία εμφανίζεται στην κορυφή του αρχείου:

```
# no more prompting for CD-ROM please
# deb cdrom:[Ubuntu 13.04 _Raring Ringtail_ - Release i386 (20111013.1)]/ raring main restricted
```

6.1. Επιπλέον Αποθετήρια

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.



Τα πακέτα στο αποθετήριο *Multiverse* συχνά έχουν θέματα άδειας που τα αποτρέπει από το να διανέμονται με ένα ελεύθερο λειτουργικό σύστημα, και μπορεί να είναι παράνομα στην τοποθεσία σας.



Πληροφορηθείτε ότι ούτε το *Universe* ούτε *Multiverse* αποθετήριο περιέχουν επισήμως υποστηριζόμενα πακέτα. Συγκεκριμένα, μπορεί να μην υπάρχουν ενημερώσεις ασφαλείας για τα συγκεκριμένα πακέτα.

Πολλές άλλες πηγές πακέτων είναι διαθέσιμες, μερικές ακόμα προσφέρουν μόνο ένα πακέτο, όπως στην περίπτωση των πηγών πακέτων που παρέχονται από τον προγραμματιστή μιας εφαρμογής. Θα πρέπει πάντα να είστε πολύ προσεκτικοί και επιφυλακτικοί όταν χρησιμοποιείτε μη-κοινές πηγές πακέτων, όμως. Ερευνήστε την πηγή και τα πακέτα προσεκτικά πριν εκτελέσετε κάποια εγκατάσταση, καθώς μερικές πηγές πακέτων και τα πακέτα τους μπορεί να καταστήσουν το σύστημά σας ασταθές ή μη-λειτουργικό σε ορισμένες απόψεις.

Εξορισμού, τα αποθετήρια *Universe* και *Multiverse* είναι ενεργοποιημένα αλλά εάν θα θέλατε να τα απενεργοποιήσετε επεξεργαστείτε το `/etc/apt/sources.list` και σχολιάστε τις ακόλουθες γραμμές.

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

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

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

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

7. Αναφορές

Το περισσότερο από το υλικό που καλύπτεται σε αυτό το κεφάλαιο είναι διαθέσιμο στις σελίδες *man*, πολλές από τις οποίες είναι διαθέσιμες 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-get man page*⁵ contain useful information regarding *apt-get* usage.
- See the *aptitude man page*⁶ for more *aptitude* options.
- Η σελίδα *Adding Repositories HOWTO (Ubuntu Wiki)*⁷ περιέχει περισσότερες λεπτομέρειες για την προσθήκη αποθετηρίων.

² <https://help.ubuntu.com/community/InstallingSoftware>

³ <http://manpages.ubuntu.com/manpages/raring/en/man1/dpkg.1.html>

⁴ <http://www.debian.org/doc/manuals/apt-howto/>

⁵ <http://manpages.ubuntu.com/manpages/raring/en/man8/apt-get.8.html>

⁶ <http://manpages.ubuntu.com/manpages/raring/man8/aptitude.8.html>

⁷ <https://help.ubuntu.com/community/Repositories/Ubuntu>

Κεφάλαιο 4. Δικτύωση

Τα δίκτυα απαρτίζονται από δύο ή περισσότερες συσκευές, όπως υπολογιστικά συστήματα, εκτυπωτές και σχετικό εξοπλισμό τα οποία είναι συνδεδεμένα είτε με φυσικά καλώδια ή με ασύρματους συνδέσμους με σκοπό να μοιράζονται και να διανέμουν πληροφορίες μεταξύ των συνδεδεμένων συσκευών.

Αυτή η ενότητα παρέχει γενικές και συγκεκριμένες πληροφορίες που αφορούν τη δικτύωση, και που περιλαμβάνουν μια επισκόπηση έννοιες δικτύου και λεπτομερή συζήτηση δημοφιλών πρωτοκόλλων δικτύου.

1. Διαμόρφωση Δικτύου

Το Ubuntu στέλνεται με έναν αριθμό γραφικών λειτουργιών για να διαμορφώσετε τις συσκευές δικτύου σας. Αυτό το έγγραφο είναι προσανατολισμένο σε διαχειριστές διακομιστή και θα εστιάσει στη διαχείριση του δικτύου σας στη γραμμή εντολών.

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-get 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`. 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 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.

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



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. Γεφύρωση

Η γεφύρωση πολλαπλών διεπαφών είναι μια πιο προηγμένη διαμόρφωση, αλλά είναι πολύ χρήσιμη για πολλά σενάρια. Ένα σενάριο είναι το στήσιμο μιας γέφυρας με πολλαπλές διεπαφές δικτύου, μετά η χρησιμοποίηση ενός τείχους προστασίας για να φιλτράρετε την κίνηση μεταξύ δύο τμημάτων δικτύου. Ένα άλλο σενάριο είναι η χρησιμοποίηση γέφυρας σε ένα σύστημα με μία διεπαφή για να επιτρέψετε σε εικονικές μηχανές άμεση πρόσβαση στο εξωτερικό δίκτυο. Το ακόλουθο παράδειγμα καλύπτει το δεύτερο σενάριο.

Πριν διαμορφώσετε μια γέφυρα θα πρέπει να εγκαταστήσετε το πακέτο `bridge-utils`. Για να εγκαταστήσετε το πακέτο, σε ένα τερματικό πληκτρολογήστε:

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

Μετά, διαμορφώστε τη γέφυρα κάνοντας επεξεργασία του `/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
```



Εισάγετε τις κατάλληλες τιμές για τη φυσική σας διεπαφή και δίκτυο.

Τώρα επανεκκινήστε τη δικτύωση για να ενεργοποιήσετε τη γέφυρα διεπαφής:

```
sudo service networking restart
```

Η καινούρια διεπαφή γέφυρας θα πρέπει τώρα να εκτελείτε. Το `brctl` παρέχει χρήσιμες πληροφορίες για την κατάσταση της γέφυρας, ελέγχει ποιες διεπαφές είναι μέρος της γέφυρας, κλπ. Δείτε το **man brctl** για περισσότερες πληροφορίες.

1.5. Πόροι

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

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>

⁷ <http://manpages.ubuntu.com/manpages/man8/brctl.8.html>

⁸ <http://www.linuxfoundation.org/en/Net:Bridge>

2. TCP/IP

Το Πρωτόκολλο Ελέγχου Μετάφρασης και το Πρωτόκολλο Διαδικτύου (TCP/IP) είναι ένα σταθερό σύνολο πρωτοκόλλων που αναπτύχθηκαν στα τέλη του 1970 από την Υπηρεσία Άμυνας Προηγμένης Έρευνας Έργου (DARPA) σαν μέσω επικοινωνίας μεταξύ δύο διαφορετικών τύπων υπολογιστών και δικτύων υπολογιστών. Το TCP/IP είναι η κινούμενη δύναμη του Ίντερνετ, και έτσι είναι το πιο δημοφιλές σύνολο πρωτοκόλλων δικτύου στη Γη.

2.1. Εισαγωγή TCP/IP

Τα δύο συστατικά πρωτόκολλα του TCP/IP αντιμετωπίζουν διαφορετικά πτυχές της δικτύωσης υπολογιστών. Το *Πρωτόκολλο Διαδικτύου*, το "IP" του TCP/IP είναι ένα πρωτόκολλο χωρίς συνδέσεις το οποίο ασχολείται μόνο με τη δρομολόγηση πακέτων δικτύου χρησιμοποιώντας το *IP Datagram* σαν τη βασική μονάδα της δικτύωσης πληροφοριών. Το IP Datagram αποτελείται από μια κεφαλίδα που ακολουθείται από ένα μήνυμα. Το *Πρωτόκολλο Ελέγχου Μετάφρασης* είναι το "TCP" στο TCP/IP και ενεργοποιεί κεντρικούς υπολογιστές δικτύου για να θεσπίσει συνδέσεις οι οποίες μπορούν να χρησιμοποιηθούν για ανταλλαγή ροών δεδομένων. Το TCP εγγυάται ότι τα δεδομένα μεταξύ συνδέσεων παραδίδονται και φτάνουν σε ένα κεντρικό υπολογιστή στην ίδια σειρά με την οποία στάλθηκαν από έναν άλλο κεντρικό υπολογιστή δικτύου.

2.2. Διαμόρφωση TCP/IP

Η διαμόρφωση του πρωτοκόλλου TCP/IP αποτελείται από πολλά στοιχεία τα οποία πρέπει να οριστούν κάνοντας επεξεργασία στα κατάλληλα αρχεία διαμόρφωσης, ή αναπτύσσοντας λύσεις όπως ο διακομιστής Πρωτοκόλλου Δυναμικής Διαμόρφωσης Κεντρικού Υπολογιστή (DHCP) οποίος με τη σειρά του, μπορεί να διαμορφωθεί για να παρέχει τις κατάλληλες ρυθμίσεις διαμόρφωσης σε πελάτες δικτύου αυτόματα. Αυτές οι τιμές διαμόρφωσης πρέπει να οριστούν σωστά ώστε να διευκολύνεται η κατάλληλη λειτουργία δικτύου του συστήματος Ubuntu σας.

Τα στοιχεία της κοινής διαμόρφωσης του TCP/IP και οι σκοποί τους είναι όπως ακολούθως:

- **IP διεύθυνση** Η διεύθυνση IP είναι μια μοναδική συμβολοσειρά εκφρασμένη σαν τέσσερις δεκαδικοί αριθμοί με εμβέλεια από μηδέν (0) μέχρι διακόσια πενήντα πέντε (255), χωρισμένοι με τελείες, με κάθε ένα από τους τέσσερις αριθμούς να εκπροσωπούν οκτώ (8) bits της διεύθυνσης για ένα συνολικό μέγεθος τριάντα δύο (32) bits για όλη τη διεύθυνση. Αυτή η μορφή ονομάζεται *διάστικη τετράδυμη σημειογραφία*.
- **Μάσκα Δικτύου** Η Μάσκα Υποδικτύου (ή απλά *μάσκα δικτύου*) είναι μια τοπική μάσκα bit, ή σύνολο σημαίων που χωρίζει τα μέρη μια IP διεύθυνσης σημαντικής για το δίκτυο από τα bits που είναι σημαντικά για το *υποδίκτυο*. Για παράδειγμα, σε ένα υποδίκτυο Κλάσης Γ, η κανονική μάσκα δικτύου είναι 255.255.255.0 η οποία καλύπτει τα πρώτα

τρία bytes μιας διεύθυνσης IP και επιτρέπει στο τελευταίο byte της διεύθυνσης IP να παραμείνει διαθέσιμο για προσδιορισμό κεντρικών υπολογιστών στο υποδίκτυο.

- **Διεύθυνση Δικτύου** Η Διεύθυνση Δικτύου αντιπροσωπεύει τα bytes που περιλαμβάνει το τμήμα δικτύου της διεύθυνσης IP. Για παράδειγμα, ο κεντρικός υπολογιστής 12.128.1.2 σε ένα δίκτυο Κλάσης Α θα χρησιμοποιούσε την 12.0.0.0 σε διεύθυνση δικτύου, όπου το δώδεκα (12) αντιπροσωπεύει το πρώτο byte της διεύθυνσης IP, (το μέρος δικτύου) και τα μηδενικά (0) σε όλα από τα υπόλοιπα τρία bytes θα αντιπροσωπεύουν τους πιθανούς κεντρικούς υπολογιστές. Ένας κεντρικός υπολογιστής που χρησιμοποιεί την ιδιωτική διεύθυνση IP 192.168.1.100 με τη σειρά του θα χρησιμοποιούσε μια Διεύθυνση Δικτύου 192.168.1.0, η οποία ορίζει τα τρία πρώτα bytes του δικτύου 192.168.1 Κλάσης Γ και ένα μηδενικό (0) για όλους τους πιθανούς κεντρικούς υπολογιστές του δικτύου.
- **Διεύθυνση Εκπομπής** Η Διεύθυνση Εκπομπής είναι μια διεύθυνση IP που επιτρέπει στα δεδομένα δικτύου να στέλνονται ταυτόχρονα σε όλους τους κεντρικούς υπολογιστές σε ένα δοσμένο υποδίκτυο αντί να προσδιορίζεται ένας συγκεκριμένος χρήστης. Η πρότυπη διεύθυνση εκπομπής για δίκτυα IP είναι 255.255.255.255, αλλά αυτή η διεύθυνση εκπομπής δεν μπορεί να χρησιμοποιηθεί για να σταλεί ένα μήνυμα εκπομπής σε κάθε κεντρικό υπολογιστή το Ίντερνετ γιατί οι δρομολογητές το μπλοκάρουν. Μια πιο κατάλληλη διεύθυνση εκπομπής ορίζεται να ταιριάζει με ένα συγκεκριμένο υποδίκτυο. Για παράδειγμα, στο ιδιωτικό δίκτυο IP Κλάσης Γ, 192.168.1.0, η διεύθυνση εκπομπής είναι 192.168.1.255. Τα μηνύματα εκπομπής παράγονται τυπικά από πρωτόκολλα δικτύου όπως το πρωτόκολλο Επίλυσης Διεύθυνσης (ARP) και το Πρωτόκολλο Πληροφοριών Δρομολόγησης (RIP)
- **Διεύθυνση Πυλώνα** Μια Διεύθυνση Πυλώνα είναι η διεύθυνση IP μέσω της οποίας ένα συγκεκριμένο δίκτυο, ή κεντρικός υπολογιστής σε δίκτυο, μπορεί να βρεθεί. Εάν ένας κεντρικός υπολογιστής δικτύου επιθυμεί να επικοινωνήσει με έναν άλλο κεντρικό υπολογιστή δικτύου, και αυτός ο υπολογιστής δε βρίσκεται στο ίδιο δίκτυο, τότε πρέπει να χρησιμοποιηθεί ένας *πυλώνας*. Σε πολλές περιπτώσεις, η Διεύθυνση Πυλώνα θα είναι αυτή ενός δρομολογητή στο ίδιο δίκτυο, ο οποίος εν συνεχεία θα μεταφέρει κίνηση σε άλλα δίκτυα ή κεντρικούς υπολογιστές, όπως κεντρικούς υπολογιστές Ίντερνετ. Η τιμή της ρύθμισης Διεύθυνσης Πυλώνα πρέπει να είναι σωστή, αλλιώς το σύστημά σας δε θα μπορεί να βρει κανέναν κεντρικό υπολογιστή πέρα από αυτούς του ίδιου δικτύου.
- **Διεύθυνση Ονόματος Διακομιστή** Οι Διευθύνσεις Ονόματος Διακομιστή εκπροσωπούν το σύστημα Υπηρεσίας Ονόματος Τομέα (DNS), το οποίο επιλύει ονόματα κεντρικών υπολογιστών δικτύου σε διευθύνσεις IP. Υπάρχουν τρία επίπεδα Διευθύνσεων Ονόματος Διακομιστή, που μπορούν να προσδιοριστούν με σειρά προτεραιότητας: Το *Πρωτογενές Όνομα Διακομιστή*, το *Δευτερογενές Όνομα Διακομιστή*, και το *Τριτογενές Όνομα Διακομιστή*. Για να μπορεί το σύστημά σας να επιλύει ονόματα κεντρικών υπολογιστών δικτύου στις αντίστοιχες διευθύνσεις IP, πρέπει να προσδιορίσετε έγκυρες Διευθύνσεις Ονομάτων Διακομιστή τις οποίες είστε εξουσιοδοτημένοι να χρησιμοποιείτε στη διαμόρφωση TCP/IP του συστήματός σας. Σε πολλές περιπτώσεις αυτές οι διευθύνσεις

μπορούν να παρασχεθούν από τον παροχέα υπηρεσιών δικτύου σας, αλλά υπάρχουν πολλά διαθέσιμα δωρεάν και προσβάσιμα δημοσίως ονόματα διακομιστών για χρήση, όπως οι διακομιστές Level3 (Verizon) με διευθύνσεις IP από 4.2.2.1 μέχρι 4.2.2.6.



Οι διευθύνσεις IP, η Μάσκα Δικτύου, η Διεύθυνση Δικτύου, η Διεύθυνση Εκπομπής, και η Διεύθυνση Πυλώνα είναι τυπικά προσδιορισμένες μέσω των κατάλληλων κωδικών παραπομπής στο αρχείο `/etc/network/interfaces`. Οι Διευθύνσεις Ονόματος Διακομιστή είναι προσδιορισμένες μέσω κωδικών παραπομπής `nameserver` στο αρχείο `/etc/resolv.conf`. Για περισσότερες πληροφορίες, δείτε τη σελίδα εγχειριδίου συστήματος για `dhclient` ή `resolv.conf` αντίστοιχα, με τις ακόλουθες εντολές σε ένα τερματικό εντολών:

Δείτε τη σελίδα εγχειριδίου για `dhclient` με την ακόλουθη εντολή:

man interfaces

Δείτε τη σελίδα εγχειριδίου `resolv.conf` με την ακόλουθη εντολή:

man resolv.conf

2.3. Δρομολόγηση IP

Η δρομολόγηση IP είναι ένα μέσω προσδιορισμού και ανακάλυψης μονοπατιών στο δίκτυο TCP/IP μαζί με το ποια δεδομένα μπορεί να αποσταλούν. Η δρομολόγηση χρησιμοποιεί ένα σύνολο *πινάκων δρομολόγησης* για να κατευθύνει την προώθηση πακέτων δεδομένων δικτύου από την πηγή στον προορισμό, συχνά μέσω ενδιάμεσων κόμβων δικτύου γνωστών ως *δρομολογητές*. Υπάρχουν δύο κύριες μορφές δρομολόγησης IP: *Στατική Δρομολόγηση* και *Δυναμική Δρομολόγηση*.

Η Στατική Δρομολόγηση περιλαμβάνει χειροκίνητη πρόσθεση δρομολογητών IP στον πίνακα δρομολόγησης, και αυτό γίνεται συνήθως χειραγωγώντας τον πίνακα δρομολόγησης με τον εντολή `route`. Η στατική δρομολόγηση έχει πολλά πλεονεκτήματα σε σχέση με τη δυναμική δρομολόγηση, όπως η απλότητα υλοποίησης για μικρότερα δίκτυα, η προβλεψιμότητα (ο πίνακας δρομολόγησης πάντα υπολογίζεται εκ των προτέρων, και έτσι η διαδρομή είναι ακριβώς η ίδια κάθε φορά που χρησιμοποιείται), και η χαμηλή επιβάρυνση στους άλλους δρομολογητές και συνδέσεις του δικτύου λόγω της έλλειψης μιας δυναμικής δρομολόγησης του πρωτοκόλλου. Ωστόσο, η στατική δρομολόγηση ενέχει κάποια μειονεκτήματα, επίσης. Για παράδειγμα, η στατική δρομολόγηση περιορίζεται σε μικρά δίκτυα και δεν κλιμακώνεται καλά. Η στατική δρομολόγηση επίσης αποτυγχάνει εντελώς να προσαρμοστεί στις διακοπές του δικτύου και τις αποτυχίες κατά μήκος της διαδρομής, λόγω της σταθερής φύσης της διαδρομής.

Η Δυναμική Δρομολόγηση βασίζεται σε μεγάλα δίκτυα με πολλές πιθανές διαδρομές IP από μια πηγή σε έναν προορισμό και κάνει χρήση μερικών ειδικών πρωτοκόλλων, όπως το

Πρωτόκολλο Πληροφορίας Δρομολόγησης (RIP), το οποίο διαχειρίζεται αναπροσαρμογές στους πίνακες δρομολόγησης που κάνει τη δυναμική δρομολόγηση εφικτή. Η δυναμική δρομολόγηση έχει αρκετά πλεονεκτήματα σε σχέση με τη στατική δρομολόγηση, όπως εξαιρετική επεκτασιμότητα και την ικανότητα προσαρμογής στις αποτυχίες και διακοπές κατά μήκος των διαδρομών του δικτύου. Επιπλέον, υπάρχει λιγότερη χειρωνακτική διαμόρφωση των πινάκων δρομολόγησης, επειδή οι δρομολογητές μαθαίνουν ο ένας από τον άλλο για την ύπαρξή τους και τις διαθέσιμες διαδρομές. Αυτό το χαρακτηριστικό καταργεί επίσης τη δυνατότητα θέσπισης λάθους στους πίνακες δρομολόγησης μέσω ανθρώπινου λάθους. Η δυναμική δρομολόγηση δεν είναι τέλεια, όμως, και παρουσιάζει μειονεκτήματα, όπως η αυξημένη πολυπλοκότητα και η πρόσθετη επιβάρυνση του δικτύου από επικοινωνίες δρομολογητών, η οποία δεν ωφελεί άμεσα τους τελικούς χρήστες, αλλά εξακολουθεί να καταναλώνει εύρος ζώνης δικτύου.

2.4. TCP και UDP

Το TCP είναι ένα πρωτόκολλο βασισμένο στη σύνδεση, το οποίο προσφέρει διόρθωση σφαλμάτων και εγγυημένη παράδοση δεδομένων μέσω αυτού που είναι γνωστό ως *έλεγχος ροής*. Ο έλεγχος ροής καθορίζει πότε η ροή ενός ρεύματος δεδομένων πρέπει να σταματήσει, και πότε πακέτα δεδομένων που έχουν σταλεί πριν πρέπει να ξανασταλούν λόγω προβλημάτων όπως οι *συγκρούσεις*, για παράδειγμα, διασφαλίζοντας έτσι πλήρη και ακριβή παράδοση δεδομένων. Το TCP χρησιμοποιείται τυπικά στην ανταλλαγή σημαντικών πληροφοριών όπως συναλλαγές βάσης δεδομένων.

Το Πρωτόκολλο Διαγραμμάτων Δεδομένων Χρήστη (UDP), από την άλλη, είναι ένα πρωτόκολλο *χωρίς συνδέσεις* το οποίο σπάνια ασχολείται με τη μεταφορά σημαντικών δεδομένων επειδή δεν έχει έλεγχο ροής ή οποιαδήποτε άλλη μέθοδο για να διασφαλίσει την αξιόπιστη μεταφορά δεδομένων. Το UDP χρησιμοποιείται συνήθως σε αναπαραγωγή ήχου και βίντεο, όπου θεωρείτε πιο γρήγορο από το TCP λόγω της έλλειψης διόρθωσης σφαλμάτων και ελέγχου ροής, και όπου η απώλεια κάποιων πακέτων δεν είναι γενικά καταστροφική.

2.5. ICMP

Το Πρωτόκολλο Ελέγχου Μηνυμάτων Ίντερνετ (ICMP) είναι μια προέκταση του Πρωτοκόλλου Διαδικτύου (IP) όπως ορίζετε στην Αίτηση για Σχόλια (RFC) #792 και υποστηρίζει πακέτα δικτύου που περιέχουν μηνύματα ελέγχου, σφαλμάτων, και πληροφοριακά μηνύματα. Το ICMP χρησιμοποιείται από εφαρμογές δικτύου όπως η λειτουργία ping, η οποία μπορεί να προσδιορίσει τη διαθεσιμότητα ενός κεντρικού υπολογιστή ή συσκευής δικτύου. Παραδείγματα μερικών μηνυμάτων σφαλμάτων που επιστρέφονται από το ICMP τα οποία είναι χρήσιμα και για κεντρικούς υπολογιστές δικτύου και για συσκευές όπως δρομολογητές, περιλαμβάνουν τα *Απρόσιτος Προορισμός* και *Λήξη Χρονικού Ορίου*.

2.6. Δαίμονες

Οι δαίμονες είναι ειδικές εφαρμογές συστήματος η οποίες τυπικά εκτελούνται συνεχώς στο παρασκήνιο και περιμένουν αιτήματα για τις λειτουργίες που παρέχουν από άλλες εφαρμογές. Πολλοί δαίμονες είναι δίκτυο-κεντρικοί, αυτό σημαίνει ότι, ένας μεγάλος αριθμός δαιμόνων που εκτελούνται στο παρασκήνιο σε ένα σύστημα Ubuntu μπορεί να παρέχει λειτουργικότητα σχετική με το δίκτυο. Μερικά παραδείγματα περιλαμβάνουν το *Δαίμονα Πρωτοκόλλου Μεταφοράς Υπερκειμένου* (httpd), ο οποίος παρέχει λειτουργικότητα διακομιστή ιστού, το *Δαίμονα Ασφαλούς Κελύφους* (sshd), ο οποίος παρέχει ασφαλή απομακρυσμένη είσοδο κελύφους και δυνατότητες μεταφοράς αρχείων, και το *Δαίμονα Πρωτοκόλλου Πρόσβασης Μηνυμάτων Διαδικτύου* (imapd), οποίος παρέχει υπηρεσίες Ηλεκτρονικής Αλληλογραφίας.

2.7. Πόροι

- There are man pages for *TCP*⁹ and *IP*¹⁰ that contain more useful information.
- Επίσης, δείτε το *TCP/IP Εγχειρίδιο Οδηγιών και Τεχνική Επισκόπηση*¹¹ IBM Redbook.
- Μια άλλη πηγή είναι το *TCP/IP Network Administration*¹².του O'Reilly.

⁹ <http://manpages.ubuntu.com/manpages/raring/en/man7/tcp.7.html>

¹⁰ <http://manpages.ubuntu.com/manpages/raring/man7/ip.7.html>

¹¹ <http://www.redbooks.ibm.com/abstracts/gg243376.html>

¹² <http://oreilly.com/catalog/9780596002978/>

3. Πρωτόκολλο Δυναμικής Διαμόρφωσης Κεντρικού Υπολογιστή (Dynamic Host Configuration Protocol (DHCP))

Το Πρωτόκολλο Δυναμικής Διαμόρφωσης Κεντρικού Υπολογιστή είναι μια υπηρεσία δικτύου που επιτρέπει στους κεντρικούς υπολογιστές να τους εκχωρηθούν ρυθμίσεις από έναν διακομιστή αυτόματα σε αντίθεση με τη χειροκίνητη διαμόρφωση κάθε κεντρικού υπολογιστή δικτύου. Οι υπολογιστές οι οποίοι διαμορφώνονται ώστε να είναι πελάτες DHCP δεν έχουν κανένα έλεγχο πάνω στις ρυθμίσεις τις οποίες λαμβάνουν από το διακομιστή DHCP, και η διαμόρφωση είναι διαφανής στο χρήστη του υπολογιστή.

Οι πιο κοινές ρυθμίσεις που παρέχονται από το διακομιστή DHCP στους πελάτες DHCP περιλαμβάνουν:

- IP address and netmask
- IP address of the default-gateway to use
- IP addresses of the DNS servers to use

Όμως, ένας διακομιστής DHCP μπορεί να παρέχει ιδιότητες διαμόρφωσης όπως:

- Όνομα Κεντρικού Υπολογιστή
- Όνομα Τομέα
- Διακομιστής Χρόνου
- Διακομιστής Εκτύπωσης

Το πλεονέκτημα της χρήσης DHCP είναι ότι οι αλλαγές στο δίκτυο, για παράδειγμα μια αλλαγή στη διεύθυνση του διακομιστή DNS, πρέπει να αλλαχτεί μόνο στο διακομιστή DHCP, και όλοι οι κεντρικοί υπολογιστές δικτύου θα επαναδιαμορφωθούν την επόμενη φορά που οι πελάτες DHCP θα καταγράψουν τον διακομιστή DHCP. Σαν επιπλέον πλεονέκτημα, είναι επίσης εύκολο να ενσωματώσετε καινούργιους υπολογιστές στο δίκτυο, καθώς δεν υπάρχει ανάγκη να ελέγξετε την διαθεσιμότητα μιας διεύθυνσης IP. Οι συγκρούσεις στην κατανομή διευθύνσεων IP μειώνονται επίσης.

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

3.1. Εγκατάσταση

Σε ένα τερματικό εντολών, πληκτρολογήστε την ακόλουθη εντολή για να εγκαταστήσετε το `dhcpcd`:

```
sudo apt-get 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 `dhcpcd` should listen to.

ΣΗΜΕΙΩΣΗ: τα μηνύματα του `dhcpcd` αποστέλλονται στο `syslog`. Κοιτάξτε εκεί για διαγνωστικά μηνύματα.

3.2. Ρυθμίσεις

Το μήνυμα σφάλματος με το οποίο τελειώνει η εγκατάσταση μπορεί να σας μπερδεύει λίγο, αλλά τα ακόλουθα βήματα θα σας βοηθήσουν να διαμορφώσετε την υπηρεσία:

Κοινώς, αυτό που θέλετε να κάνετε είναι να ορίσετε τυχαία μια διεύθυνση IP. Αυτό μπορεί να γίνει με ρυθμίσεις ως εξής:

```
# 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 service isc-dhcp-server restart
```

3.3. Αναφορές

- 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/raring/en/man5/dhcpd.conf.5.html>

¹⁵ <http://www.isc.org/software/dhcp>

4. Συγχρονισμός Ώρας με NTP

Το NTP είναι ένα πρωτόκολλο TCP/IP για να συγχρονίζεται την ώρα σε ένα δίκτυο. Βασικά ο πελάτης κάνει αίτηση για την τρέχοντα ώρα από έναν διακομιστή, και τον χρησιμοποιεί για να ρυθμίσει το δικό του ρολόι.

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 uses ntpdate and ntpd.

4.1. ntpdate

Ubuntu comes with ntpdate as standard, and will run it once at boot time to set up your time according to Ubuntu's NTP server.

```
ntpdate -s ntp.ubuntu.com
```

4.2. 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.

4.3. Εγκατάσταση

To install ntpd, from a terminal prompt enter:

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

4.4. Ρυθμίσεις

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 service ntp reload

4.5. View status

Use ntpq to see 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
```

4.6. Αναφορές

- See the *Ubuntu Time*¹⁶ wiki page for more information.
- *ntp.org, home of the Network Time Protocol project*¹⁷

¹⁶ <https://help.ubuntu.com/community/UbuntuTime>

¹⁷ <http://www.ntp.org/>

Κεφάλαιο 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* [56] for a complete listing

Πίνακας 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_callout** attribute without interrupting service.

1.2. Επισκόπηση

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.

Πίνακας 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 <code>/etc/rc.sysinit</code> , it can also be started up by a udev program whenever a block device is added or it can be run by the <code>initramfs</code> 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 <code>/etc/multipath.conf</code> 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

Component	Description
	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:

```
# service multipath-tools stop
# 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:

```
# service multipath-tools start
```

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

```
# service multipath-tools stop
# 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:

```
# service multipath-tools start
```

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 **multipath** 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:

```
# service multipath-tools restart
```

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
```

¹ <http://wiki.debian.org/DebianInstaller/MultipathSupport>

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

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="" hwhandler="0" wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
   |- 0:0:0:0 sda 8:0 [-----
```

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

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

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

```
create: 3600a0b80001327510000009b4362163e undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
   |- 2:0:0:3 sdd 8:64 undef ready running
   `-- 3:0:0:3 sdg 8:128 undef ready running
```

2. 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.

```
# service multipath-tools reload
```

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

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

```
create: 3600a0b80001327510000009b4362163e undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
```

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

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 [75]*.

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 [66]*
- *Configuration File Blacklist [67]*
- *Configuration File Defaults [69]*
- *Configuration File Multipath Attributes [74]*
- *Configuration File Devices [75]*

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 [67]*
 - By device name, as described in *Blacklisting By Device Name [67]*
 - By device type, as described in *Blacklisting By Device Type [68]*

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 [67]*

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* [68]

```
blacklist {
    devnode "^(ram|raw|loop|fd|md|dm-[sr]sdc|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 [70]* 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.

Πίνακας 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 <code>/dev</code> .
multipath_dir	The directory where the dynamic shared objects are stored. The default value is system dependent, commonly <code>/lib/multipath</code> .
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • failover = 1 path per priority group • multibus = all valid paths in 1 priority group

Attribute	Description
	<ul style="list-style-type: none"> • 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. <p>The default value is failover.</p>
getuid_callout	<p>Specifies the default program and arguments to call out to obtain a unique path identifier. An absolute path is required.</p> <p>The default value is /lib/udev/scsi_id --whitelisted --device=/dev/%n.</p>
prio	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>The default value is const.</p>
prio_args	<p>The arguments string passed to the prio function. Most prio functions do not need arguments. The datacore prioritizer needs one. Example, "timeout=1000 preferredsds=foo". The default value is (null) "".</p>
features	<p>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, <i>"Issues with queue_if_no_path feature"</i>.</p>

Attribute	Description
path_checker	<p>Specifies the default method used to determine the state of the paths. Possible values include:</p> <ul style="list-style-type: none"> • 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 stat for LSI/Engenio RDAC storage controller. • directio: Read the first sector with direct I/O. <p>The default value is directio.</p>
failback	<p>Manages path group failback.</p> <ul style="list-style-type: none"> • A value of immediate specifies immediate failback to the highest priority path group that contains active paths. • 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. <p>The default value is manual.</p>
rr_min_io	<p>Specifies the number of I/O requests to route to a path before switching to the next path in the current path group.</p> <p>The default value is 1000.</p>
rr_weight	<p>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.</p> <p>The default value is uniform.</p>
no_path_retry	<p>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</p>

Attribute	Description
	<p>immediate failure, without queueing. A value of queue indicates that queueing should not stop until the path is fixed.</p> <p>The default value is 0.</p>
user_friendly_names	<p>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.</p> <p>The default value is no.</p>
queue_without_daemon	<p>If set to no, the multipathd daemon will disable queueing for all devices when it is shut down.</p> <p>The default value is yes.</p>
flush_on_last_del	<p>If set to yes, then multipath will disable queueing when the last path to a device has been deleted.</p> <p>The default value is no.</p>
max_fds	<p>Sets the maximum number of open file descriptors that can be opened by multipath and the multipathd daemon. This is equivalent to the 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.</p>
checker_timer	<p>The timeout to use for path checkers that issue SCSI commands with an explicit timeout, in seconds.</p> <p>The default value is taken from /sys/block/sdx/device/timeout, which is 30 seconds as of 12.04 LTS</p>
fast_io_fail_tmo	<p>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.</p>

Attribute	Description
	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 [74]* 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.

Πίνακας 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 <code>multipath.conf</code> 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 <code>mpathn</code> ; 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 is 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 [76]* 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* [74].

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.

Πίνακας 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: <ul style="list-style-type: none">• 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

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

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

- 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* [82] describes some options of the **multipath** command that you might find useful.

Πίνακας 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>

Κεφάλαιο 6. Απομακρυσμένη Διαχείριση

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

1. OpenSSH Server

1.1. Εισαγωγή

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.

Το συστατικό του διακομιστή OpenSSH, sshd, ακούει συνεχώς για συνδέσεις πελάτη από κάθε ένα από τα εργαλεία πελάτη. Όταν προκύπτει ένα αίτημα σύνδεσης, το sshd στήνει τη σωστή σύνδεση βασισμένη στον τύπο του εργαλείου πελάτη που συνδέεται. Για παράδειγμα, αν ο απομακρυσμένος υπολογιστής συνδέεται με εφαρμογή πελάτη ssh, ο διακομιστής OpenSSH στήνει μια συνεδρία απομακρυσμένου ελέγχου μετά την πιστοποίηση. Εάν ένας απομακρυσμένος χρήστης συνδεθεί σε ένα διακομιστή OpenSSH με scp, ο δαίμονας διακομιστή OpenSSH ξεκινάει μια ασφαλή αντιγραφή αρχείων ανάμεσα στον διακομιστή και τον πελάτη μετά την πιστοποίηση. Το OpenSSH μπορεί να χρησιμοποιήσει πολλές μεθόδους πιστοποίησης, περιλαμβάνοντας απλό κωδικό, δημόσιο κλειδί, και εισιτήρια Kerberos.

1.2. Εγκατάσταση

Η εγκατάσταση των εφαρμογών πελάτη και διακομιστή OpenSSH είναι απλή. Για να εγκαταστήσετε τις εφαρμογές πελάτη OpenSSH στο σύστημα Ubuntu σας, χρησιμοποιείτε αυτή την εντολή από ένα τερματικό εντολών:

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

Για να εγκαταστήσετε την εφαρμογή διακομιστή OpenSSH, και τα σχετικά αρχεία υποστήριξης, χρησιμοποιείτε αυτή την εντολή από ένα τερματικό εντολών:

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

Το πακέτο openssh-server μπορεί επίσης να επιλεγθεί να εγκατασταθεί κατά τη διαδικασία εγκατάστασης της Έκδοσης Διακομιστή.

1.3. Ρυθμίσεις

Μπορείτε να διαμορφώσετε την προεπιλεγμένη συμπεριφορά της εφαρμογής διακομιστή OpenSSH, `sshd`, κάνοντας επεξεργασία στο αρχείο `/etc/ssh/sshd_config`. Για περισσότερες πληροφορίες για τη διαμόρφωση κωδικών παραπομπής που χρησιμοποιούνται σε αυτό το αρχείο, μπορείτε να δείτε την κατάλληλη σελίδα εγχειριδίου με την ακόλουθη εντολή σε ένα τερματικό εντολών:

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.



Πριν επεξεργαστείτε το αρχείο διαμόρφωσης, θα πρέπει να δημιουργήσετε ένα αντίγραφο του αυθεντικού αρχείου και να το προστατέψετε από επεξεργασία ώστε να έχετε τις αρχικές ρυθμίσεις σας αναφορά και να τις επαναχρησιμοποιήσετε όπου χρειάζεται.

Αντιγράψτε το αρχείο `/etc/ssh/sshd_config` και προστατέψτε το από επεξεργασία με τις ακόλουθες εντολές, σε ένα τερματικό εντολών:

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

Τα ακόλουθα είναι παραδείγματα κωδικών παραπομπής που μπορείτε να αλλάξετε:

- Για να θέσετε το OpenSSH σας να ακούει την TCP θύρα 2222 αντί την προεπιλεγμένη TCP θύρα 22, αλλάξτε τον κώδικα παραπομπής Port ως εκ τούτου:

Port 2222

- Για να επιτρέπει το `sshd` διαπιστευτήρια σύνδεσης βασισμένα σε δημόσιο κλειδί, απλώς προσθέστε ή τροποποιήστε τη γραμμή:

PubkeyAuthentication yes

If the line is already present, then ensure it is not commented out.

- Για να κάνετε το διακομιστή OpenSSH να προβάλει περιεχόμενα του αρχείου `/etc/issue.net` σαν ένα λάβαρο πριν τη σύνδεση, απλώς προσθέστε ή τροποποιήστε τη γραμμή:

Banner /etc/issue.net

Στο αρχείο `/etc/ssh/sshd_config`.

Αφού κάνετε αλλαγές στο αρχείο `/etc/ssh/sshd_config`, αποθηκεύστε το αρχείο, και επανεκκινήστε την εφαρμογή διακομιστή `sshd` ώστε να ενεργοποιηθούν οι αλλαγές χρησιμοποιώντας την ακόλουθη εντολή σε ένα τερματικό εντολών:

sudo service ssh restart



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. Κλειδιά SSH

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.

Για να παράγετε κλειδιά, από ένα τερματικό εντολών πληκτρολογείτε:

ssh-keygen -t dsa

This will generate the keys using the *Digital Signature Algorithm (DSA)* method. During the process you will be prompted for a password. Simply hit *Enter* when prompted to create the key.

Εξορισμού το *δημόσιο* κλειδί αποθηκεύεται στο αρχείο `~/.ssh/id_dsa.pub`, ενώ το `~/.ssh/id_dsa` είναι το *ιδιωτικό* κλειδί. Τώρα αντιγράψτε το αρχείο `id_dsa.pub` στον απομακρυσμένο κεντρικό υπολογιστή και επισυνάψτε το στο `~/.ssh/authorized_keys` πληκτρολογώντας:

ssh-copy-id username@remotehost

Τέλος, επανελέγξτε τα δικαιώματα στο αρχείο `authorized_keys`, μόνο ο πιστοποιημένος χρήστης θα πρέπει να έχει διακαιώματα ανάγνωσης και επεξεργασίας. Εάν τα δικαιώματα δεν είναι σωστά αλλάξτε τα:

chmod 600 ~/.ssh/authorized_keys

Τώρα θα πρέπει να μπορείτε να συνδέεστε με SSH στον κεντρικό υπολογιστή χωρίς να σας ζητηθεί κωδικός.

1.5. Αναφορές

- *Ubuntu Wiki SSH*¹ page.

¹ <https://help.ubuntu.com/community/SSH>

- *Ιστοσελίδα OpenSSH*²
- *Προηγμένη Σελίδα Wiki OpenSSH*³

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 *Κεφάλαιο 8, Υπηρεσία ονομάτων τομέα (DNS) [145]* 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. Εγκατάσταση

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

```
sudo apt-get install puppetmaster
```

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

```
sudo apt-get install puppet
```

2.3. Ρυθμίσεις

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 service puppetmaster restart
```

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

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

```
START=yes
```

Then start the service:

```
sudo service puppet start
```

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 its 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 *Τμήμα 2.4, Πόροι*; [91].

2.4. Πόροι

- See the *Official Puppet Documentation*⁴ web site.
- See the *Puppet forge*⁵, online repository of puppet modules.
- Also see *Pro Puppet*⁶.
- Another source of additional information is the *Ubuntu Wiki Puppet Page*⁷.

⁴ <http://docs.puppetlabs.com/>

⁵ <http://forge.puppetlabs.com/>

⁶ <http://www.apress.com/9781430230571>

⁷ <https://help.ubuntu.com/community/Puppet>

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 helps to avoid errors in the network configuration and administration and allows to save time. Zentyal is open source, released under the GNU General Public License (GPL) and runs on top of Ubuntu GNU/Linux.

Zentyal consists of a serie 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 advantages of using Zentyal are: unified, graphical user interface to configure all network services and high, out-of-the-box integration between them.

3.1. Εγκατάσταση

Zentyal 2.3 is available on Ubuntu 12.04 Universe repository. The modules available are:

- zentyal-core & zentyal-common: the core of the Zentyal interface and the common libraries of the framework. Also include 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 forbidden 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.
- **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.

To install Zentyal, in a terminal on the *server* enter (where `<zentyal-module>` is any of the modules from the previous list):

sudo apt-get install <zentyal-module>



Zentyal publishes one major stable release once a year (in September) based on latest Ubuntu LTS release. Stable releases always have even minor numbers (e.g. 2.2, 3.0) and beta releases have odd minor numbers (e.g. 2.1, 2.3). Ubuntu 12.04 comes with Zentyal 2.3 packages. If you want to upgrade to a new stable release published after the release of Ubuntu 12.04 you can use *Zentyal Team PPA*⁸. Upgrading to newer stable releases can provide you minor bugfixes not backported to 2.3 in Precise and newer features.



If you need more information on how to add packages from a PPA see *Add a Personal Package Archive (PPA)*⁹.



Not present on Ubuntu Universe repositories, but on *Zentyal Team PPA*¹⁰ 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 bandwidth usage of your LAN clients.

⁸ <https://launchpad.net/~zentyal/>

⁹ <https://help.ubuntu.com/13.04/ubuntu-help/addremove-ppa.html>

¹⁰ <https://launchpad.net/~zentyal/>

- 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.

3.2. First steps

Any system account belonging to the sudo group is allowed to log into Zentyal web interface. If you are using the user created during the installation, this should be in the sudo group by default.



If you need to add another user to the sudo group, just execute:

sudo adduser username sudo

To access Zentyal web interface, browse into <https://localhost/> (or the IP of your remote server). As Zentyal creates its own self-signed SSL certificate, you will have to accept a security exception on your browser.

Once logged in you will see the dashboard with an overview of your server. To configure any of the features of your installed modules, go to the different sections on the left menu. When you make any changes, on the upper right corner appears a red *Save changes* button that you must click to save all configuration changes. To apply these configuration changes in your server, the module needs to be enabled first, you can do so from the *Module Status* entry on the left menu. Every time you enable a module, a pop-up will appear asking for a confirmation to perform the necessary actions and changes on your server and configuration files.



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>.`

3.3. Αναφορές

*Zentyal Official Documentation*¹¹ page.

See also *Zentyal Community Documentation*¹² page.

And don't forget to visit the *forum*¹³ for community support, feedback, feature requests, etc.

¹¹ <http://doc.zentyal.org/>

¹² <http://trac.zentyal.org/wiki/Documentation>

¹³ <http://forum.zentyal.org/>

Κεφάλαιο 7. Πιστοποίηση δικτύου

This section applies LDAP to network authentication and authorization.

1. Εξυηρητητής OpenLDAP

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 LDAP implementation used in Ubuntu is OpenLDAP, currently at version 2.4.25 (Oneiric).

So this 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: it's *Distinguished Name* (DN or dn). This consists of it's *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. It's DN is "cn=John Doe,dc=example,dc=com"; it's RDN is "cn=John Doe"; and it's 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. Εγκατάσταση

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 localhost. If you want something different, edit `/etc/hosts` and replace the domain name with one that will give you the suffix you desire. For instance, if you want a suffix of `dc=example,dc=com` then your file would have a line similar to this:

```
127.0.1.1    hostname.example.com hostname
```

You can revert the change after package installation.



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

Proceed with the install:

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

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/
```

```
### cn=config
# ### cn=module{0}.ldif
# ### cn=schema
# # ### cn={0}core.ldif
# # ### cn={1}cosine.ldif
# # ### cn={2}nis.ldif
# # ### cn={3}inetorgperson.ldif
# ### cn=schema.ldif
# ### olcBackend={0}hdb.ldif
# ### olcDatabase={0}config.ldif
# ### olcDatabase={-1}frontend.ldif
# ### olcDatabase={1}hdb.ldif
### cn=config.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}hdb,cn=config
```

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

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

dn: olcDatabase={1}hdb,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}hdb,cn=config*: the 'hdb' 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}hdb,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}hdb,cn=config database (dc=example,dc=com). Create a file, call it uid_index.ldif, with the following contents:

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

Then issue the command:

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

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

You can confirm the change in this way:

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

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

- 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={1}corba,cn=schema,cn=config
```



When slapd injects 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={1}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. Καταγραφή

Activity logging for slapd is indispensable 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
add: 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 service rsyslog restart
```

³ <http://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html>

1.6. Αναπαραγωγή

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 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}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq

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

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

# Accesslog db syncprov.
```



```
dn: olcOverlay=syncprov,olcDatabase={2}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE
```

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

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

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

2. The apparmor profile for slapd will need to be adjusted for the accesslog database location. Edit `/etc/apparmor.d/local/usr.sbin.slapd` by adding the following:

```
/var/lib/ldap/accesslog/ r,
/var/lib/ldap/accesslog/** rwk,
```

Create a directory, set up a database config file, and reload the apparmor profile:

```
sudo -u openldap mkdir /var/lib/ldap/accesslog
sudo -u openldap cp /var/lib/ldap/DB_CONFIG /var/lib/ldap/accesslog
sudo service apparmor reload
```

3. Add the new content and, due to the apparmor change, restart the daemon:

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

The Provider is now configured.

1.6.2. Consumer Configuration

And now configure the *Consumer*.

1. Install the software by going through *Τμήμα 1.1, “Εγκατάσταση” [98]*. Make sure the slapd-config database is identical to the Provider's. In particular, make sure schemas and the database 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}hdb,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. Δοκιμή

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 steadily 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 DN's 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 hdb database ("dc=example,dc=com") and those of the frontend database:

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

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



The rootDN always has full rights to it's database. Including it in an ACL does provide an explicit configuration but it also causes slapd to incur a performance penalty.

```
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 ACL is crucial:

```
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymous
auth by dn="cn=admin,dc=example,dc=com" write by * none
```

This can be represented differently for easier digestion:

```
to attrs=userPassword
by self write
by anonymous auth
by dn="cn=admin,dc=example,dc=com" write
by * none
```

```
to attrs=shadowLastChange
by self write
by anonymous auth
by dn="cn=admin,dc=example,dc=com" write
by * none
```

This compound ACL (there are 2) enforces the following:

- Anonymous 'auth' access is provided to the *userPassword* attribute for the initial connection to occur. Perhaps counter-intuitively, 'by anonymous auth' is needed even when anonymous access to the DIT is unwanted. Once the remote end is connected, however, authentication can occur (see next point).

- Authentication can happen because all users have 'read' (due to 'by self write') access to the *userPassword* attribute.
- The *userPassword* attribute is otherwise inaccessible by all other users, with the exception of the rootDN, who has complete access to it.
- In order for users to change their own password, using **passwd** or other utilities, the *shadowLastChange* attribute needs to be accessible once a user has authenticated.

This DIT can be searched anonymously because of 'by * read' in this ACL:

```
to *  
by self write  
by dn="cn=admin,dc=example,dc=com" write  
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 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-get 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/ca-cert.pem
```

5. Make a private key for the server:

```
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
```

⁴ <http://manpages.ubuntu.com/manpages/en/man5/slapd.access.5.html>

```
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
```

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 /etc/ssl/certinfo.ldif
```

Contrary 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.

Tighten up ownership and permissions:

```
sudo adduser openldap ssl-cert
sudo chgrp ssl-cert /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap01_slapd_key.pem
```

Restart OpenLDAP:

```
sudo service slapd restart
```

Check your host's logs (/var/log/syslog) to see if the server has started properly.

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 eavesdropping. 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 *Τμήμα 1.6, “Αναπαραγωγή” [106]* and have configured TLS for authentication on the Provider by following *Τμήμα 1.8, “TLS” [112]*.

As previously stated, the objective (for us) with replication is high availability 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 it's 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.p
```

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-get install ssl-cert
sudo adduser 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 ssl-cert /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap02_slapd_key.pem
```

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}hdb,cn=config
replace: olcSyncrepl
olcSyncrepl: rid=0 provider=ldap://ldap01.example.com bindmethod=simple
binddn="cn=admin,dc=example,dc=com" credentials=secret searchbase="dc=example,dc=com"
```

```
logbase="cn=accesslog" logfilter="(&(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 service slapd restart
```

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. Πιστοποίηση LDAP

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-get 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
```

Τα αποτελέσματα των επιλογών σας στο διάλογο φαίνονται στο αρχείο `/etc/ldap.conf`. Αν ο εξυπηρετητής σας απαιτεί επιλογές που δεν περιλαμβάνονται στο μενού, θα χρειαστεί να επεξεργαστείτε αυτό το αρχείο.

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 *Τμήμα 2, “Samba και LDAP” [123]* for details.



An alternative to the `libnss-ldap` package is the `libnss-ldapd` package. This, however, will bring in the `nscd` package which is probably not wanted. Simply remove it afterwards.

1.11. Διαχείριση χρηστών και ομάδων

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-get 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:

- Δημιουργία νέου χρήστη:

```
sudo ldapadduser george example
```

Δημιουργεί χρήστη με uid *george* και ορίζει την *example* ως πρωτεύουσα ομάδα του χρήστη (gid).

- Αλλαγή κωδικού χρήστη:

```
sudo ldapsetpasswd george
```

Changing password for user uid=george,ou=People,dc=example,dc=com

New Password:

New Password (verify):

- Διαγραφή χρήστη:

```
sudo ldapdeleteuser george
```

- Προσθήκη ομάδας:

```
sudo ldapaddgroup qa
```

- Διαγραφή ομάδας:

```
sudo ldapdeletgroup qa
```

- Προσθήκη χρήστη σε ομάδα:

```
sudo ldapaddusertogroup george qa
```

Θα πρέπει να έχει εμφανιστεί ένα γνώρισμα *memberUid* για την ομάδα *qa*, με τιμή *george*.

- Αφαίρεση χρήστη από ομάδα:

```
sudo ldapdeleteuserfromgroup george qa
```

Το γνώρισμα *memberUid* θα πρέπει να έχει αφαιρεθεί από την ομάδα *qa*.

- Το σενάριο *ldapmodifyuser* σας επιτρέπει να προσθέτετε, να αφαιρείτε και να αντικαθιστάτε τα γνώρισμα ενός χρήστη. Το σενάριο αυτό χρησιμοποιεί την ίδια σύνταξη με το *ldapmodify*. Π.χ.:

```
sudo ldapmodifyuser george
```

```
# Θα τροποποιηθεί η ακόλουθη εγγραφή :
```

```
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:: e1NTSEF9eXFcTFcyWlhWkF1eGUybVdFWHZKRzJVMjFTSG9vcHk=
```

```
# Εισάγετε τις αλλαγές σας εδώ και τελειώστε με CTRL-D.
```

```
dn: uid=george,ou=People,dc=example,dc=com
```

```
replace: gecos
```

```
gecos: George Carlin
```

Το *gecos* θα πρέπει να έχει γίνει `“George Carlin”`.

- A nice feature of *ldapscrip*ts 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/ldapscrip`ts/`ldapscrip`ts.conf changing:

```
UTEMPLATE="/etc/ldapscrip
```

ts/ldapadduser.template"

Στον κατάλογο `/etc/ldapscrip`ts υπάρχουν *δείγματα* προτύπων. Αντιγράψτε ή μετονομάστε το αρχείο `ldapadduser.template.sample` σε `/etc/ldapscrip`ts/`ldapadduser.template`:

```
sudo cp /usr/share/doc/ldapscrip
```

ts/examples/`ldapadduser.template.sample` \
`/etc/ldapscrip`ts/`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 it's value.

There are utilities in the package that were not covered here. Here is a complete list:

```
ldaprenamemachine5
ldapadduser6
ldapdeleteuserfromgroup7
ldpfinger8
ldapid9
ldapgid10
ldapmodifyuser11
ldaprenameuser12
lsldap13
ldapaddusertogroup14
ldapsetpasswd15
ldapinit16
ldapaddgroup17
ldapdeletgroup18
ldapmodifygroup19
ldapdeletemachine20
ldaprenamegroup21
ldapaddmachine22
ldapmodifymachine23
```

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/ldpfinger.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/ldapdeletgroup.1.html>

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>

*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:

```
sudo service slapd stop
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
```

²⁴ <http://manpages.ubuntu.com/manpages/en/man1/ldapsetprimarygroup.1.html>

²⁵ <http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuser.1.html>

```
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 service slapd start
```

1.13. Πόροι

- The primary resource is the upstream documentation: www.openldap.org²⁶
- 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 και 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 *Τμήμα 1, Εξυπηρετητής OpenLDAP*; [97] 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.

2.1. Software Installation

There are three packages needed when integrating Samba with LDAP: samba, samba-doc, and smbldap-tools packages.

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

2.2. LDAP Configuration

We will now configure the LDAP server so that it can accommodate 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 *Τμήμα 1.4, Εξυπηρετητής OpenLDAP*; [102].

1. The schema is found in the now-installed samba-doc package. It needs to be unzipped and copied to the `/etc/ldap/schema` directory:

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

2. Have the configuration file `schema_convert.conf` that contains 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
include /etc/ldap/schema/samba.schema
```

3. Have the directory `ldif_output` hold output.
4. Determine the index of the schema:

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

```
dn: cn={14}samba,cn=schema,cn=config
```

5. Convert the schema to LDIF format:

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H \
ldap:///cn={14}samba,cn=schema,cn=config -l cn=samba.ldif
```

6. Edit the generated `cn=samba.ldif` file by removing index information to arrive at:

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

Remove the bottom lines:

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

Your attribute values will vary.

7. Add the new schema:

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

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}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

Using the `ldapmodify` utility load the new 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}hdb olcDbIndex
```

2.2.3. Adding Samba LDAP objects

Next, configure the `smbldap-tools` package to match your environment. The package is supposed to come with a configuration helper script (`smbldap-config.pl`, formerly

configure.pl) that will ask questions about the needed options but there is a *bug*³⁷ whereby it is not installed (but found in the source code; 'apt-get source smbldap-tools').

To manually configure the package you need to create and edit the files /etc/smbldap-tools/smbldap.conf and /etc/smbldap-tools/smbldap_bind.conf.

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:

```
sudo smbldap-populate
```

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 it's data per usual.

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

2.3. Ρύθμιση Samba

There are multiple ways to configure Samba. For details on some common configurations see *Κεφάλαιο 18, Samba [301]*. To configure Samba to use LDAP, edit it's configuration file /etc/samba/smb.conf commenting out the default *passdb backend* parameter and adding some ldap-related ones:

```
# passdb backend = tdbsam

# Ρυθμίσεις LDAP
passdb backend = ldapsam:ldap://hostname
ldap suffix = dc=example,dc=com
ldap user suffix = ou=People
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers
ldap idmap suffix = ou=Idmap
ldap admin dn = cn=admin,dc=example,dc=com
ldap ssl = start tls
ldap passwd sync = yes
...
add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w "%u"
```

Change the values to match your environment.

Επανεκκινήστε το samba για να ενεργοποιήσετε τις νέες ρυθμίσεις:

³⁷ <https://bugs.launchpad.net/serverguide/+bug/997172>

```
sudo restart smbd  
sudo restart nmbd
```

Now inform Samba about the rootDN user's password (the one set during the installation of the slapd package):

```
sudo smbpasswd -w password
```

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 attributes. The smbpasswd utility can do this as well (your host will need to be able to see (enumerate) those users via NSS; install and configure either libnss-ldapd or libnss-ldap):

```
sudo smbpasswd -a username
```

You will be prompted to enter a password. It will be considered as the new password for that user. Making it the same as before is reasonable.

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:

```
sudo smbldap-useradd -a -P 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.

- 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*³⁸
*smbldap-groupdel*³⁹
*smbldap-groupmod*⁴⁰
*smbldap-groupshow*⁴¹
*smbldap-passwd*⁴²
*smbldap-populate*⁴³
*smbldap-useradd*⁴⁴
*smbldap-userdel*⁴⁵
*smbldap-userinfo*⁴⁶
*smbldap-userlist*⁴⁷
*smbldap-usermod*⁴⁸
*smbldap-usershow*⁴⁹

2.4. Πόροι

- For more information on installing and configuring Samba see *Κεφάλαιο 18, Samba [301]* of this Ubuntu Server Guide.
- There are multiple places where LDAP and Samba is documented in the upstream *Samba HOWTO Collection*⁵⁰.
- Regarding the above, see specifically the *passdb section*⁵¹.

³⁸ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupadd.8.html>

³⁹ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupdel.8.html>

⁴⁰ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupmod.8.html>

⁴¹ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupshow.8.html>

⁴² <http://manpages.ubuntu.com/manpages/en/man8/smbldap-passwd.8.html>

⁴³ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-populate.8.html>

⁴⁴ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-useradd.8.html>

⁴⁵ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-userdel.8.html>

⁴⁶ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-userinfo.8.html>

⁴⁷ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-userlist.8.html>

⁴⁸ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-usermod.8.html>

⁴⁹ <http://manpages.ubuntu.com/manpages/en/man8/smbldap-usershow.8.html>

⁵⁰ <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/>

⁵¹ <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/passdb.html>

- Although dated (2007), the *Linux Samba-OpenLDAP HOWTO*⁵² contains valuable notes.
- The main page of the *Samba Ubuntu community documentation*⁵³ has a plethora of links to articles that may prove useful.

⁵² <http://download.gna.org/smbldap-tools/docs/samba-ldap-howto/>

⁵³ <https://help.ubuntu.com/community/Samba#samba-ldap>

3. Kerberos

Το Kerberos είναι ένα σύστημα πιστοποίησης δικτύου που βασίζεται στην αρχή του έμπιστου τρίτου μέρους. Όπου τα άλλα δύο μέρη είναι ο χρήστης και η υπηρεσία στην οποία θέλει να πιστοποιηθεί ο χρήστης. Δεν μπορούν όλες οι υπηρεσίες και εφαρμογές να χρησιμοποιούν το Kerberos, αλλά για αυτές που μπορούν, το περιβάλλον δικτύου προσεγγίζει κατά ένα ακόμη βήμα το ιδανικό της μοναδικής εισόδου (Single Sign On - SSO).

Αυτή η ενότητα καλύπτει την εγκατάσταση και ρύθμιση ενός εξυπηρετητή Kerberos, καθώς και ορισμένα παραδείγματα ρυθμίσεων πελάτη.

3.1. Επισκόπηση

Αν είστε καινούριο στο Kerberos, υπάρχουν ορισμένοι όροι που είναι καλό να γνωρίζετε πριν στήσετε έναν εξυπηρετητή Kerberos. Οι περισσότεροι από αυτούς τους όρους μπορεί να σας θυμίζουν άλλα περιβάλλοντα:

- *Principal (Διευθυντής)*: όλοι οι χρήστες, υπολογιστές και υπηρεσίες που παρέχονται από εξυπηρετητές πρέπει να έχουν οριστεί ως Kerberos Principals.
- *Instances*: χρησιμοποιούνται για τους διευθυντές υπηρεσιών και τους ειδικούς διαχειριστικούς διευθυντές.
- *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 - Βασικό Κέντρο Διανομής)*: αποτελείται από τρία τμήματα, μια βάση δεδομένων με όλους τους διευθυντές, τον εξυπηρετητή πιστοποίησης και τον εξυπηρετητή εκχώρησης ticket. Κάθε realm πρέπει να διαθέτει τουλάχιστον ένα KDC.
- *Ticket Granting Ticket (Δελτίο Εκχώρησης Δελτίου)*: εκδίδεται από τον εξυπηρετητή πιστοποίησης (AS). Το Δελτίο Εκχώρησης Δελτίου (TGT) κρυπτογραφείται με τον κωδικό του χρήστη, που είναι γνωστός μόνο στον χρήστη και το KDC.
- *Ticket Granting Server (Εξυπηρετητής Εκχώρησης Δελτίων - TGS)*: Εκχωρεί δελτία υπηρεσιών στους πελάτες μετά από αίτημά τους.
- *Tickets (Δελτία)*: επιβεβαιώνουν την ταυτότητα των δύο διευθυντών. Όπου ο ένας διευθυντής είναι χρήστης και ο άλλος μία υπηρεσία που έχει ζητήσει ο χρήστης. Τα δελτία χρησιμοποιούν ένα κλειδί κρυπτογράφησης που διασφαλίζει την επικοινωνία κατά τη διάρκεια της πιστοποιημένης συνεδρίας.
- *Αρχεία Keytab*: είναι αρχεία που εξάγονται από τη βάση δεδομένων διευθυντών του KDC και περιέχουν το κλειδί κρυπτογράφησης μιας υπηρεσίας ή ενός μηχανήματος.

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. Εξυπηρετητής Kerberos

3.2.1. Εγκατάσταση

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 *Τμήμα 2.3, “Κύριος Master” [148]* 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 *Τμήμα 4, “Συγχρονισμός Ώρας με NTP” [53]*.

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-get 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.

Στη συνέχεια, δημιουργήστε το νέο realm χρησιμοποιώντας το `kdb5_newrealm`:

```
sudo krb5_newrealm
```

3.2.2. Ρυθμίσεις

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.



Αντικαταστήστε τα *EXAMPLE.COM* και *steve* με το Realm σας και το όνομα χρήστη του διαχειριστή.

2. Στη συνέχεια, ο νέος χρήστης - διαχειριστής πρέπει να αποκτήσει τα κατάλληλα δικαιώματα ACL. Τα δικαιώματα ορίζονται στο αρχείο `/etc/krb5kdc/kadm5.acl`.

```
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. Τώρα, επανεκκινήστε το `krb5-admin-server` για να ενεργοποιήσετε το ACL:

sudo service krb5-admin-server restart

4. Μπορείτε να δοκιμάσετε το νέο principal χρησιμοποιώντας το εργαλείο `kinit`:

kinit steve/admin

steve/admin@EXAMPLE.COM's Password:

Αφού εισάγετε τον κωδικό, χρησιμοποιήστε το `klist` για να δείτε πληροφορίες σχετικά με το 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.
```



Αντικαταστήστε τα *EXAMPLE.COM*, *kdc01*, και *kdc02* με το όνομα του domain, το πρωτεύον KDC και το δευτερεύον KDC.

Δείτε το *Κεφάλαιο 8, Υπηρεσία ονομάτων τομέα (DNS) [145]* για λεπτομερείς οδηγίες ρυθμίσεις του DNS.

Το νέο Kerberos Realm είναι πλέον σε θέση να πιστοποιεί πελάτες.

3.3. Δευτερεύον 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. Καταρχάς, εγκαταστήστε τα πακέτα και, όταν σας ζητηθούν τα ονόματα των εξυπηρετητών Kerberos και διαχειριστή, εισάγετε το όνομα του πρωτεύοντος KDC:

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

2. Αφού εγκατασταθούν τα πακέτα, δημιουργήστε τον `principal` του δευτερεύοντος KDC. Από το τερματικό, δίνετε:

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



Στη συνέχεια, κάθε φορά που θα εκτελείτε εντολές `kadmin`, θα ερωτάστε για τον κωδικό του `principal` `username/admin@EXAMPLE.COM`.

3. Εξάγετε το αρχείο `keytab`:

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

4. Θα πρέπει πλέον να διαθέτετε ένα αρχείο `keytab.kdc02` στον τρέχοντα κατάλογο, το οποίο θα πρέπει να μετακινήσετε στο `/etc/krb5.keytab`:

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



Αν η διαδρομή προς το αρχείο `keytab.kdc02` είναι διαφορετική, τροποποιήστε την κατάλληλα.

Επίσης, μπορείτε να απαριθμήσετε τους `principal` σε ένα αρχείο `Keytab` (χρήσιμο για αποσφαλμάτωση), χρησιμοποιώντας το `klist`:

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

The `-k` option indicates the file is a keytab file.

5. Περαιτέρω, χρειάζεται ένα αρχείο `kpropd.acl` σε κάθε KDC, που να απαριθμεί όλα τα KDC του Realm. Π.χ., τόσο στο πρωτεύον όσο και στο δευτερεύον KDC, δημιουργήστε ένα αρχείο `/etc/krb5kdc/kpropd.acl`:

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

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

6. Δημιουργήστε μια άδεια βάση δεδομένων στο *δευτερεύον KDC*:

```
sudo kdb5_util -s create
```

7. Τώρα, εκκινήστε την υπηρεσία `kpropd`, που αφουγκράζεται για συνδέσεις από την υπηρεσία `kprop`. Το `kprop` χρησιμοποιείται για τη μεταφορά αρχείων `dump`:

```
sudo kpropd -S
```

8. Από το τερματικό στο *πρωτεύον KDC*, δημιουργήστε ένα αρχείο `dump` της βάσης δεδομένων των `principal`:

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

9. Εξάγετε το αρχείο *keytab* του πρωτεύοντος KDC και αντιγράψτε το στο */etc/krb5.keytab*:

```
kadmin -q "ktadd -k keytab.kdc01 host/kdc01.example.com"
sudo mv keytab.kdc01 /etc/krb5.keytab
```



Βεβαιωθείτε ότι υπάρχει *host* για το *kdc01.example.com* πριν εξάγετε το αρχείο *keytab*.

10. Χρησιμοποιώντας το *kprop*, σπρώξτε (push) τη βάση δεδομένων στο δευτερεύον KDC:

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



Αν επιτύχει η διαδικασία, θα πρέπει να εμφανιστεί το μήνυμα *SUCCEEDED*. Αν εμφανιστεί μήνυμα σφάλματος, ελέγξτε το */var/log/syslog* του δευτερεύοντος KDC για περισσότερες πληροφορίες.

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. Επιστρέφοντας στο *δευτερεύον KDC*, δημιουργήστε ένα αρχείο *αποθήκευσης (stash)* για το κύριο (master) κλειδί του Kerberos:

```
sudo kdb5_util stash
```

12. Τέλος, εκκινήστε την υπηρεσία *krb5-kdc* στο δευτερεύον KDC:

```
sudo service krb5-kdc start
```

The *Secondary KDC* should now be able to issue tickets for the Realm. You can test this by stopping the *krb5-kdc* daemon on the Primary KDC, then 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. Πελάτης Kerberos για Linux

Αυτή η ενότητα καλύπτει τη ρύθμιση ενός συστήματος Linux ως πελάτη Kerberos. Αυτό θα σας προσφέρει πρόσβαση σε όλες τις υπηρεσίες Kerberos μετά την επιτυχή είσοδο ενός χρήστη στο σύστημα.

3.4.1. Εγκατάσταση

Για να γίνει η πιστοποίηση σε realm Kerberos, απαιτούνται τα πακέτα krb5-user και libpam-krb5, καθώς και ορισμένα ακόμη, που, αν και δεν είναι απολύτως απαραίτητα, διευκολύνουν σημαντικά το έργο σας. Για να τα εγκαταστήσετε, πληκτρολογείτε στο τερματικό:

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

Το πακέτο auth-client-config σας επιτρέπει να ρυθμίζεται εύκολα το PAM για πιστοποίηση από πολλαπλές πηγές, ενώ το libpam-ccreds αποθηκεύει τα στοιχεία πιστοποίησης, έτσι ώστε να μπορείτε να κάνετε είσοδο σε περίπτωση που το Κέντρο Διανομής Κλειδιών (KDC) δεν είναι διαθέσιμο. Το πακέτο αυτό είναι χρήσιμο και για φορητούς υπολογιστές που κάνουν πιστοποίηση μέσω Kerberos όταν βρίσκονται στο εταιρικό δίκτυο, αλλά που θα πρέπει να μπορούν να χρησιμοποιηθούν και εκτός δικτύου.

3.4.2. Ρυθμίσεις

Για να ρυθμίσετε τον πελάτη, εισαγάγετε τα παρακάτω στο τερματικό:

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

Θα σας ζητηθεί το όνομα του realm του Kerberos. Επίσης, αν το DNS δεν έχει ρυθμιστεί με τις εγγραφές SRV του Kerberos, θα σας ζητηθεί το hostname του KDC και ο εξυπηρετητής διαχείρισης του realm.

Το dpkg-reconfigure προσθέτει εγγραφές στο αρχείο /etc/krb5.conf του realm. Οι εγγραφές σας θα πρέπει να μοιάζουν στις ακόλουθες:

```
[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 *Τμήμα 3.2.1, Εγκατάσταση* [131], 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**.

Μπορείτε να δοκιμάσετε τις ρυθμίσεις ζητώντας ένα δελτίο (ticket) μέσω του kinit. Π.χ.:

```
kinit steve@EXAMPLE.COM
```

Password for steve@EXAMPLE.COM:

Αφού εκχωρηθεί το δελτίο, μπορείτε να δείτε τις σχετικές πληροφορίες μέσω 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

Στη συνέχεια, χρησιμοποιήστε το auth-client-config για να ρυθμίσετε το άρθρωμα libpam-krb5 έτσι ώστε να ζητάει δελτίο κατά την είσοδο:

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

Θα πρέπει πλέον να λαμβάνετε δελτίο μετά από κάθε επιτυχή πιστοποίηση εισόδου.

3.5. Πόροι

- For more information on MIT's version of Kerberos, see the *MIT Kerberos*⁵⁴ site.
- The *Ubuntu Wiki Kerberos*⁵⁵ page has more details.
- Το εγχειρίδιο *Kerberos: The Definitive Guide*⁵⁶ του O'Reilly είναι ένα εξαιρετικό έργο αναφοράς για την εγκατάσταση του Kerberos.
- Also, feel free to stop by the *#ubuntu-server* and *#kerberos* IRC channels on *Freenode*⁵⁷ if you have Kerberos questions.

⁵⁴ <http://web.mit.edu/Kerberos/>

⁵⁵ <https://help.ubuntu.com/community/Kerberos>

⁵⁶ <http://oreilly.com/catalog/9780596004033/>

⁵⁷ <http://freenode.net/>

4. Kerberos και 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.

Η αντιγραφή μιας βάσης δεδομένων principal Kerberos μεταξύ δύο εξυπηρετητών μπορεί να είναι πολύπλοκη διαδικασία, ενώ επίσης προσθέτει μία ακόμη βάση δεδομένων χρήστη στο δίκτυό σας. Ευτυχώς, το Kerberos του MIT μπορεί να ρυθμιστεί έτσι ώστε να χρησιμοποιεί έναν κατάλογο LDAP ως βάση δεδομένων principal. Αυτή η ενότητα καλύπτει τη διαδικασία ρύθμισης ενός πρωτεύοντος και ενός δευτερεύοντος εξυπηρετητή kerberos ώστε να χρησιμοποιούν το OpenLDAP για τη βάση δεδομένων principal.



The examples presented here assume MIT Kerberos and OpenLDAP.

4.1. Ρύθμιση του OpenLDAP

Καταρχάς, πρέπει να φορτωθεί το κατάλληλο *σχήμα* πεσε έναν εξυπηρετητή OpenLDAP με δικτυακή σύνδεση στα πρωτεύοντα και δευτερεύοντα KDC. Στο υπόλοιπο αυτής της ενότητας υποθέτουμε ότι έχετε ρυθμίσει την αντιγραφή του LDAP μεταξύ δύο τουλάχιστον εξυπηρετητών. Για πληροφορίες σχετικά με τη ρύθμιση του OpenLDAP δείτε το *Τμήμα 1, “Εξυπηρετητής OpenLDAP” [97]*.

Επίσης, απαιτείται η ρύθμιση του OpenLDAP για συνδέσεις TLS και SSL, έτσι ώστε να κρυπτογραφείται η κίνηση μεταξύ KDC και εξυπηρετητή LDAP. Δείτε το *Τμήμα 1.8, “TLS” [112]* για λεπτομέρειες.



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.

- Για να φορτώσετε το σχήμα στο LDAP, εγκαταστήστε το πακέτο krb5-kdc-ldap στον εξυπηρετητή LDAP. Από το τερματικό, δίνετε:

```
sudo apt-get install krb5-kdc-ldap
```

- Στη συνέχεια, εξάγετε το αρχείο kerberos.schema.gz:

```
sudo gzip -d /usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz
```

```
sudo cp /usr/share/doc/krb5-kdc-ldap/kerberos.schema /etc/ldap/schema/
```

- Το σχήμα του *kerberos* πρέπει να προστεθεί στο δέντρο του *cn=config*. Η διαδικασία προσθήκης νέου σχήματος στο slapd περιγράφεται και στο *Τμήμα 1.4, “Modifying the slapd Configuration Database” [102]*.
 1. Καταρχάς, δημιουργήστε ένα αρχείο ρυθμίσεων με όνομα *schema_convert.conf*, ή κάτι εξίσου περιγραφικό, που θα περιέχει τις ακόλουθες γραμμές:


```
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. Δημιουργήστε έναν προσωρινό κατάλογο για τα αρχεία LDIF:

```
mkdir /tmp/ldif_output
```

3. Τώρα, χρησιμοποιήστε το `slapcat` για να μετατρέψετε τα αρχεία σχημάτων:

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s \  
"cn={12}kerberos,cn=schema,cn=config" > /tmp/cn=kerberos.ldif
```

Αλλάξτε τα ονόματα των αρχείων και διαδρομών αν έχετε χρησιμοποιήσει διαφορετικά.

4. Τροποποιήστε το αρχείο `/tmp/cn\=kerberos.ldif` που προκύπτει, αλλάζοντας τα ακόλουθα γνωρίσματα:

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

Και αφαιρέστε τις ακόλουθες γραμμές από το τέλος του αρχείου:

```
structuralObjectClass: olcSchemaConfig  
entryUUID: 18ccd010-746b-102d-9fbe-3760cca765dc  
creatorsName: cn=config  
createTimestamp: 20090111203515Z  
entryCSN: 20090111203515.326445Z#000000#000#000000  
modifiersName: cn=config  
modifyTimestamp: 20090111203515Z
```

Οι τιμές των γνωρισμάτων μπορεί να διαφέρουν, εσείς απλά βεβαιωθείτε ότι αφαιρέθηκαν τα συγκεκριμένα γνωρίσματα.

5. Φορτώστε το νέο αρχείο με το `ldapadd`:

```
ldapadd -x -D cn=admin,cn=config -W -f /tmp/cn\=kerberos.ldif
```

6. Προσθέστε ένα ευρετήριο για το γνώρισμα *krb5principalname*:

```
ldapmodify -x -D cn=admin,cn=config -W
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: krbPrincipalName eq,pres,sub
```

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

7. Τέλος, ενημερώστε τις Λίστες Ελέγχου Πρόσβασης (ACL):

```
ldapmodify -x -D cn=admin,cn=config -W
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
replace: olcAccess
olcAccess: to attrs=userPassword,shadowLastChange,krbPrincipalKey by
dn="cn=admin,dc=example,dc=com" write by anonymous auth by self write by * none
-
add: olcAccess
olcAccess: to dn.base="" by * read
-
add: olcAccess
olcAccess: to * by dn="cn=admin,dc=example,dc=com" write by * read
```

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

Αυτό ήταν, ο κατάλογος LDAP είναι τώρα έτοιμος να λειτουργήσει ως βάση δεδομένων principal Kerberos.

4.2. Ρύθμιση πρωτεύοντος KDC

Αφού ρυθμιστεί το OpenLDAP θα πρέπει να ρυθμιστεί και το KDC.

- Καταρχάς, εγκαταστήστε τα απαραίτητα πακέτα από το τερματικό, εισάγοντας:

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

- Τώρα, τροποποιήστε το */etc/krb5.conf*, προσθέτοντας τις ακόλουθες επιλογές στα κατάλληλα σημεία:

```
[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_kadmin_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
}

```



Αντικαταστήστε τα *example.com*, *dc=example,dc=com*, *cn=admin,dc=example,dc=com*, and *ldap01.example.com* με το κατάλληλο domain, αντικείμενο LDAP, και εξυπηρετητή LDAP.

- Στη συνέχεια, χρησιμοποιήστε το `kdb5_ldap_util` για να δημιουργήσετε το 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
```

- Αποθηκεύστε κρυφά (stash) τον κωδικό που χρησιμοποιείται σε σύνδεση με τον εξυπηρετητή LDAP. Πρόκειται για τον κωδικό που χρησιμοποιείται στις επιλογές *ldap_kdc_dn* και *ldap_kadmin_dn* του `/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
```

- Αντιγράψτε το πιστοποιητικό CA από τον εξυπηρετητή LDAP:

```
scp ldap01:/etc/ssl/certs/cacert.pem .
sudo cp cacert.pem /etc/ssl/certs
```

Και αλλάξτε το `/etc/ldap/ldap.conf` έτσι ώστε να χρησιμοποιεί το πιστοποιητικό:

```
TLS_CACERT /etc/ssl/certs/cacert.pem
```



Το πιστοποιητικό θα πρέπει να αντιγραφεί και στο δευτερεύον KDC, για να επιτρέπεται η σύνδεση στους εξυπηρετητές LDAP μέσω LDAPS.

Τώρα, μπορείτε να προσθέσετε τους `principal` Kerberos στη βάση δεδομένων LDAP. Θα αντιγραφούν και στους υπόλοιπους εξυπηρετητές LDAP που έχουν ρυθμιστεί για αντιγραφή. Για να προσθέσετε ένα `principal` χρησιμοποιήστε το `kadmin.local` και εισάγετε:

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.
```

Τα γνωρίσματα `krbPrincipalName`, `krbPrincipalKey`, `krbLastPwdChange`, and `krbExtraData` θα πρέπει πλέον να έχουν προστεθεί στο αντικείμενο χρήστη `uid=steve,ou=people,dc=example,dc=com`. Χρησιμοποιήστε τα `kinit` και `klist` για να ελέγξετε αν όντως εκδόθηκε δελτίο (ticket) για τον χρήστη.



Αν το αντικείμενο χρήστη έχει ήδη δημιουργηθεί, θα χρειαστεί η επιλογή `-x dn="..."` για την προσθήκη των γνωρισμάτων Kerberos. Διαφορετικά θα δημιουργηθεί νέο αντικείμενο *principal* στο υποδέντρο του `realm`.

4.3. Ρύθμιση δευτερεύοντος KDC

Η ρύθμιση του δευτερεύοντος KDC μέσω του backend του LDAP είναι παρόμοια με τη ρύθμισή του για χρήση της κανονικής βάσης δεδομένων Kerberos.

1. Καταρχάς, εγκαταστήστε τα απαραίτητα πακέτα από το τερματικό, εισάγοντας:

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

2. Στη συνέχεια, τροποποιήστε το `/etc/krb5.conf` ώστε να χρησιμοποιεί το backend του LDAP:

```
[libdefaults]
```

```

default_realm = EXAMPLE.COM

...

[realms]
    EXAMPLE.COM = {
        kdc = kdc01.example.com
        kdc = kdc02.example.com
        admin_server = kdc01.example.com
        admin_server = kdc02.example.com
        default_domain = example.com
        database_module = openldap_ldapconf
    }

...

[domain_realm]
    .example.com = EXAMPLE.COM

...

[dbdefaults]
    ldap_kerberos_container_dn = dc=example,dc=com

[dbmodules]
    openldap_ldapconf = {
        db_library = kldap
        ldap_kdc_dn = "cn=admin,dc=example,dc=com"

        # this object needs to have read rights on
        # the realm container, principal container and realm sub-trees
        ldap_kadmind_dn = "cn=admin,dc=example,dc=com"

        # this object needs to have read and write rights on
        # the realm container, principal container and realm sub-trees
        ldap_service_password_file = /etc/krb5kdc/service.keyfile
        ldap_servers = ldaps://ldap01.example.com ldaps://ldap02.example.com
        ldap_conns_per_server = 5
    }

```

3. Αποθηκεύστε τον κωδικό (stash) σύνδεσης με το LDAP:

```

sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com stashsrvpw -f \
/etc/krb5kdc/service.keyfile cn=admin,dc=example,dc=com

```

4. Τώρα, στο *πρωτεύον KDC* αντιγράψτε το κρυμμένο *κύριο κλειδί (master)* του */etc/krb5kdc/.k5.EXAMPLE.COM* στο δευτερεύον KDC. Θυμηθείτε να κάνετε την αντιγραφή μέσω κρυπτογραφημένης σύνδεσης, π.χ. με το *scp*, ή χρησιμοποιώντας φυσικό μέσο.

```

sudo scp /etc/krb5kdc/.k5.EXAMPLE.COM steve@kdc02.example.com:~
sudo mv .k5.EXAMPLE.COM /etc/krb5kdc/

```



Και εδώ, αντικαταστήστε το *EXAMPLE.COM* με το δικό σας realm.

5. Back on the *Secondary KDC*, (re)start the ldap server only,

sudo service slapd restart

6. Τέλος, εκκινήστε την υπηρεσία krb5-kdc:

sudo service krb5-kdc start

7. Verify the two ldap servers (and kerberos by extension) are in sync.

Τώρα το δίκτυό σας διαθέτει εφεδρικό KDC και μαζί με εφεδρικούς εξυπηρετητές LDAP, θα μπορείτε να συνεχίζετε να πιστοποιείτε χρήστες, ακόμη και αν δεν είναι διαθέσιμοι ένας εξυπηρετητής Kerberos, ένας εξυπηρετητής LDAP ή ένας εξυπηρετητής Kerberos και ένας LDAP.

4.4. Πόροι

- Ο *οδηγός διαχείρισης του Kerberos*⁵⁸ διαθέτει ορισμένες επιπλέον λεπτομέρειες.
- For more information on kdb5_ldap_util see *Section 5.6*⁵⁹ and the *kdb5_ldap_util man page*⁶⁰.
- Another useful link is the *krb5.conf man page*⁶¹.
- Also, see the *Kerberos and LDAP*⁶² Ubuntu wiki page.

⁵⁸ http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Configuring-Kerberos-with-OpenLDAP-back_002dend

⁵⁹ <http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Global-Operations-on-the-Kerberos-LDAP-Database>

⁶⁰ http://manpages.ubuntu.com/manpages/raring/en/man8/kdb5_ldap_util.8.html

⁶¹ <http://manpages.ubuntu.com/manpages/raring/en/man5/krb5.conf.5.html>

⁶² <https://help.ubuntu.com/community/Kerberos#kerberos-ldap>

Κεφάλαιο 8. Υπηρεσία ονομάτων τομέα (DNS)

Η υπηρεσία ονομάτων τομέα (DNS) είναι μια διαδικτυακή υπηρεσία που αντιστοιχίζει διευθύνσεις IP και πλήρως πιστοποιημένα ονόματα τομέα (FQDN) το ένα στο άλλο. Με αυτόν τον τρόπο, το DNS μας απαλλάσσει από την ανάγκη να θυμόμαστε διευθύνσεις IP. Οι υπολογιστές που εκτελούν το DNS ονομάζονται *εξυπηρετητές ονομάτων*. Το Ubuntu έρχεται με το BIND (Berkley Internet Naming Daemon), το πιο κοινό πρόγραμμα που χρησιμοποιείται για τη διατήρηση ενός εξυπηρετητή ονομάτων στο Linux.

1. Εγκατάσταση

Σε ένα τερματικό, πληκτρολογήστε την ακόλουθη εντολή για να εγκαταστήσετε το dns:

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


2. Ρυθμίσεις

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

- Όταν είναι ρυθμισμένο ως εξυπηρετητής ονομάτων προσωρινής αποθήκευσης, το BIND9 θα βρίσκει την απάντηση σε ερωτήματα ονομάτων και θα θυμάται την απάντηση όταν ερωτάται ξανά για το όνομα.
- 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. Επισκόπηση

Τα αρχεία ρυθμίσεων του DNS είναι αποθηκευμένα στον κατάλογο `/etc/bind`. Το κύριο αρχείο ρυθμίσεων είναι το `/etc/bind/named.conf`.

Η γραμμή *include* καθορίζει το όνομα του αρχείου που περιέχει τις επιλογές DNS. Η γραμμή *directory* στο αρχείο `/etc/bind/named.conf.options` λέει στο DNS πού να ψάξει για αρχεία.

Όλα τα αρχεία που χρησιμοποιεί το BIND θα είναι σε σχετική τοποθεσία με αυτόν τον κατάλογο.

Το αρχείο με όνομα `/etc/bind/db.root` περιγράφει τους κεντρικούς (root) εξυπηρετητές ονομάτων σε όλο τον κόσμο. Οι εξυπηρετητές αλλάζουν με την πάροδο του χρόνου, οπότε το αρχείο `/etc/bind/db.root` πρέπει να συντηρείται ανά διαστήματα. Αυτό συνήθως γίνεται με ενημερώσεις του πακέτου bind9. Η ενότητα *zone* ορίζει έναν εξυπηρετητή master και είναι αποθηκευμένη σε ένα αρχείο που αναφέρεται στην επιλογή *file*.

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. Εξυπηρετητής ονομάτων προσωρινής αποθήκευσης

Η προεπιλεγμένη ρύθμιση είναι η εγκατάσταση να λειτουργεί ως εξυπηρετητής προσωρινής αποθήκευσης. Αυτό που χρειάζεται είναι απλά η προσθήκη των διευθύνσεων IP των εξυπηρετητών DNS του παρόχου (ISP) σας. Απλά αποσχολιάστε και επεξεργαστείτε τα ακόλουθα στο `/etc/bind/named.conf.options`:

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



Αντικαταστήστε τα *1.2.3.4* και *5.6.7.8* με τις διευθύνσεις IP των πραγματικών εξυπηρετητών ονομάτων.

Τώρα επανεκκινήστε τον εξυπηρετητή DNS, για να ενεργοποιήσετε τις νέες ρυθμίσεις. Σε ένα τερματικό πληκτρολογήστε:

```
sudo service bind9 restart
```

Δείτε το *Τμήμα 3.1.2, “dig” [153]* για πληροφορίες σχετικά με τον έλεγχο ενός εξυπηρετητή DNS προσωρινής αποθήκευσης.

2.3. Κύριος Master

Σε αυτή την ενότητα το BIND9 θα ρυθμιστεί ως ο Κύριος Master εξυπηρετητής για τον χώρο *example.com*. Απλά αντικαταστήστε το *example.com* με το FQDN (Πλήρως πιστοποιημένο όνομα τομέα) σας.

2.3.1. Αρχείο ζώνης Forward

Για να προσθέσετε μια ζώνη DNS στο BIND9, μετατρέποντάς το σε έναν Κύριο Master εξυπηρετητή, το πρώτο βήμα είναι να επεξεργαστείτε το */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.)

Τώρα χρησιμοποιήστε ένα υπάρχον αρχείο ζώνης ως πρότυπο για να δημιουργήσετε το αρχείο */etc/bind/db.example.com*:

```
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
```

Πρέπει να αυξάνετε τον *σειριακό αριθμό* κάθε φορά που κάνετε αλλαγές στο αρχείο ζώνης. Αν κάνετε πολλές αλλαγές πριν επανεκκινήσετε το BIND9, απλά αυξήστε τον σειριακό αριθμό μία φορά.

Τώρα, μπορείτε να προσθέσετε καταγραφές DNS στο κάτω μέρος του αρχείου ζώνης. Δείτε το *Τμήμα 4.1, Κοινοί τύποι καταγραφών*; [157] για περισσότερες πληροφορίες.



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 service bind9 restart

2.3.2. Αρχείο ζώνης Reverse

Τώρα που η ζώνη έχει ρυθμιστεί και επιλύει ονόματα σε διευθύνσεις IP, χρειάζεται επίσης και μία *ζώνη Reverse*. Μία ζώνη Reverse επιτρέπει στο DNS να επιλύει διευθύνσεις σε ονόματα.

Επεξεργαστείτε το */etc/bind/named.conf.local* και προσθέστε τα ακόλουθα:

```
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```



Αντικαταστήστε το *1.168.192* με τις πρώτες τρεις οκτάδες (octets) του δικτύου που χρησιμοποιείτε. Επίσης, ονομάστε το αρχείο ζώνης */etc/bind/db.192* κατάλληλα. Πρέπει να είναι ταιριάζει με την πρώτη οκτάδα του δικτύου σας.

Τώρα δημιουργήστε το αρχείο `/etc/bind/db.192`:

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

Μετά επεξεργαστείτε το `/etc/bind/db.192` αλλάζοντας βασικά τις ίδιες επιλογές όπως στο `/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`.

Αφού δημιουργήσετε το αρχείο ζώνης reverse, επανεκκινήστε το BIND9:

```
sudo service bind9 restart
```

2.4. Δευτερεύων Master

Μόλις ένας *Κύριος Master* εξυπηρετητής έχει ρυθμιστεί, ένας *Δευτερεύων Master* χρειάζεται για να διατηρηθεί η διαθεσιμότητα του χώρου σε περίπτωση που ο Κύριος εξυπηρετητής δεν είναι διαθέσιμος.

Πρώτα, στον Κύριο Master εξυπηρετητή, η μεταφορά ζωνών πρέπει να επιτραπεί. Προσθέστε την επιλογή *allow-transfer* στα παραδείγματα ζωνών Forward και Reverse στο `/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; };  
};
```



Αντικαταστήστε το *192.168.1.11* με την διεύθυνση IP του δευτερεύοντα εξυπηρετητή ονομάτων.

Restart BIND9 on the Primary Master:

```
sudo service bind9 restart
```

Μετά, στον Δευτερεύοντα Master, εγκαταστήστε το πακέτο bind9 με τον ίδιο τρόπο όπως στον Κύριο. Μετά, επεξεργαστείτε το `/etc/bind/named.conf.local` και προσθέστε τις ακόλουθες γραμμές για τις ζώνες Forward και Reverse:

```
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; };  
};
```



Αντικαταστήστε το *192.168.1.10* με τη διεύθυνση IP του πρωτεύοντος εξυπηρετητή ονομάτων.

Επανεκκινήστε το BIND9 στον Δευτερεύοντα Master:

```
sudo service bind9 restart
```

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 *Τμήμα 4, “AppArmor” [176]*.

3. Επίλυση Προβλημάτων

Αυτή η ενότητα καλύπτει τρόπους που βοηθούν στην εύρεση της αιτίας όταν δημιουργούνται προβλήματα με το DNS και το BIND9.

3.1. Δοκιμή

3.1.1. resolv.conf

Το πρώτο βήμα για να δοκιμάσετε το BIND9 είναι να προσθέσετε τη διεύθυνση IP του εξυπηρετητή ονομάτων σε έναν επιλυτή (hosts resolver). Ο Κύριος εξυπηρετητής ονομάτων θα πρέπει να είναι ρυθμισμένος όπως και ένας άλλος υπολογιστής για να ελέγχονται δύο φορές τα πράγματα. Απλά επεξεργαστείτε το `/etc/resolv.conf` και προσθέστε τα ακόλουθα:

```
nameserver 192.168.1.10
nameserver 192.168.1.11
```



Θα πρέπει επίσης να προσθέσετε την διεύθυνση IP του δευτερεύοντος εξυπηρετητή ονομάτων για την περίπτωση που ο πρωτεύων δεν είναι διαθέσιμος.

3.1.2. dig

Αν εγκαταστήσετε το πακέτο `dnsutils`, μπορείτε να ελέγξετε την εγκατάστασή σας χρησιμοποιώντας το εργαλείο αναζήτησης DNS `dig`:

- Αφού εγκαταστήσετε το BIND9 χρησιμοποιήστε το `dig` με την διεπαφή `loopback` για να σιγουρευτείτε πως αναμένει για συνδέσεις στην θύρα 53. Σε ένα τερματικό πληκτρολογήστε:

```
dig -x 127.0.0.1
```

Θα πρέπει να δείτε γραμμές παρόμοιες με τις παρακάτω στο αποτέλεσμα της εντολής:

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

- Αν έχετε ρυθμίσει το BIND9 ως εξυπηρετητή ονομάτων *προσωρινής αποθήκευσης* (Caching), «κάντε» `dig` σε ένα εξωτερικό όνομα τομέα για να ελέγξετε τον χρόνο του ερωτήματος:

```
dig ubuntu.com
```

Παρατηρήστε τον χρόνο του ερωτήματος προς το τέλος του αποτελέσματος της εντολής:

:: Query time: 49 msec

Μετά από μία δεύτερη εκτέλεση του `dig` θα πρέπει να υπάρχει βελτίωση:

:: Query time: 1 msec

3.1.3. `ping`

Τώρα για να δείτε πώς οι εφαρμογές χρησιμοποιούν το DNS για να αναλύσουν ένα όνομα υπολογιστή χρησιμοποιήστε το εργαλείο `ping` για να στείλετε ένα αίτημα `echo ICMP`. Σε ένα τερματικό πληκτρολογήστε:

`ping example.com`

Αυτό ελέγχει αν ο εξυπηρετητής ονομάτων μπορεί να επιλύσει το όνομα *ns.example.com* σε διεύθυνση IP. Το αποτέλεσμα της εντολής θα πρέπει να μοιάζει με:

```
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`

Ένας πολύ καλός τρόπος για να ελέγξετε τα αρχεία ζώνης σας είναι χρησιμοποιώντας το εργαλείο `named-checkzone` που εγκαθίσταται με το πακέτο `bind9`. Αυτό το εργαλείο σας επιτρέπει να σιγουρευτείτε πως οι ρυθμίσεις είναι σωστές πριν επανεκκινήσετε το `BIND9` και να κάνετε τις αλλαγές άμεσα.

- Για να ελέγξετε το παράδειγμά μας αρχείου ζώνης `Forward` πληκτρολογήστε το παρακάτω σε μία γραμμή εντολών:

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

Αν τα πάντα είναι σωστά ρυθμισμένα, θα πρέπει να δείτε αποτέλεσμα παρόμοιο με:

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

- Παρομοίως, για να ελέγξετε το αρχείο ζώνης `Reverse` πληκτρολογήστε το ακόλουθο:

`named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192`

Η έξοδος πρέπει να είναι παρόμοια με:

```
zone 1.168.192.in-addr.arpa/IN: loaded serial 3  
OK
```




Ο σειριακός αριθμός της ζώνης σας πιθανότατα θα είναι διαφορετικός.

3.2. Καταγραφή

Το BIND9 έχει μια μεγάλη ποικιλία επιλογών για τη ρύθμιση της καταγραφής. Υπάρχουν δύο κύριες επιλογές. Η επιλογή *channel* ρυθμίζει πού πάνε οι καταγραφές και η επιλογή *category* καθορίζει τι πληροφορίες θα καταγράφονται.

Αν δεν οριστεί επιλογή καταγραφής, η προεπιλεγμένη επιλογή είναι:

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

Αυτή η ενότητα καλύπτει τη ρύθμιση του BIND9 ώστε να στέλνει πληροφορίες αποσφαλμάτωσης σχετικές με τα ερωτήματα DNS σε ένα ξεχωριστό αρχείο.

- Πρώτα, χρειάζεται να ρυθμίσουμε ένα κανάλι (*channel*) για να ορίσουμε σε ποιο αρχείο θα στέλνονται τα μηνύματα. Επεξεργαστείτε το `/etc/bind/named.conf.local` και προσθέστε το ακόλουθο:

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

- Μετά, ρυθμίστε μια κατηγορία (*category*) που θα στέλνει όλα τα ερωτήματα DNS στο αρχείο ερωτημάτων:

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



Σημείωση: Η επιλογή *debug* μπορεί να πάρει τιμή από 1 έως 3. Αν δεν οριστεί επίπεδο, η προεπιλογή είναι το επίπεδο 1.

- Αφού η υπηρεσία *named* εκτελείται ως ο χρήστης *bind*, το αρχείο `/var/log/query.log` πρέπει να δημιουργηθεί και να αλλαχτεί ο ιδιοκτήτης του:

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

sudo chown bind /var/log/query.log

- Πριν η υπηρεσία named μπορέσει να γράψει στο νέο αρχείο καταγραφής, το προφίλ του AppArmor πρέπει να ενημερωθεί. Πρώτα, επεξεργαστείτε το /etc/apparmor.d/usr.sbin.named και προσθέστε:

/var/log/query.log w,

Μετά, επαναφορτώστε το προφίλ:

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

Για περισσότερες πληροφορίες σχετικά με το AppArmor δείτε το *Τμήμα 4, “AppArmor” [176]*

- Τώρα επανεκκινήστε το BIND9 για να τεθούν σε ισχύ οι αλλαγές:

sudo service bind9 restart

Θα πρέπει να δείτε το αρχείο /var/log/query.log να γεμίζει με πληροφορίες ερωτημάτων. Αυτό είναι ένα απλό παράδειγμα των επιλογών καταγραφής που προσφέρει το BIND9. Για κάλυψη προχωρημένων επιλογών δείτε το *Τμήμα 4.2, “Περισσότερες πληροφορίες” [157]*.

4. Αναφορές

4.1. Κοινοί τύποι καταγραφών

Αυτή η ενότητα καλύπτει κάποιους από τους πιο κοινούς τύπους καταγραφών DNS.

- Καταγραφή *A*: Αυτή η καταγραφή αντιστοιχίζει μια διεύθυνση IP σε ένα όνομα συστήματος.

```
www IN A 192.168.1.12
```

- Καταγραφή *CNAME*: Χρησιμοποιείται για τη δημιουργία μιας συντόμευσης σε μία υπάρχουσα καταγραφή *A*. Δεν μπορείτε να δημιουργήσετε μια καταγραφή *CNAME* που να δείχνει σε άλλη καταγραφή *CNAME*.

```
web IN CNAME www
```

- Καταγραφή *MX*: Χρησιμοποιείται για να ορίσει πού θα πρέπει να στέλνονται τα email. Πρέπει να δείχνει σε μία καταγραφή *A*, όχι σε *CNAME*.

```
IN MX 1 mail.example.com.  
mail IN A 192.168.1.13
```

- Καταγραφή *NS*: Χρησιμοποιείται για να ορίσει ποιοι εξυπηρετητές παρέχουν αντίγραφα μιας ζώνης. Πρέπει να δείχνει σε μία καταγραφή *A*, όχι σε *CNAME*. Εδώ είναι που ορίζονται ο Πρωτεύων και ο Δευτερεύων εξυπηρετητής.

```
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. Περισσότερες πληροφορίες

- 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.

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>

- Ένα πολύ καλό μέρος για να ζητήσετε βοήθεια για το BIND9, και να συμμετάσχετε στην κοινότητα του Ubuntu Server, είναι το κανάλι IRC *#ubuntu-server* στο δίκτυο *freenode*⁶.

⁶ <http://freenode.net>

Κεφάλαιο 9. Ασφάλεια

Η ασφάλεια θα πρέπει πάντα να λαμβάνετε υπόψιν εγκαθιστάτε, αναπτύσσετε, και χρησιμοποιείται κάθε σύστημα υπολογιστή. Παρά το γεγονός ότι μια νέα εγκατάσταση Ubuntu είναι σχετικά ασφαλής για άμεση χρήση του Διαδικτύου, είναι σημαντικό να έχετε μια ισόρροπη κατανόηση της ασφάλειας του συστήματός σας για το πως θα χρησιμοποιηθεί μετά την ανάπτυξη.

This chapter provides an overview of security related topics as they pertain to Ubuntu 13.04 Server Edition, and outlines simple measures you may use to protect your server and network from any number of potential security threats.

1. Διαχείριση Χρηστών

Η διαχείριση χρηστών είναι ένα κρίσιμο σημείο για να διατηρηθεί η ασφάλεια συστήματος. Αναποτελεσματική διαχείριση χρηστών και προνομίων οδηγούν συχνά πολλά συστήματα σε κίνδυνο. Επομένως, είναι σημαντικό να καταλάβετε πώς μπορείτε να προστατεύσετε τον διακομιστή σας μέσα από απλές και αποτελεσματικές τεχνικές διαχείρισης του λογαριασμού χρήστη.

1.1. Που είναι η βάση;

Οι προγραμματιστές Ubuntu πήραν μια ευσυνείδητη να απενεργοποιήσουν το λογαριασμό διαχείρισης βάσης εξορισμού σε όλες τις εγκαταστάσεις Ubuntu. Αυτό δε σημαίνει ότι ο λογαριασμός βάσης έχει διαγραφεί ή δεν μπορεί να προσπελαστεί. Απλά του έχει δοθεί ένας κωδικός ο οποίος δεν ταιριάζει με καμία κρυπτογραφημένη τιμή, έτσι δεν μπορεί να συνδεθεί άμεσα μόνος του.

Αντίθετα, οι χρήστες ενθαρρύνονται να δημιουργήσουν ένα εργαλείο με όνομα `sudo` για να εκτελέσουν διαχειριστικά καθήκοντα του συστήματος. Το Sudo επιτρέπει σε έναν εξουσιοδοτημένο χρήστη προσωρινά να ανυψώσει τα δικαιώματά του χρησιμοποιώντας το δικό τους κωδικό αντί να πρέπει να γνωρίσουν τον κωδικό που ανήκει στο λογαριασμό βάσης. Αυτή η απλή αλλά αποτελεσματική μεθοδολογία παρέχει ευθύνη για όλες τις ενέργειες χρήστη, και δίνει στο διαχειριστή έλεγχο για το ποιες ενέργειες ένας χρήστης μπορεί να εκτελέσει με τα συγκεκριμένα προνόμια.

- Εάν για κάποιο λόγο θέλετε να ενεργοποιήσετε τον λογαριασμό βάσης, απλώς δώστε του έναν κωδικό:



Configurations with root passwords are not supported.

`sudo passwd`

Το Sudo θα σας ζητήσει τον κωδικό σας, και μετά θα σας ζητήσει να παρέχετε έναν καινούριο κωδικό για τη βάση όπως φαίνεται παρακάτω:

```
[sudo] password for username: (εισάγετε τον κωδικό σας)
Enter new UNIX password: (εισάγετε έναν καινούριο κωδικό για τη βάση)
Retype new UNIX password: (επαναλάβετε τον καινούριο κωδικό για τη βάση)
passwd: password updated successfully
```

- Για να απενεργοποιήσετε τον λογαριασμό βάσης, χρησιμοποιείτε την ακόλουθη σύνταξη `passwd`:

`sudo passwd -l root`

- Πρέπει να διαβάσετε περισσότερα για το Sudo κοιτώντας την αρχική του σελίδα:

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. Προσθήκη και Διαγραφή Χρηστών

Η διαδικασία διαχείρισης τοπικών χρηστών και ομάδων είναι άμεση και διαφέρει πολύ λίγο από τα περισσότερα λειτουργικά συστήματα GNU/Linux. Το Ubuntu και άλλες διανομές βασισμένες σε Debian, ενθαρρύνουν τη χρήση του πακέτου "adduser" για διαχείριση λογαριασμών.

- Για να προσθέσετε ένα λογαριασμό χρήστη, χρησιμοποιείτε την ακόλουθη σύνταξη, και ακολουθήστε τις προτροπές να δώσετε κωδικό στο λογαριασμό και αναγνωρίσιμα χαρακτηριστικά όπως πλήρες όνομα, τηλέφωνο, κλπ.

sudo adduser username

- Για να διαγράψετε ένα λογαριασμό χρήστη και την πρωταρχική του ομάδα, χρησιμοποιήστε την ακόλουθη σύνταξη:

sudo deluser username

Η διαγραφή ενός λογαριασμού δεν διαγράφει και τον αντίστοιχο αρχικό φάκελο. Εναπόκειται σε εσάς εάν επιθυμείτε να διαγράψετε τον φάκελο χειροκίνητα ή να τον κρατήσετε σύμφωνα με τις επιθυμητές πολιτικές διατήρησης σας.

Θυμηθείτε, κάθε χρήστης που προστίθεται αργότερα με το ίδιο UID/GID με τον προηγούμενο ιδιοκτήτη τώρα έχει πρόσβαση σε αυτόν τον φάκελο εάν δεν έχετε λάβει τις κατάλληλες προφυλάξεις.

Ίσως θέλετε να αλλάξετε τις τιμές UID/GID σε κάτι πιο κατάλληλο, όπως ο λογαριασμός βάσης, και πιθανόν ακόμα και να μεταφέρετε το φάκελο για να αποφευχθούν μελλοντικές συγκρούσεις:

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

- Για να κλειδώσετε ή να ξεκλειδώσετε προσωρινά ένα λογαριασμό χρήστη, χρησιμοποιήστε την ακόλουθη σύνταξη, αντιστοίχως:

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

- Για να προσθέσετε ή να διαγράψετε μια προσαρμοσμένη ομάδα, χρησιμοποιήστε την ακόλουθη σύνταξη, αντίστοιχα:

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

- Για να προσθέσετε μια ομάδα χρηστών, χρησιμοποιήστε την ακόλουθη σύνταξη:

```
sudo adduser username groupname
```

1.3. Ασφάλεια Προφίλ Χρήστη

Όταν δημιουργείτε ένας καινούριος χρήστης, η λειτουργία `adduser` δημιουργεί έναν ολοκαίνουριο αρχικό κατάλογο με όνομα `/home/username`, αντίστοιχα. Το προεπιλεγμένο προφίλ δημιουργείτε από τα περιεχόμενα που βρίσκονται στον κατάλογο `/etc/skel`, που περιλαμβάνει όλα τα βασικά στοιχεία προφίλ.

Εάν ο διακομιστής σας θα είναι αρχικός για πολλαπλούς χρήστες, θα πρέπει να προσέξετε πολύ τα δικαιώματα του αρχικού καταλόγου χρήστη για να βεβαιωθείτε για την εμπιστευτικότητα. Εξορισμού, οι αρχικοί καταλόγοι χρήστη στο Ubuntu δημιουργούνται με δικαιώματα ανάγνωσης/εκτέλεσης. Αυτό σημαίνει, ότι όλοι οι χρήστες μπορούν να περιηγηθούν και να έχουν πρόσβαση στα περιεχόμενα αρχικών καταλόγων άλλων χρηστών. Αυτό ίσως δεν είναι κατάλληλο για το περιβάλλον σας.

- Για να επαληθεύσετε τα δικαιώματα αρχικών καταλόγων των τρεχόντων χρηστών σας, χρησιμοποιήστε την ακόλουθη σύνταξη:

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

Η ακόλουθη έξοδος δείχνει ότι ο κατάλογος `/home/username` έχει δικαιώματα ανάγνωσης για όλους:

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

- Μπορείτε να αφαιρέσετε τα δικαιώματα ανάγνωσης για όλους χρησιμοποιώντας την ακόλουθη σύνταξη:

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



Μερικοί άνθρωποι έχουν την τάση να χρησιμοποιούν την αναδρομική επιλογή (-R) η οποία τροποποιεί αδιακρίτως όλους τους εξαρτημένους φακέλους και τα αρχεία, αλλά αυτό δεν είναι αναγκαίο, και μπορεί να αποφέρει άλλα ανεπιθύμητα αποτελέσματα. Ο γονικός κατάλογος από μόνος του είναι ικανός να εμποδίσει την παράνομη πρόσβαση σε οτιδήποτε κάτω από το γονικό κατάλογο.

Μια πολύ πιο αποτελεσματική προσέγγιση του θέματος θα ήταν να τροποποιήσετε τα εξορισμού καθολικά δικαιώματα του `adduser` όταν δημιουργείτε αρχικούς καταλόγους χρηστών. Απλώς επεξεργαστείτε το `/etc/adduser.conf` και ρυθμίστε τη μεταβλητή `DIR_MODE` σε κάτι κατάλληλο, ώστε όλοι οι καινούριοι αρχικοί κατάλογοι να λαμβάνουν τα σωστά δικαιώματα.

```
DIR_MODE=0750
```

- Αφού διορθώσετε τα δικαιώματα καταλόγου χρησιμοποιώντας τις προαναφερθείσες τεχνικές, επαληθεύστε τα αποτελέσματα χρησιμοποιώντας την ακόλουθη σύνταξη:

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

Τα αποτελέσματα παρακάτω δείχνουν ότι τα δικαιώματα ανάγνωσης για όλους έχουν αφαιρεθεί:

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

1.4. Πολιτική Κωδικού

Μια ισχυρή πολιτική κωδικού πρόσβασης είναι μία από τις πιο σημαντικές πτυχές της στάσης ασφαλείας σας. Πολλές επιτυχημένες παραβιάσεις της ασφάλειας περιλαμβάνουν απλά ωμή βία και επιθέσεις λεξικού εναντίον αδύναμων κωδικών πρόσβασης. Εάν σκοπεύετε να προσφέρετε οποιαδήποτε μορφή απομακρυσμένης πρόσβασης που να αφορά το τοπικό σύστημα κωδικού σας, βεβαιωθείτε ότι αντιμετωπίζετε ικανοποιητικά τις ελάχιστες απαιτήσεις της πολυπλοκότητας κωδικού πρόσβασης, το ανώτατο όριο διάρκειας ζωής κωδικού πρόσβασης, και τους συχνούς ελέγχους των συστημάτων ελέγχου ταυτότητας σας.

1.4.1. Ελάχιστο Μήκος Κωδικού

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=2 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=2 default=ignore] pam_unix.so obscure sha512 min=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. Λήξη Κωδικού

Όταν δημιουργείτε λογαριασμούς χρηστών, θα πρέπει να δημιουργήσετε μια πολιτική να έχετε ελάχιστη και μέγιστη ζωή κωδικού αναγκάζοντας τους χρήστες να αλλάζουν τους κωδικούς τους όταν λήγουν.

- Για να δείτε εύκολα την τρέχουσα κατάσταση ενός λογαριασμού χρήστη, χρησιμοποιείτε την ακόλουθη σύνταξη:

sudo chage -l username

Η έξοδος παρακάτω δείχνει ενδιαφέροντα στοιχεία για το λογαριασμό χρήστη, δηλαδή ότι δεν υπάρχουν πολιτικές που εφαρμόζονται:

```
Τελευταία αλλαγή κωδικού           : Jan 20, 2008
Ο Κωδικός λήγει                     : ποτέ
Κωδικός ανενεργός                   : ποτέ
Ο Λογαριασμός λήγει                 : ποτέ
Ελάχιστος αριθμών ημερών μεταξύ αλλαγών κωδικού : 0
Μέγιστος αριθμών ημερών μεταξύ αλλαγών κωδικού : 99999
Αριθμός ημερών προειδοποίησης πριν λήξει ο κωδικός : 7
```

- Για να ορίσετε οποιαδήποτε από αυτές τις τιμές, απλά χρησιμοποιείτε την ακόλουθη σύνταξη, και ακολουθήστε τις διαδραστικές προτροπές:

sudo chage username

Το ακόλουθο είναι επίσης ένα παράδειγμα για το πως να αλλάξετε χειροκίνητα την ρητή ημερομηνία λήξης (-E) σε 01/31/2008, την ελάχιστη ηλικία κωδικού (-m) σε 5 μέρες, την μέγιστη ηλικία κωδικού (-M) σε 90 μέρες, την περίοδο αδράνειας (-I) σε 5 μέρες μετά τη λήξη του κωδικού, και μια περίοδο προειδοποίησης (-W) 14 ημερών πριν λήξει ο κωδικός.

sudo chage -E 01/31/2011 -m 5 -M 90 -I 30 -W 14 username

- Για να επαληθεύσετε τις αλλαγές, χρησιμοποιήστε την ίδια σύνταξη που χρησιμοποιήθηκε προηγουμένως:

sudo chage -l username

Η έξοδος παρακάτω δείχνει τις νέες πολιτικές που έχουν θεσπιστεί για το λογαριασμό:

```
Τελευταία αλλαγή κωδικού           : Jan 20, 2008
Ο Κωδικός λήγει                     : Apr 19, 2008
Κωδικός ανενεργός                   : May 19, 2008
Ο Λογαριασμός λήγει                 : Jan 31, 2008
Ελάχιστος αριθμών ημερών μεταξύ αλλαγών κωδικού : 5
```

Μέγιστος αριθμών ημερών μεταξύ αλλαγών κωδικού : 90
Αριθμός ημερών προειδοποίησης πριν λήξει ο κωδικός : 14

1.5. Άλλα Θέματα Ασφάλειας

Πολλές εφαρμογές χρησιμοποιούν εναλλακτικούς μηχανισμούς πιστοποίησης οι οποίοι μπορούν εύκολα να παραβλεφθούν ακόμα και από έμπειρους διαχειριστές συστημάτων. Ως εκ τούτου, είναι σημαντικό να καταλάβετε και να ελέγξετε πως οι χρήστες πιστοποιούν την ταυτότητά τους και αποκτούν πρόσβαση σε υπηρεσίες και εφαρμογές στο διακομιστή σας.

1.5.1. Πρόσβαση SSH από Απενεργοποιημένους Χρήστες

Με το να απενεργοποιήσετε/κλειδώσετε τον λογαριασμό ενός χρήστη δε θα τον αποτρέψετε από το να συνδέετε στο διακομιστή σας εξ αποστάσεως εάν έχει στήσει στο παρελθόν ένα δημόσιο κλειδί πιστοποίησης RSA. Θα μπορεί ακόμα να αποκτά πρόσβαση κελύφους στο διακομιστή, χωρίς να χρειάζεται κωδικό. Θυμηθείτε να ελέγξετε το αρχικό κατάλογο του χρήστη για αρχεία που θα επιτρέψουν αυτού του είδους την πιστοποιημένη SSH πρόσβαση πχ. `/home/username/.ssh/authorized_keys`.

Διαγράψτε ή μετονομάστε τον κατάλογο `.ssh/` στον αρχικό κατάλογο του χρήστη για να αποτραπούν οι περαιτέρω δυνατότητες πιστοποίησης SSH.

Σιγουρευτείτε ότι ελέγξατε για εγκατεστημένες συνδέσεις SSH από τον απενεργοποιημένο χρήστη, καθώς είναι πιθανό να έχουν υπαρκτές εισερχόμενες ή εξερχόμενες συνδέσεις. Τερματίστε όποιες βρείτε.

Περιορίστε την πρόσβαση SSH μόνο σε λογαριασμούς χρηστών που πρέπει να την έχουν. Για παράδειγμα, μπορείτε να δημιουργήσετε μια ομάδα με όνομα `"sshlogin"` και να εισάγετε το όνομα της ομάδας στην τιμή που είναι συναφής με τη μεταβλητή `AllowGroups` που βρίσκεται στο αρχείο `/etc/ssh/sshd_config`.

```
AllowGroups sshlogin
```

Ύστερα προσθέστε τους χρήστες στους οποίους επιτρέπεται το SSH στην ομάδα `"sshlogin"`, και επανεκκινήστε την υπηρεσία SSH.

```
sudo adduser username sshlogin  
sudo service ssh restart
```

1.5.2. Εξωτερική Ταυτοποίηση Χρήστη Βάσης Δεδομένων

Τα περισσότερα δίκτυα επιχειρήσεων απαιτούν κεντρικό έλεγχο ταυτότητας και ελέγχους πρόσβασης για όλους τους πόρους συστήματος. Εάν έχετε διαμορφώσει το διακομιστή σας να πιστοποιεί τους χρήστες από εξωτερικές βάσεις δεδομένων, βεβαιωθείτε ότι έχετε

απενεργοποιήσει τους λογαριασμούς χρηστών εξωτερικά και τοπικά, με αυτόν τον τρόπο εξασφαλίζεται ότι η τοπική επαναφορά ταυτοποίησης δεν είναι δυνατή.

2. Ασφάλεια Κονσόλας

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.

Οι ακόλουθες οδηγίες θα βοηθήσουν να υπερασπίσετε το διακομιστή σας ενάντια σε θέματα που θα μπορούσαν να αποφέρουν σοβαρές συνέπειες.

2.1. Απενεργοποίηση Ctrl+Alt+Delete

Πρώτο και κυριότερο, ο καθένας που έχει φυσική πρόσβαση στο πληκτρολόγιο μπορεί απλά να χρησιμοποιήσει τον συνδυασμό κλειδιών **Ctrl+Alt+Delete** για να επανεκκινήσει το διακομιστή χωρίς να χρειαστεί να συνδεθεί. Σίγουρα, κάποιος μπορούσε απλά να αποσυνδέσει την παροχή ρεύματος, αλλά θα πρέπει ακόμα να εμποδίσετε την χρήση αυτού του συνδυασμού κλειδιών σε έναν διακομιστή παραγωγής. Αυτό αναγκάζει έναν επιτιθέμενο να λάβει πιο δραστικά μέτρα για να επανεκκινήσει το διακομιστή και θα εμποδίσει τυχαίες επανεκκινήσεις την ίδια ώρα.

- Για να απενεργοποιήσετε την ενέργεια επανεκκίνησης που γίνεται πατώντας το συνδυασμό πλήκτρων **Ctrl+Alt+Delete**, διαγράψτε το σχόλιο από την ακόλουθη γραμμή στο αρχείο `/etc/init/control-alt-delete.conf`.

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

3. Τείχος Προστασίας

3.1. Εισαγωγή

Ο πυρήνας Linux περιλαμβάνει το υποσύστημα *Netfilter*, το οποίο χρησιμοποιείται για να χειραγωγεί ή να αποφασίσει τη μοίρα της κίνησης δικτύου που κινείται προς ή μέσω του διακομιστή σας. Όλες οι μοντέρνες λύσεις τείχους προστασίας Linux χρησιμοποιούν αυτό το σύστημα για φιλτράρισμα πακέτων.

Το σύστημα φιλτραρίσματος πακέτων του πυρήνα θα ήταν ελάχιστης χρήσης για τους διαχειριστές χωρίς μια διεπαφή χώρου χρήστη για να το διαχειρίζεται. Αυτός είναι ο σκοπός των πινάκων ip. Όταν ένα πακέτο φτάνει στο διακομιστή σας, θα περαστεί στο υποσύστημα Netfilter για αποδοχή, χειραγώγηση, ή απόρριψη βάσει των κανόνων που παραχωρούνται από το χώρο χρήστη μέσω των πινάκων ip. Έτσι, οι πίνακες ip είναι το μόνο που χρειάζεστε για να διαχειριστείτε το τείχος προστασίας εάν είστε εξοικειωμένοι με αυτό, αλλά υπάρχουν και πολλές προσόψεις διαθέσιμες για να απλοποιήσετε το έργο.

3.2. ufw - Απλό Τείχος Προστασίας

Το προεπιλεγμένο εργαλείο διαμόρφωσης του τείχους προστασίας για το Ubuntu είναι το ufw. Αναπτυγμένο για να διευκολύνει τη διαμόρφωση πινάκων ip τείχους προστασίας, το ufw παρέχει έναν φιλικό προς το χρήστη τρόπο να δημιουργήσει ένα IPv4 ή IPv6 τείχος προστασίας βασισμένο σε κεντρικό υπολογιστή

Το ufw εξορισμού είναι αρχικά απενεργοποιημένο. Από την κεντρική σελίδα ufw:

Το ufw δεν προορίζεται για να παρέχει πλήρη λειτουργικότητα του τοίχου προστασίας μέσω της διεπαφής εντολών, αλλά αντίθετα παρέχει έναν εύκολο τρόπο να προσθέτετε ή να αφαιρείται απλούς κανόνες. Προς το παρόν χρησιμοποιείται κυρίως για τείχη προστασίας βασισμένα σε κεντρικό υπολογιστή.

Τα ακόλουθα είναι κάποια παραδείγματα για το πως να χρησιμοποιήσετε το ufw:

- Πρώτον, το ufw χρειάζεται να ενεργοποιηθεί. Από ένα τερματικό εντολών εισάγετε:

```
sudo ufw enable
```

- Για να ανοίξετε μια θύρα (ssh σε αυτό το παράδειγμα):

```
sudo ufw allow 22
```

- Κανόνες μπορούν επίσης να προστεθούν χρησιμοποιώντας τη μορφή *numbered*:

```
sudo ufw insert 1 allow 80
```

- Ομοίως, για να κλείσετε μια ανοιχτή θύρα:

sudo ufw deny 22

- Για να αφαιρέσετε έναν κανόνα, χρησιμοποιείτε delete ακολουθούμενο από τον κανόνα:

sudo ufw delete deny 22

- Είναι επίσης πιθανό να επιτραπεί πρόσβαση από συγκεκριμένους κεντρικούς υπολογιστές και δίκτυα σε μια θύρα. Το ακόλουθο παράδειγμα επιτρέπει πρόσβαση ssh από τον κεντρικό υπολογιστή 192.168.0.2 σε οποιαδήποτε διεύθυνση ip σε αυτόν τον κεντρικό υπολογιστή:

sudo ufw allow proto tcp from 192.168.0.2 to any port 22

Αντικαταστήστε το 192.168.0.2 με 192.168.0.0/24 για να επιτρέψετε πρόσβαση ssh από ολόκληρο το υποδίκτυο.

- Προσθέτοντας την επιλογή *--dry-run* σε μια εντολή *ufw* θα έχει έξοδο τους ακόλουθους κανόνες, αλλά δε θα τους εφαρμόσει. Για παράδειγμα, το ακόλουθο είναι αυτό που θα εφαρμοζόταν αν ανοίγατε την θύρα HTTP:

sudo ufw --dry-run allow http

*filter

:ufw-user-input - [0:0]

:ufw-user-output - [0:0]

:ufw-user-forward - [0:0]

:ufw-user-limit - [0:0]

:ufw-user-limit-accept - [0:0]

RULES

tuple ### allow tcp 80 0.0.0.0/0 any 0.0.0.0/0

-A ufw-user-input -p tcp --dport 80 -j ACCEPT

END RULES

-A ufw-user-input -j RETURN

-A ufw-user-output -j RETURN

-A ufw-user-forward -j RETURN

-A ufw-user-limit -m limit --limit 3/minute -j LOG --log-prefix "[UFW LIMIT]: "

-A ufw-user-limit -j REJECT

-A ufw-user-limit-accept -j ACCEPT

COMMIT

Rules updated

- Το *ufw* μπορεί να απενεργοποιηθεί με:

sudo ufw disable

- Για να δείτε την κατάσταση του τείχους προστασίας, πληκτρολογείτε:

sudo ufw status

- Και για περισσότερες πληροφορίες κατάστασης πληκτρολογείτε:

sudo ufw status verbose

- Για να δείτε τη μορφή *numbered*:

sudo ufw status numbered



Εάν η θύρα που θέλετε να ανοίξετε ή κλείσετε ορίζετε στο `/etc/services`, μπορείτε να χρησιμοποιήσετε το όνομα της θύρας αντί για το νούμερο. Στα παραπάνω παραδείγματα, αντικαταστήστε το 22 με *ssh*.

Αυτή είναι μια γρήγορη εισαγωγή για το πως να χρησιμοποιήσετε το ufw. Παρακαλώ αναφερθείτε στη σελίδα ufw για περισσότερες πληροφορίες.

3.2.1. Συγκεκρισμός Εφαρμογή ufw

Οι εφαρμογές που ανοίγουν θύρες μπορούν να περιλαμβάνουν ένα προφίλ ufw, το οποίο αναφέρει λεπτομέρειες για το ποιες θύρες χρειάζονται ώστε η εφαρμογή να εκτελεστεί κανονικά. Τα προφίλ κρατούνται στο `/etc/ufw/applications.d`, και μπορούν να επεξεργαστούν εάν οι προεπιλεγμένες θύρες έχουν αλλάξει.

- Για να δείτε ποιες εφαρμογές έχουν εγκαταστήσει ένα προφίλ, πληκτρολογήστε τα ακόλουθα σε ένα τερματικό:

sudo ufw app list

- Όμοια με το να επιτρέψετε κίνηση σε μια θύρα, το να χρησιμοποιήσετε ένα προφίλ εφαρμογής γίνεται πληκτρολογώντας:

sudo ufw allow Samba

- Μια επεκτεταμένη σύνταξη είναι επίσης διαθέσιμη:

ufw allow from 192.168.0.0/24 to any app Samba

Αντικαταστήστε τα *Samba* και *192.168.0.0/24* με το προφίλ εφαρμογής που χρησιμοποιείτε και την εμβέλεια IP για το δίκτυό σας.



Δεν είναι αναγκαίο να προσδιορίσουμε το *πρωτόκολλο* για την εφαρμογή, επειδή αυτή η πληροφορία είναι λεπτομερής στο προφίλ. Επίσης, σημειώστε ότι το όνομα *εφαρμογής* αντικαθιστά το νούμερο της *θύρας*.

- Για να δείτε λεπτομέρειες για το ποιες θύρες, πρωτόκολλα, κλπ προσδιορίζονται για μια εφαρμογή, πληκτρολογείτε:

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. Μεταμφίεση IP

Ο σκοπός της Μεταμφίεσης IP είναι να επιτρέψει σε μηχανές με ιδιωτικές, μη δρομολογήσιμες διευθύνσεις IP του δικτύου σας να έχουν πρόσβαση στο διαδικτύου μέσω της μηχανής που κάνει τη μεταμφίεση. Η κίνηση από τα ιδιωτικά σας δίκτυα που προορίζεται για το Διαδίκτυο, πρέπει να χειραγωγηθεί ώστε να είναι οι απαντήσεις δρομολογήσιμες πίσω στην μηχανή που έκανε την αίτηση. Για να το κάνετε αυτό, ο πυρήνας πρέπει να τροποποιήσει την *πηγαία* διεύθυνση IP για κάθε πακέτο ώστε οι απαντήσεις να δρομολογούνται πίσω σε αυτό, και όχι στην ιδιωτική διεύθυνση IP η οποία έκανε το αίτημα, κάτι αδύνατο μέσω του Διαδικτύου. Το Linux χρησιμοποιεί *Εντοπισμό Σύνδεσης* (conntrack) για να ελέγχει ποιες συνδέσεις ανήκουν σε ποιες μηχανές και να αναδρομολογήσει κάθε πακέτο επιστροφής ανάλογα. Η κίνηση που αφήνει το ιδιωτικό σας δίκτυο είναι γι' αυτό "μεταμφιεσμένη" σαν να προήλθε από μηχανή πυλώνα Ubuntu. Αυτή η διαδικασία αναφέρεται στις βοηθητικές οδηγίες της Microsoft σαν Διαμοιρασμός Διαδικτυακής Σύνδεσης.

3.3.1. Μεταμφίεση ufw

Η Μεταμφίεση IP μπορεί να επιτευχθεί χρησιμοποιώντας προσαρμοσμένους κανόνες ufw. Αυτό είναι πιθανό επειδή το τρέχων πρόγραμμα υποστήριξης για το ufw είναι iptables-restore με τους κανόνες του αρχείου να βρίσκονται στο /etc/ufw/*.rules. Αυτά τα αρχεία είναι ένα τέλειο μέρος για να προσθέσετε παλιούς κανόνες πινάκων ip που χρησιμοποιούνται χωρίς ufw, και κανόνες που είναι περισσότερο συναφείς με πυλώνες δικτύου ή γέφυρες.

Οι κανόνες χωρίζονται σε δύο διαφορετικά αρχεία, σε κανόνες που πρέπει να εκτελεστούν πριν τους κανόνες γραμμής εντολών ufw, και κανόνες που πρέπει να εκτελεστούν μετά τους κανόνες γραμμής εντολών ufw.

- Πρώτα, η προώθηση πακέτου πρέπει να ενεργοποιηθεί στο ufw. Δύο αρχεία διαμόρφωσης θα πρέπει να προσαρμοστούν, στο /etc/default/ufw αλλάξτε το `DEFAULT_FORWARD_POLICY` σε `“ACCEPT”;`

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

Μετά επεξεργαστείτε το /etc/ufw/sysctl.conf αποσχολιάστε το:

```
net/ipv4/ip_forward=1
```

Ομοίως, για την προώθηση IPv6 αποσχολιάστε το:

```
net/ipv6/conf/default/forwarding=1
```

- τώρα θα προσθέσουμε κανόνες στο αρχείο `/etc/ufw/before.rules`. Οι προεπιλεγμένοι κανόνες διαμορφώνουν μόνο τον πίνακα *φίλτρων*, και για να ενεργοποιήσουμε τη μεταμφίηση του πίνακα *nat* θα πρέπει να διαμορφωθεί. Προσθέστε τα ακόλουθα στην κορυφή του αρχείου μετά τα σχόλια κεφαλίδας:

```
# ανόνες Πίνακα nat
```

```
*nat
```

```
:POSTROUTING ACCEPT [0:0]
```

```
# Προωθήστε κίνηση από eth1 μέσω eth0.
```

```
-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE
```

```
# μην διαγράψετε τη γραμμή 'COMMIT' ή αλλιώς οι κανόνες πίνακα nat δε θα μεταποιηθούν  
COMMIT
```

Τα σχόλια δεν είναι αυστηρώς αναγκαία, αλλά θεωρείται καλή άσκηση να καταγράφετε τη διαμόρφωσή σας. Επίσης, όταν διαμορφώνετε οποιοδήποτε από τα αρχεία *κανόνων* στο `/etc/ufw`, σιγουρευτείτε ότι αυτές οι γραμμές είναι οι τελευταίες γραμμές για κάθε πίνακα που διαμορφώνετε.

```
# μη διαγράψετε τη γραμμή 'COMMIT' αλλιώς αυτοί οι κανόνες δε θα μεταποιηθούν  
COMMIT
```

Για κάθε *Πίνακα* μια αντίστοιχη δήλωση *COMMIT* απαιτείται. Σε αυτά τα παραδείγματα εμφανίζονται οι πίνακες *nat* και *φίλτρου*, αλλά μπορείτε επίσης να προσθέσετε κανόνες για τους πίνακες *raw* και *mangle*.



Στο παραπάνω παράδειγμα αντικαταστήστε τα *eth0*, *eth1*, και *192.168.0.0/24* με την κατάλληλη διεπαφή και εμβέλεια IP για το δίκτυό σας.

- Τέλος, απενεργοποιήστε και επαναενεργοποιήστε το ufw για να ισχύσουν οι αλλαγές:

```
sudo ufw disable && sudo ufw enable
```

Η Μεταμφίηση IP πρέπει τώρα να έχει ενεργοποιηθεί. Μπορείτε επίσης να εισάγετε όποιους επιπλέον κανόνες ΠΡΟΩΘΗΣΗΣ στο `/etc/ufw/before.rules`. Συστήνεται ότι αυτοί οι επιπρόσθετοι κανόνες μπορούν να προστεθούν στην αλυσίδα *ufw-before-forward*.

3.3.2. Μεταμφίηση Πινάκων IP

iptables can also be used to enable Masquerading.

- Ομοίως με το `ufw`, το πρώτο βήμα είναι να ενεργοποιήσετε την προώθηση πακέτου IPv4 κάνοντας επεξεργασία στο `/etc/sysctl.conf` και αποσχολιάζοντας την ακόλουθη γραμμή

```
net.ipv4.ip_forward=1
```

Εάν επιθυμείτε να ενεργοποιήσετε την προώθηση IPv6 επίσης αποσχολιάστε το:

```
net.ipv6.conf.default.forwarding=1
```

- Μετά, εκτελέστε την εντολή `sysctl` για να ενεργοποιήσετε τις καινούριες ρυθμίσεις στο αρχείο διαμόρφωσης:

```
sudo sysctl -p
```

- Η Μεταμφίεση IP μπορεί τώρα να επιτευχθεί με έναν απλό κανόνα πίνακα `ip`, ο οποίος μπορεί να διαφέρει λίγο ανάλογα με τη διαμόρφωση δικτύου σας:

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

Η παραπάνω εντολή υποθέτει ότι ο χώρος των ιδιωτικών σας διευθύνσεων είναι `192.168.0.0/16` και ότι η συσκευή αντιμετώπισης Διαδικτύου είναι `ppp0`. Η σύνταξη αναλύεται όπως ακολούθως:

- `-t nat` -- ο κανόνας πρέπει να πάει στον πίνακα `nat`
- `-A POSTROUTING` -- ο κανόνας πρέπει να προσαρτηθεί στην αλυσίδα (`-A`) `POSTROUTING`
- `-s 192.168.0.0/16` -- ο κανόνας εφαρμόζεται στην κίνηση που παράγεται από τον προσαρμοσμένο χώρο διευθύνσεων
- `-o ppp0` -- ο κανόνας εφαρμόζεται σε κίνηση σχεδιασμένη να δρομολογηθεί μέσω της συσκευής δικτύου
- `-j MASQUERADE` -- η κίνηση που ταιριάζει σε αυτόν τον κανόνα πρέπει να "μεταπηδήσει" (`-j`) στο στόχο `MASQUERADE` για να χειραγωγηθεί όπως αναφέρεται παραπάνω
- Επίσης, κάθε αλυσίδα τον πίνακα φίλτρου (ο προεπιλεγμένος πίνακας, και εκεί που γίνεται το περισσότερο ή όλο το φιλτράρισμα πακέτων) έχει μια προεπιλεγμένη *πολιτική* ΑΠΟΔΟΧΗΣ, αλλά εάν δημιουργείτε ένα τείχος προστασίας εκτός από μια μηχανή πυλών, ίσως έχετε ορίσει τις πολιτικές ΡΗΞΗ ή ΑΠΟΡΡΙΨΗ, στην οποία περίπτωση η μεταμφιεσμένη κίνηση πρέπει να επιτρέπεται μέσω της αλυσίδας ΠΡΟΩΘΗΣΗΣ για να δουλέψει ο παραπάνω κανόνας:

```
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
```

Οι παραπάνω εντολές θα επιτρέψουν όλες τις συνδέσεις από το τοπικό σας δίκτυο στο Διαδίκτυο και όλη την κίνηση που σχετίζεται με εκείνες τις συνδέσεις να επιστρέψει στην μηχανή που τις επέτρεψε.

- Εάν θέλετε να ενεργοποιείται η μεταμφίεση κατά την εκκίνηση, κάτι που μάλλον θέλετε, επεξεργαστείτε το `/etc/rc.local` και προσθέστε οποιοδήποτε σχόλιο χρησιμοποιήθηκε παραπάνω. Για παράδειγμα προσθέστε την πρώτη εντολή χωρίς φίλτρα:

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

3.4. Ιστορικά

Τα ιστορικά του Τείχους Προστασίας είναι σημαντικά για αναγνώριση επιθέσεων, επίλυση προβλημάτων των κανόνων του τείχους προστασίας, και για παρατήρηση ασυνήθιστης δραστηριότητας στο δίκτυό σας. Πρέπει να περιλάβετε κανόνες δημιουργίας ιστορικού στο τείχος προστασίας για να παραχθούν, όμως, οι κανόνες δημιουργίας ιστορικού πρέπει να έρθουν πριν από κάθε εφαρμοστέο κανόνα τερματισμού (ένας κανόνας με στόχο που αποφασίζει την τύχη του πακέτου, όπως ΑΠΟΔΟΧΗ, ΡΗΞΗ, ή ΑΠΟΡΡΙΨΗ).

Εάν χρησιμοποιείτε το `ufw`, μπορείτε να ενεργοποιήσετε τη δημιουργία ιστορικού πληκτρολογώντας σε ένα τερματικό εντολών:

sudo ufw logging on

Για να απενεργοποιήσετε τη δημιουργία ιστορικού του `ufw`, απλώς αντικαταστήστε το *on* με *off* στην παραπάνω εντολή.

Εάν χρησιμοποιείτε πίνακες `ip` αντί του `ufw`, πληκτρολογήστε:

```
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=00:00:00:00:00:00:00:00:00:00:00:08:00
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. Άλλα Εργαλεία

Υπάρχουν πολλά διαθέσιμα εργαλεία για να σας βοηθήσουν να κατασκευάσετε ένα πλήρες τείχος προστασίας χωρίς οικεία γνώση πινάκων ip. Για την GUI-κλίση:

- Το *fwbuilder*¹ είναι πολύ ισχυρό και θα φαίνεται γνώριμο σε έναν διαχειριστή ο οποίος έχει χρησιμοποιήσει μια λειτουργία εμπορικού τείχους προστασίας όπως το Checkpoint Firewall-1.

Εάν προτιμάτε ένα εργαλείο γραμμής-εντολών με διαμόρφωση αρχείων απλού-κειμένου:

- Το *Shorewall*² είναι μια πολύ ισχυρή λύση για να σας βοηθήσει να διαμορφώσετε ένα προηγμένο τείχος προστασίας για κάθε δίκτυο.

3.6. Αναφορές

- The *Ubuntu Firewall*³ wiki page contains information on the development of ufw.
- Επίσης, η σελίδα εγχειριδίου του ufw περιέχει μερικές πολύ χρήσιμες πληροφορίες: **man ufw**.
- Δείτε το *packet-filtering-HOWTO*⁴ για περισσότερες πληροφορίες για τη χρήση πινάκων ip.
- Το *nat-HOWTO*⁵ περιέχει επιπλέον λεπτομέρειες για τη μεταμφίηση.
- 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

Το AppArmor είναι μία εκτέλεση Υπομονάδας Ασφαλείας Linux υποχρεωτικών ελέγχων πρόσβαση βασισμένης σε ονόματα. Το AppArmor περιορίζει μεμονωμένα προγράμματα σε ένα σύνολο απ αριθμημένων αρχείων και προσχέδιων ικανοτήτων posix 1003.1e

Το AppArmor εγκαθιστάται και φορτώνεται από προεπιλογή. Χρησιμοποιεί *προφίλ* μιας εφαρμογής για να διαπιστώσει τι αρχεία και διακαιώματα απαιτεί η εφαρμογή. Μερικά πακέτα θα εγκαταστήσουν τα δικά του προφίλ, και επιπρόσθετα προφίλ μπορούν βρεθούν στο πακέτο apparmor-profiles.

Για να εγκαταστήσετε το πακέτο apparmor-profiles από ένα τερματικό εντολών:

```
sudo apt-get install apparmor-profiles
```

Τα προφίλ του AppArmor έχουν δύο καταστάσεις εκτέλεσης:

- **Complaining/Learning:** οι παραβάσεις προφίλ επιτρέπονται και καταγράφονται. Χρήσιμο για έλεγχο και ανάπτυξη νέων προφίλ.
- **Enforced/Confined:** ενισχύει την πολιτική προφίλ καθώς και την καταγραφή παραβάσεων.

4.1. Χρήση AppArmor

Το πακέτο apparmor-utils περιέχει λειτουργίες γραμμής εντολών τις οποίες μπορείτε να χρησιμοποιήσετε ώστε να αλλάξετε την κατάσταση εκτέλεσης του AppArmor, να βρείτε την κατάσταση ενός προφίλ, να δημιουργήσετε νέα προφίλ, κλπ.

- Το `apparmor_status` χρησιμοποιείται για να προβληθεί η τρέχουσα κατάσταση των προφίλ του AppArmor.

```
sudo apparmor_status
```

- Το `aa-complain` βάζει ένα προφίλ σε κατάσταση *complain*

```
sudo aa-complain /path/to/bin
```

- Το `aa-enforce` τοποθετεί ένα προφίλ σε κατάσταση *enforce*.

```
sudo aa-enforce /path/to/bin
```

- Ο κατάλογος `/etc/apparmor.d` είναι εκεί όπου βρίσκονται τα προφίλ του AppArmor. Μπορεί να χρησιμοποιηθεί για να χειραγωγηθεί η κατάσταση όλων των προφίλ.

Πληκτρολογείτε τα ακόλουθα για να τοποθετήσετε όλα τα προφίλ σε κατάσταση `complain`:

```
sudo aa-complain /etc/apparmor.d/*
```

Για να τοποθετήσετε όλα τα προφίλ σε κατάσταση enforce:

```
sudo aa-enforce /etc/apparmor.d/*
```

- Το `apparmor_parser` χρησιμοποιείται για να φορτώσετε ένα προφίλ στον πυρήνα. Μπορεί επίσης να χρησιμοποιηθεί για να επαναφορτώσετε ένα ήδη φορτωμένο προφίλ χρησιμοποιώντας την επιλογή `-r`. Για να φορτώσετε ένα προφίλ:

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

Για να επαναφορτώσετε ένα προφίλ:

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -r
```

- `service apparmor` can be used to *reload* all profiles:

```
sudo service apparmor reload
```

- Ο κατάλογος `/etc/apparmor.d/disable` μπορεί να χρησιμοποιηθεί μαζί με την επιλογή `apparmor_parser -R` για να *απενεργοποιήσετε* ένα προφίλ.

```
sudo ln -s /etc/apparmor.d/profile.name /etc/apparmor.d/disable/  
sudo apparmor_parser -R /etc/apparmor.d/profile.name
```

Για να *επανεπενεργοποιήσετε* ένα απενεργοποιημένο προφίλ αφαιρέστε τον συμβολικό σύνδεσμο του προφίλ στο `/etc/apparmor.d/disable/`. Ύστερα φορτώστε το προφίλ χρησιμοποιώντας την επιλογή `-a`.

```
sudo rm /etc/apparmor.d/disable/profile.name  
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

- Το `AppArmor` μπορεί να απενεργοποιηθεί, και η υπομονάδα πυρήνα να αποφορτωθεί πληκτρολογώντας τα ακόλουθα:

```
sudo service apparmor stop  
sudo update-rc.d -f apparmor remove
```

- Για να επανεργοποιήσετε το `AppArmor` πληκτρολογείτε:

```
sudo service apparmor start  
sudo update-rc.d apparmor defaults
```



Αντικαταστήστε το *profile.name* με το όνομα του προφίλ το οποίο θέλετε να παραποιήσετε. Επίσης, αντικαταστήστε το `/path/to/bin/` με το πραγματικό μονοπάτι

εκτελέσιμου αρχείου. Για παράδειγμα για την εντολή `ping` χρησιμοποιείτε το `/bin/ping`

4.2. Προφίλ

Τα προφίλ του AppArmor είναι απλά αρχεία κειμένου που βρίσκονται στο AppArmor. Τα αρχεία παίρνουν το όνομά τους από το πλήρες μονοπάτι του εκτελέσιμου αντικαθιστώντας το `/` με `.`. Για παράδειγμα το `/etc/apparmor.d/bin.ping` είναι το προφίλ AppArmor για την εντολή `/bin/ping`.

Υπάρχουν δύο κύριοι τύποι κανόνων που χρησιμοποιούνται στα προφίλ:

- *Καταχωρήσεις μονοπατιού*: που δίνουν λεπτομέρειες για το σε ποια αρχεία στο σύστημα αρχείων μπορεί να έχει πρόσβαση μια εφαρμογή
- *Καταχωρήσεις ικανοτήτων*: καθορίζουν τι δικαιώματα επιτρέπεται να χρησιμοποιεί μια περιορισμένη διαδικασία.

Σαν παράδειγμα κοιτάξτε στο `/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>*: περίληψη δηλώσεων από άλλα αρχεία. Αυτό επιτρέπει σε δηλώσεις που αφορούν πολλές εφαρμογές να τοποθετηθούν σε ένα κοινό αρχείο.
- */bin/ping flags=(complain)*: μονοπάτι στο πρόγραμμα του προφίλ, επίσης θέτει την κατάσταση σε *complain*.
- *capability net_raw*: επιτρέπει στην εφαρμογή πρόσβαση στο CAP_NET_RAW Posix.1e capability.
- */bin/ping mixr*: επιτρέπει στην εφαρμογή πρόσβαση ανάγνωσης και εκτέλεσης στο αρχείο.



Αφού επεξεργαστείτε ένα αρχείο προφίλ το προφίλ θα πρέπει να επαναφορτωθεί. Δείτε το [Τμήμα 4.1, Χρήση AppArmor](#); [176] για λεπτομέρειες.

4.2.1. Δημιουργία ενός Προφίλ

- *Σχεδιάστε ένα δοκιμαστικό σχέδιο:* Προσπαθήστε να σκεφτείτε πως η εφαρμογή θα πρέπει να ασκείται. Το σχέδιο ελέγχου θα πρέπει να διαχωριστεί σε πολλές υποθέσεις ελέγχου. Κάθε υπόθεση ελέγχου θα πρέπει να έχει μια μικρή περιγραφή και να καταγράφει τα βήματα που ακολουθούν.

Κάποιες πρότυπες υποθέσεις ελέγχου είναι:

- Εκκίνηση του προγράμματος.
- Τερματισμός του προγράμματος.
- Επαναφόρτωση του προγράμματος.
- Έλεγχος όλων των εντολών που υποστηρίζονται από το σενάριο `init`.
- *Παραγωγή του καινούριου προφίλ:* Χρησιμοποιείτε το `aa-genprof` για να παράγετε ένα καινούριο προφίλ. Από ένα τερματικό:

aa-genprof

Για παράδειγμα:

sudo aa-genprof slapd

- Για να συμπεριλάβετε το καινούριο σας προφίλ στο πακέτο `apparmor-profiles`, υποβάλετε ένα σφάλμα στο *Launchpad* εναντίον του πακέτου *AppArmor*⁷:
- Συμπεριλάβετε το σχέδιο ελέγχου και τις υποθέσεις ελέγχου.
- Επισυνάψτε το καινούριο προφίλ στο σφάλμα.

4.2.2. Ενημέρωση Προφίλ

Όταν ένα πρόγραμμα συμπεριφέρεται άσχημα, μηνύματα ελέγχου αποστέλλονται στα αρχεία ιστορικού. Το πρόγραμμα `aa-logprof` μπορεί να χρησιμοποιηθεί για να σαρώσετε τα αρχεία ιστορικού για μηνύματα ελέγχου `AppArmor`, να τα αναθεωρήσετε και να ενημερώσετε τα προφίλ. Από ένα τερματικό:

sudo aa-logprof

4.3. Αναφορές

- Δείτε το *AppArmor Administration Guide*⁸ για προηγμένες επιλογές διαμόρφωσης.
- Για πληροφορίες για το πως να χρησιμοποιήσετε το `AppArmor` με άλλες κυκλοφορίες Ubuntu δείτε τη σελίδα *AppArmor Community Wiki*⁹.

⁷ <https://bugs.launchpad.net/ubuntu/+source/apparmor/+filebug>

⁸ http://www.novell.com/documentation/apparmor/apparmor201_sp10_admin/index.html?page=/documentation/apparmor/apparmor201_sp10_admin/data/book_apparmor_admin.html

⁹ <https://help.ubuntu.com/community/AppArmor>

- The *OpenSUSE AppArmor*¹⁰ page is another introduction to AppArmor.
- Ένα τέλειο μέρος για να ζητήσετε βοήθεια για το AppArmor, και να λάβετε μέρος στην κοινότητα Διακομιστή Ubuntu, είναι το κανάλι IRC *#ubuntu-server* στο *freenode*¹¹.

¹⁰ http://en.opensuse.org/SDB:AppArmor_geeks

¹¹ <http://freenode.net>

5. Πιστοποιητικά

Μια από τις πιο κοινές μορφές κρυπτογραφίας σήμερα είναι η κρυπτογραφία *δημόσιου-κλειδιού*. Η κρυπτογραφία δημοσίου κλειδιού χρησιμοποιεί ένα *δημόσιο κλειδί* και ένα *ιδιωτικό κλειδί*. Το σύστημα λειτουργεί *κρυπτογραφώντας* πληροφορίες με τη χρήση του δημοσίου κλειδιού. Οι πληροφορίες μπορούν να *αποκρυπτογραφηθούν* μόνο με τη χρήση του ιδιωτικού κλειδιού.

Μια κοινή χρήση της κρυπτογραφίας δημοσίου κλειδιού είναι η κρυπτογράφηση κίνησης εφαρμογών χρησιμοποιώντας σύνδεση Στρώματος Ασφαλούς Υποδοχέα (Secure Socket Layer (SSL)) ή Μεταφοράς Στρώματος Ασφάλειας (Transport Layer Security (TLS)). Για παράδειγμα, η διαμόρφωση του Apache ώστε να παρέχει *HTTPS*, το πρωτόκολλο HTTP πάνω από SSL. Αυτό επιτρέπει έναν τρόπο να κρυπτογραφήσετε κίνηση χρησιμοποιώντας ένα πρωτόκολλο το οποίο δεν παρέχει κρυπτογράφηση από μόνο του.

Το *Certificate* είναι μια μέθοδος που χρησιμοποιείται για να διανέμει ένα *δημόσιο κλειδί* και άλλες πληροφορίες για έναν διακομιστή και τον οργανισμό ο οποίος είναι υπεύθυνος για αυτόν. Τα πιστοποιητικά μπορεί να είναι ψηφιακά υπογεγραμμένα από μια *Αρχή Πιστοποίησης* ή ΑΠ. Η ΑΠ είναι ένας αξιόπιστος τρίτος που έχει επιβεβαιώσει ότι οι πληροφορίες που περιέχονται στο πιστοποιητικό είναι ακριβείς.

5.1. Είδη Πιστοποιητικών

Για να στήσετε έναν ασφαλή διακομιστή χρησιμοποιώντας κρυπτογράφηση δημοσίου-κλειδιού, στις περισσότερες περιπτώσεις, στέλνετε το αίτημα πιστοποιητικού (συμπεριλαμβανομένου και του δημοσίου κλειδιού σας), απόδειξη την ταυτότητας της εταιρίας σας, και πληρωμή σε μια ΑΠ. Η ΑΠ επαληθεύει το αίτημα πιστοποιητικού και την ταυτότητά σας, και μετά σας στέλνει ένα πιστοποιητικό για τον ασφαλή διακομιστή σας. Εναλλακτικά, μπορείτε να δημιουργήσετε το δικό σας *υπογεγραμμένο από εσάς* πιστοποιητικό.



Σημειώστε, ότι πιστοποιητικά υπογεγραμμένα από εσάς δε θα πρέπει να χρησιμοποιούνται στα περισσότερα περιβάλλοντα παραγωγής.

Συνεχίζοντας το παράδειγμα HTTPS, ένα πιστοποιητικό υπογεγραμμένο από ΑΠ παρέχει δύο σημαντικές δυνατότητες που ένα πιστοποιητικό υπογεγραμμένο από εσάς δεν παρέχει:

- Οι φυλλομετρητές (συνήθως) αναγνωρίζουν αυτόματα το πιστοποιητικό και επιτρέπουν μια ασφαλή σύνδεση να δημιουργηθεί χωρίς να προτρέψει το χρήστη.
- Όταν μια ΑΠ εκδίδει ένα υπογεγραμμένο πιστοποιητικό, εγγυάται την ταυτότητα του οργανισμού ο οποίος παρέχει τη σελίδα ιστού στο φυλλομετρητή.

Οι περισσότεροι φυλλομετρητές Ιστού, και υπολογιστές, οι οποίοι υποστηρίζουν SSL έχουν λίστα ΑΠ των οποίων τα πιστοποιητικά αποδέχονται αυτόματα. Εάν ένας φυλλομετρητής

αντιμετωπίσει ένα πιστοποιητικό του οποίου η εξουσιοδοτημένη ΑΠ δεν είναι στη λίστα, ο φυλλομετρητής ζητάει από τον χρήστη να δεχθεί ή να απορρίψει την σύνδεση. Επίσης, άλλες εφαρμογές μπορούν να παράγουν ένα μήνυμα σφάλματος όταν χρησιμοποιούν ένα πιστοποιητικό υπογεγραμμένο από εσάς.

Η διαδικασία του να πάρετε ένα πιστοποιητικό από μια ΑΠ είναι σχετικά εύκολο. Μια γρήγορη επισκόπηση είναι όπως ακολούθως:

1. Δημιουργήστε ένα ζευγάρι ιδιωτικού και δημόσιου κλειδιού κρυπτογράφησης.
2. Δημιουργήστε ένα αίτημα πιστοποιητικού βασισμένο στο δημόσιο κλειδί. Το αίτημα πιστοποιητικού περιέχει πληροφορίες για το διακομιστή σας και την εταιρία που τον στεγάζει.
3. Στείλτε το αίτημα πιστοποιητικού, μαζί με αρχεία που αποδεικνύουν την ταυτότητά σας, σε μια ΑΠ. Δεν μπορούμε να σας πούμε πια αρχή πιστοποίησης να διαλέξετε. Η απόφασή σας μπορεί να βασίζεται σε παλαιότερη εμπειρία, ή σε εμπειρίες των φίλων ή συναδέλφων σας, ή αμιγώς σε οικονομικούς παράγοντες.

Όταν έχετε αποφασίσει σε μια ΑΠ, πρέπει να ακολουθήσετε τις οδηγίες που παρέχουν για το πως να αποκτήσετε ένα πιστοποιητικό από αυτούς.

4. Όταν η ΑΠ έχει βεβαιωθεί ότι είστε αυτός που ισχυρίζεστε, σας στέλνουν ένα ψηφιακό πιστοποιητικό.
5. Εγκαταστήστε το πιστοποιητικό σας στον ασφαλή διακομιστή σας, και διαμορφώστε τις κατάλληλες εφαρμογές για να χρησιμοποιήσετε το πιστοποιητικό.

5.2. Παραγωγή ενός Αιτήματος Υπογραφής Πιστοποιητικού (ΑΥΠ)

Είτε πάρετε ένα πιστοποιητικό από μια ΑΠ είτε παράγετε το δικό σας υπογεγραμμένο από εσάς, το πρώτο βήμα είναι η παραγωγή κλειδιού.

Εάν το πιστοποιητικό θα χρησιμοποιηθεί σε δαίμονες υπηρεσιών, όπως τα Apache, Postfix, Dovecot, κλπ, ένα κλειδί χωρίς κωδική φράση είναι συνήθως κατάλληλο. Η μη χρησιμοποίηση κωδικής φράσης επιτρέπει στις υπηρεσίες να εκκινούν χωρίς χειροκίνητη παρέμβαση, συνήθως ο προτιμώμενος τρόπος να ξεκινήσει ένας δαίμονας.

Αυτή η ενότητα θα καλύψει την παραγωγή κλειδιού με κωδική φράση, και ενός χωρίς. Το κλειδί χωρίς κωδική φράση θα χρησιμοποιηθεί ύστερα για την παραγωγή ενός πιστοποιητικού το οποίο μπορεί να χρησιμοποιηθεί σε ποικίλους δαίμονες υπηρεσιών.



Το να εκτελείτε την ασφαλή υπηρεσία σας χωρίς κωδική φράση είναι βολικό επειδή δεν χρειάζεται να εισάγετε την κωδική φράση κάθε φορά που εκκινείτε την ασφαλή υπηρεσία σας. Αλλά δεν είναι ασφαλές και η έκθεση κλειδιού σημαίνει την έκθεση του διακομιστή επίσης.

Για να παράγετε ένα κλειδί για το Αίτημα Υπογραφής Πιστοποιητικού (ΑΥΠ) εκτελέστε την ακόλουθη εντολή από ένα τερματικό εντολών:

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:

Τώρα μπορείτε να εισάγετε την κωδική φράση. Για μεγαλύτερη ασφάλεια, πρέπει να περιέχει τουλάχιστον οκτώ χαρακτήρες. Το ελάχιστο μέγεθος όταν προσδιορίζετε `-des3` είναι τέσσερις χαρακτήρες. Θα πρέπει να περιλαμβάνει αριθμούς και/ή σημεία στίξης και όχι να είναι μια λέξη σε ένα λεξικό. Επίσης θυμηθείτε ότι η κωδική σας φράση είναι ευαίσθητη στα κεφαλαία-μικρά γράμματα.

Επαναπληκτρολογείστε την κωδική φράση για να την επαληθεύσετε. Όταν την έχετε επαναπληκτρολογήσει σωστά, το κλειδί διακομιστή παράγεται και αποθηκεύεται στο αρχείο `server.key`.

Τώρα δημιουργήστε το μη ασφαλές κλειδί, αυτό χωρίς κωδική φράση, και ανακατέψτε τα ονόματα κλειδιών:

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

Το μη ασφαλές κλειδί έχει τώρα όνομα `server.key`, και μπορείτε να χρησιμοποιήσετε αυτό το αρχείο για να παράγετε ένα ΑΥΠ χωρίς κωδική φράση.

Για να δημιουργήσετε ένα ΑΥΠ, εκτελέστε την ακόλουθη εντολή σε ένα τερματικό εντολών:

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.

Μπορείτε τώρα να υποβάλετε αυτό το αρχείο ΑΥΠ σε μια ΑΠ για διεργασία. Η ΑΠ θα χρησιμοποιήσει αυτό ΑΥΠ αρχείο κα θα εκδώσει ένα πιστοποιητικό. Αφ' ετέρου, μπορείτε να δημιουργήσετε ένα πιστοποιητικό υπογεγραμμένο από εσάς με αυτό το ΑΥΠ.

5.3. Δημιουργία ενός Πιστοποιητικού Υπογεγραμμένου από εσάς

Για να δημιουργήσετε ένα πιστοποιητικό υπογεγραμμένο από εσάς, εκτελέστε την ακόλουθη εντολή σε ένα τερματικό εντολών:

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

Η παραπάνω εντολή θα σας ζητήσει να εισάγετε την κωδική φράση. Όταν εισάγετε τη σωστή κωδική φράση, το πιστοποιητικό σας θα δημιουργηθεί και θα αποθηκευτεί στο αρχείο `server.crt`.



Αν ο ασφαλής διακομιστής σας θα χρησιμοποιηθεί σε περιβάλλον παραγωγής, πιθανόν χρειάζεστε ένα πιστοποιητικό υπογεγραμμένο από μια ΑΠ. Δε συστήνεται να χρησιμοποιήσετε ένα πιστοποιητικό υπογεγραμμένο από εσάς.

5.4. Εγκατάσταση του Πιστοποιητικού

Μπορείτε να εγκαταστήσετε το αρχείο κλειδιού `server.key` και το αρχείο πιστοποιητικού `server.crt`, ή το αρχείο πιστοποιητικού που έχει παραχθεί από την ΑΠ, εκτελώντας τις ακόλουθες εντολές σε ένα τερματικό εντολών:

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

Τώρα απλώς διαμορφώστε τις εφαρμογές, με την ικανότητα χρήσης κρυπτογράφησης δημόσιου-κλειδιού, για να χρησιμοποιήσουν τα αρχεία *πιστοποιητικού* και *κλειδιού*. Για παράδειγμα, ο Apache μπορεί να παρέχει HTTPS, το Dovecot μπορεί να παρέχει IMAPS και POP3S, κ.λ.π.

5.5. Αρχή Πιστοποίησης

Εάν οι υπηρεσίες του δικτύου σας απαιτούν παραπάνω από μερικά πιστοποιητικά υπογεγραμμένα από εσάς ίσως αξίζει τον κόπο να στήσετε μια εσωτερική *Αρχή Πιστοποίησης (ΑΠ)*. Χρησιμοποιώντας πιστοποιητικά υπογεγραμμένα από τη δική σας ΑΠ, επιτρέπει τις διάφορες υπηρεσίες που χρησιμοποιούν τα πιστοποιητικά να εμπιστεύονται εύκολα άλλες υπηρεσίες που χρησιμοποιούν πιστοποιητικά που έχουν παραχθεί από την ίδια ΑΠ>

1. Πρώτον, δημιουργήστε τους καταλόγους που θα κρατήσουν τα πιστοποιητικά ΑΠ και τα σχετικά αρχεία:

```
sudo mkdir /etc/ssl/CA
sudo mkdir /etc/ssl/newcerts
```

2. Η ΑΠ χρειάζεται μερικά επιπρόσθετα αρχεία για να λειτουργήσει, ένα για να παρακολουθεί τους τελευταίους σειριακούς αριθμούς που χρησιμοποιήθηκαν από την ΑΠ, κάθε πιστοποιητικό πρέπει να έχει ένα μοναδικό σειριακό αριθμό, και ένα άλλο αρχείο να καταγράφει ποια πιστοποιητικά έχουν εκδοθεί:

```
sudo sh -c "echo '01' > /etc/ssl/CA/serial"
```

```
sudo touch /etc/ssl/CA/index.txt
```

3. Το τρίτο αρχείο είναι ένα αρχείο διαμόρφωσης της ΑΠ. Παρόλο που δεν είναι αυστηρώς αναγκαίο, είναι πολύ βολικό όταν εκδίδονται πολλαπλά πιστοποιητικά. Επεξεργαστείτε το `/etc/ssl/openssl.cnf`, και το `[CA_default]` αλλάξτε τα:

```
dir          = /etc/ssl/          # Όπου όλα διατηρούνται
database     = $dir/CA/index.txt  # βάση δεδομένων αρχείου ευρετηρίου.
certificate   = $dir/certs/cacert.pem # Το πιστοποιητικό ΑΠ
serial       = $dir/CA/serial     # Ο τρέχων σειριακός αριθμός
private_key   = $dir/private/cakey.pem # Το ιδιωτικό κλειδί
```

4. Μετά, δημιουργήστε το υπογεγραμμένο από εσάς πιστοποιητικό βάσης:

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
```

Ύστερα θα σας ζητηθεί να εισάγετε λεπτομέρειες σχετικές με το πιστοποιητικό.

5. Τώρα εγκαταστήστε το πιστοποιητικό και το κλειδί βάσης:

```
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
```

6. Είστε τώρα έτοιμοι να αρχίσετε να υπογράφετε πιστοποιητικά. Το πρώτο αντικείμενο που χρειάζεστε είναι ένα Αίτημα Υπογραφής Πιστοποιητικού (ΑΥΠ), δείτε *Τμήμα 5.2, “Παραγωγή ενός Αιτήματος Υπογραφής Πιστοποιητικού (ΑΥΠ)” [182]* για λεπτομέρειες. Όταν έχετε ένα ΑΥΠ, εισάγετε τα ακόλουθα για να παράγετε ένα πιστοποιητικό υπογεγραμμένο από την ΑΠ:

```
sudo openssl ca -in server.csr -config /etc/ssl/openssl.cnf
```

Αφού εισάγετε τον κωδικό για το κλειδί ΑΠ, θα σας ζητηθεί να υπογράψετε το πιστοποιητικό, και ξανά να παραδώσετε το νέο πιστοποιητικό. Ύστερα θα πρέπει να δείτε ένα σχετικά μεγάλο όγκο εξόδου σχετικό με τη δημιουργία του πιστοποιητικού.

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.

Μεταγενέστερα πιστοποιητικά θα ονομαστούν `02.pem`, `03.pem`, κλπ.



Αντικαταστήστε το `mail.example.com.crt` με το δικό σας περιγραφικό όνομα.

8. Τέλος, αντιγράψτε το καινούριο πιστοποιητικό στον κεντρικό υπολογιστή που το χρειάζεται, και διαμορφώστε τις κατάλληλες εφαρμογές για να το χρησιμοποιήσουν. Η εξορισμού τοποθεσία για να εγκαταστήσετε πιστοποιητικά είναι η `/etc/ssl/certs`. Αυτό

επιτρέπει σε πολλαπλές υπηρεσίες να χρησιμοποιούν τα ίδια πιστοποιητικά χωρίς ιδιαίτερα περίπλοκες άδειες αρχείων.

Για εφαρμογές που μπορούν να διαμορφωθούν για να χρησιμοποιήσουν ένα πιστοποιητικό ΑΠ, θα πρέπει επίσης να αντιγράψετε το αρχείο `the /etc/ssl/certs/cacert.pem` στον κατάλογο `/etc/ssl/certs/` σε κάθε διακομιστή.

5.6. Αναφορές

- Για πιο λεπτομερείς οδηγίες για τη χρήση κρυπτογράφησης δείτε το *SSL Certificates HOWTO*¹² από το `tldp.org`
- Η σελίδα της Wikipedia *HTTPS*¹³ περιέχει περισσότερες πληροφορίες σχετικά με το HTTPS.
- Για περισσότερες πληροφορίες για το *OpenSSL* δείτε την *Κεντρική Σελίδα OpenSSL*¹⁴.
- Επίσης, το *Network Security with OpenSSL*¹⁵ του O'Reilly είναι μια καλή σε βάθος αναφορά.

¹² <http://tldp.org/HOWTO/SSL-Certificates-HOWTO/index.html>

¹³ <http://en.wikipedia.org/wiki/Https>

¹⁴ <http://www.openssl.org/>

¹⁵ <http://oreilly.com/catalog/9780596002701/>

6. eCryptfs

Το *eCryptfs* είναι ένα συμμορφωμένο με POSIX κρυπτογραφικό σύστημα αρχείων κατηγορίας επιχειρήσεων σε στοίβα για Linux. Δημιουργώντας στρώμα πάνω από το στρώμα του συστήματος αρχείων το *eCryptfs* προστατεύει αρχεία χωρίς να έχει σημασία το υποκείμενο σύστημα αρχείων, ο τύπος διαμερίσματος, κλπ.

Κατά τη διάρκεια της εγκατάστασης υπάρχει μια επιλογή να κρυπτογραφήσετε το `/home` διαμέρισμα. Αυτό θα διαμορφώσει αυτόματα ότι χρειάζεται για να κρυπτογραφηθεί και να φορτωθεί το διαμέρισμα.

As an example, this section will cover configuring `/srv` to be encrypted using *eCryptfs*.

6.1. Χρήση του eCryptfs.

Πρώτον, εγκαταστήστε τα απαραίτητα πακέτα. Από ένα τερματικό εντολών πληκτρολογείτε:

```
sudo apt-get install ecryptfs-utils
```

Τώρα φορτώστε ένα διαμέρισμα να κρυπτογραφηθεί:

```
sudo mount -t ecryptfs /srv /srv
```

Ύστερα θα σας ζητηθούν κάποιες λεπτομέρειες για το πως το `ecryptfs` να κρυπτογραφήσει τα δεδομένα.

Για να ελέγξετε αν τα αρχεία που τοποθετήθηκαν στο `/srv` όντως αποκρυπτογραφήθηκαν αντιγράψτε το φάκελο `/etc/default` στο `/srv`:

```
sudo cp -r /etc/default /srv
```

Τώρα, αποφορτώστε το `/srv`, και προσπαθήστε να δείτε το αρχείο:

```
sudo umount /srv  
cat /srv/default/cron
```

Φορτώνοντας ξανά το `/srv` χρησιμοποιώντας το `ecryptfs` θα κάνει τα δεδομένα να προβληθούν ξανά.

6.2. Αυτόματη Φόρτωση Κρυπτογραφημένων Διαμερισμάτων

Υπάρχουν κάποιοι τρόποι να φορτώνετε αυτόματα ένα κρυπτογραφημένο `ecryptfs` σύστημα αρχείων κατά την εκκίνηση. Αυτό το παράδειγμα θα χρησιμοποιήσει ένα αρχείο `/root/.ecryptfsrc` το οποίο περιέχει επιλογές φόρτωσης, μαζί με ένα αρχείο κωδικής φράσης που βρίσκεται σε ένα κλειδί USB.

Πρώτον, δημιουργήστε το `/root/.ecryptfs` που περιέχει:

```
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
```



Προσαρμόστε το `ecryptfs_sig` στην υπογραφή στο `/root/.ecryptfs/sig-cache.txt`.

Μετά, δημιουργήστε ένα αρχείο κωδικής φράσης `/mnt/usb/passwd_file.txt`:

```
passphrase_passwd=[secrets]
```

Τώρα προσθέστε τις απαραίτητες γραμμές στο `/etc/fstab`:

```
/dev/sdb1 /mnt/usb ext3 ro 0 0
/srv /srv encryptfs defaults 0 0
```

Βεβαιωθείτε ότι ο οδηγός USB είναι φορτωμένος πριν από το κρυπτογραφημένο διαμέρισμα.

Finally, reboot and the `/srv` should be mounted using *eCryptfs*.

6.3. Άλλες Λειτουργίες

Το πακέτο `ecryptfs-utils` περιλαμβάνει πολλές άλλες χρήσιμες λειτουργίες:

- *ecryptfs-setup-private*: δημιουργεί έναν `~/Private` για να περιέχει κρυπτογραφημένες πληροφορίες. Αυτή η λειτουργία μπορεί να εκτελεστεί από χρήστες χωρίς δικαιώματα για να διατηρηθούν τα δεδομένα ιδιωτικά από άλλους χρήστες στο σύστημα.
- *ecryptfs-mount-private* and *ecryptfs-umount-private*: θα φορτώσει και αποφορτώσει αντίστοιχα, έναν `~/Private` κατάλογο χρήστη.
- *ecryptfs-add-passphrase*: προσθέτει μια καινούρια κωδική φράση στην κλειδοθήκη του πυρήνα.
- *ecryptfs-manager*: διαχειρίζεται αντικείμενα *eCryptfs* όπως κλειδιά.
- *ecryptfs-stat*: σας επιτρέπει να προβάλετε τις *ecryptfs* meta πληροφορίες για ένα αρχείο.

6.4. Αναφορές

- For more information on *eCryptfs* see the *Launchpad project page*¹⁶.
- There is also a *Linux Journal*¹⁷ article covering *eCryptfs*.

¹⁶ <https://launchpad.net/ecryptfs>

¹⁷ <http://www.linuxjournal.com/article/9400>

- Also, for more `ecryptfs` options see the *ecryptfs man page*¹⁸.
- The *eCryptfs Ubuntu Wiki*¹⁹ page also has more details.

¹⁸ <http://manpages.ubuntu.com/manpages/raring/en/man7/ecryptfs.7.html>

¹⁹ <https://help.ubuntu.com/community/eCryptfs>

Κεφάλαιο 10. Παρακολούθηση

1. Επισκόπηση

Η παρακολούθηση των εξυπηρετητών και υπηρεσιών ζωτικής σημασίας αποτελεί σημαντικό συστατικό της διαχείρισης συστημάτων. Οι περισσότερες υπηρεσίες δικτύου παρακολουθούνται και ελέγχονται όσον αφορά την απόδοση ή/και τη διαθεσιμότητά τους. Αυτή η ενότητα θα καλύψει την εγκατάσταση και ρύθμιση του Nagios για την παρακολούθηση της διαθεσιμότητας και του Munin για την παρακολούθηση της απόδοσης.

Στα παραδείγματα αυτής της ενότητας θα χρησιμοποιηθούν δύο εξυπηρετητές με ονόματα *server01* και *server02*. Στον *Server01* θα γίνει ρύθμιση του Nagios για την παρακολούθηση των υπηρεσιών στον ίδιο και στον *server02*. Στον *Server01* θα εγκατασταθεί και το πακέτο *munin* για τη συλλογή πληροφοριών από το δίκτυο. Χρησιμοποιώντας το πακέτο *munin-node*, ο *server02* θα ρυθμιστεί έτσι ώστε να αποστέλλει πληροφορίες στον *server01*.

Ελπίζουμε ότι αυτά τα απλά παραδείγματα θα σας επιτρέψουν να παρακολουθείτε διάφορους εξυπηρετητές και υπηρεσίες στο δίκτυό σας.

2. Nagios

2.1. Εγκατάσταση

Καταρχάς, εγκαταστήστε το πακέτο `nagios` στον `server01`. Εισάγετε σε τερματικό:

```
sudo apt-get install nagios3 nagios-nrpe-plugin
```

Θα σας ζητηθεί να εισάγετε κωδικό για τον χρήστη `nagiosadmin`. Τα στοιχεία του χρήστη αποθηκεύονται στο `/etc/nagios3/htpasswd.users`. Για να αλλάξετε τον κωδικό του `nagiosadmin` ή για να προσθέσετε νέους χρήστες στα σενάρια Nagios CGI, χρησιμοποιήστε το `htpasswd` από το πακέτο `apache2-utils`.

Π.χ., για να αλλάξετε τον κωδικό του χρήστη `nagiosadmin` εισάγετε:

```
sudo htpasswd /etc/nagios3/htpasswd.users nagiosadmin
```

Για να προσθέσετε χρήστη εισάγετε:

```
sudo htpasswd /etc/nagios3/htpasswd.users steve
```

Στη συνέχεια, εγκαταστήστε το πακέτο `nagios-nrpe-server` στον `server02`. Από τον `server02` εισάγετε σε τερματικό:

```
sudo apt-get install nagios-nrpe-server
```



Το NRPE σας επιτρέπει να εκτελείτε τοπικούς ελέγχους σε απομακρυσμένους `host`. Αυτό μπορείτε να το κάνετε και μέσω άλλων προσθέτων του Nagios ή χρησιμοποιώντας άλλους ελέγχους.

2.2. Συνοπτική περιγραφή ρυθμίσεων

Τα αρχεία ρυθμίσεων και ελέγχου του Nagios περιέχονται σε ορισμένους καταλόγους.

- `/etc/nagios3`: περιέχει αρχεία ρυθμίσεων για τη λειτουργία της υπηρεσίας, των αρχείων CGI, των `host nagios`, κτλ.
- `/etc/nagios-plugins`: περιέχει αρχεία ρυθμίσεων για τους ελέγχους υπηρεσιών.
- `/etc/nagios`: περιέχει τα αρχεία ρυθμίσεων του `nagios-nrpe-server` στον απομακρυσμένο `host`.
- `/usr/lib/nagios/plugins/`: εδώ αποθηκεύονται τα εκτελέσιμα αρχεία των ελέγχων. Για να ενημερωθείτε για τις επιλογές ενός ελέγχου χρησιμοποιήστε την επιλογή `-h`.

Π.χ.: `/usr/lib/nagios/plugins/check_dhcp -h`

Πληθώρα ελέγχων του Nagios μπορούν να ρυθμιστούν ώστε να εκτελούνται για οποιοδήποτε δοσμένο υπολογιστή. Στο παράδειγμα το Nagios θα ρυθμιστεί ώστε να ελέγχει το διαθέσιμο χώρο στο δίσκο, το DNS και μία ομάδα host MySQL. Ο έλεγχος του DNS θα γίνει στον *server02*, ενώ η ομάδα MySQL θα συμπεριλαμβάνει τόσο τον *server01* όσο και τον *server02*.



Δείτε το *Τμήμα 1, “HTTPD - Apache2 Διακομιστής Ιστού” [200]* για λεπτομέρειες σχετικά με τη ρύθμιση του Apache, το *Κεφάλαιο 8, Υπηρεσία ονομάτων τομέα (DNS) [145]* για το DNS και το *Τμήμα 1, “MySQL” [222]* για τη MySQL.

Επιπλέον, υπάρχουν κάποιοι όροι των οποίων η κατανόηση θα έπρεπε να διευκολύνει τη ρύθμιση του Nagios:

- *Host*: εξυπηρετητής, σταθμός εργασίας, συσκευή δικτύου, κτλ. που παρακολουθείται.
- *Ομάδα host*: μια ομάδα παρεμφερών host. Π.χ. μια ομάδα που θα περιλαμβάνει όλους τους εξυπηρετητές ιστού, τους εξυπηρετητές αρχείων, κτλ.
- *Υπηρεσία*: η παρακολουθούμενη υπηρεσία στον host. Π.χ. HTTP, DNS, NFS, κτλ.
- *Ομάδα υπηρεσιών*: σας επιτρέπει να ομαδοποιείτε πολλαπλές υπηρεσίες. Χρησιμεύει π.χ. στην ομαδοποίηση πολλαπλών HTTP.
- *Επαφή*: άτομο που λαμβάνει κοινοποίηση όταν συμβαίνει κάτι. Το Nagios μπορεί να ρυθμιστεί έτσι ώστε να αποστέλλει email, μηνύματα SMS, κτλ.

Από προεπιλογή το Nagios ελέγχει το HTTP, το χώρο στο δίσκο, το SSH, και τους τρέχοντες χρήστες, διεργασίες, και φόρτο του *τοπικού host*. Επίσης, το Nagios εκτελεί έλεγχο ring της *πύλης (gateway)*.

Η ρύθμιση μεγάλων εγκαταστάσεων Nagios μπορεί να αποβεί αρκετά πολύπλοκη. Συνήθως, είναι καλύτερο να ξεκινάτε με έναν ή δύο υπολογιστές, να τους ρυθμίζετε όπως επιθυμείτε, και στη συνέχεια να επεκτείνετε περαιτέρω.

2.3. Ρυθμίσεις

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
```



Στο παραπάνω και στα παρακάτω παραδείγματα, αντικαταστήστε τα *"server01"*, *"server02"*, *172.18.100.100* και *172.18.100.101* με τα ονόματα και τις διευθύνσεις IP των δικών σας εξυπηρετητών.

2. Στη συνέχεια, τροποποιήστε το */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. Επανεκκινήστε την υπηρεσία `nagios` για να ενεργοποιήσετε τις νέες ρυθμίσεις:

`sudo service nagios3 restart`

- 1. Τώρα, προσθέστε έναν ορισμό υπηρεσίας για τον έλεγχο MySQL, προσθέτοντας τα ακόλουθα στο `/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. Ο έλεγχος του Nagios θα πρέπει να πιστοποιηθεί στην MySQL. Για να προσθέσετε έναν χρήστη *nagios* στην MySQL εισάγετε:

`mysql -u root -p -e "create user nagios identified by 'secret';"`



Ο χρήστης *nagios* θα προστεθεί σε όλους τους host της ομάδας *mysql-servers*.

4. Επανεκκινήστε το `nagios` για να αρχίσετε να ελέγχετε τους εξυπηρετητές MySQL.

sudo service nagios3 restart

- 1. Τέλος, ρυθμίστε το NRPE έτσι ώστε να ελέγχει το χώρο στο δίσκο του *server02*.

Στον *server01* προσθέστε τον έλεγχο υπηρεσίας στο `/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. Τώρα, στον *server02*, τροποποιήστε το `/etc/nagios/nrpe.cfg` κάνοντας τις παρακάτω αλλαγές:

```
allowed_hosts=172.18.100.100
```

Και από κάτω, στην περιοχή ορισμών εντολών, προσθέστε:

```
command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -e
```

- 3. Τέλος, επανεκκινήστε το `nagios-nrpe-server`:

sudo service nagios-nrpe-server restart

- 4. Επίσης, στον *server01*, επανεκκινήστε το `nagios`:

sudo service nagios3 restart

Τώρα θα πρέπει να μπορείτε να βλέπετε τους ελέγχους host και υπηρεσιών στα αρχεία Nagios CGI. Για να αποκτήσετε πρόσβαση, πηγαίνετε στη σελίδα `http://server01/nagios3` από τον περιηγητή σας. Θα σας ζητηθεί το όνομα και ο κωδικός χρήστη του *nagiosadmin*.

2.4. Αναφορές

Αυτή η ενότητα δεν άγγιξε παρά μόνο επιφανειακά τα διάφορα χαρακτηριστικά του Nagios. Τα πακέτα `nagios-plugins-extra` και `nagios-snmp-plugins` περιέχουν πολλούς περισσότερους ελέγχους υπηρεσιών.

- Για περισσότερες πληροφορίες ανατρέξτε στον ιστότοπο του *Nagios*¹.
- Και συγκεκριμένα, στον ιστότοπο *Online Τεκμηρίωση*².
- Επίσης, υπάρχει ένας κατάλογος με *βιβλία*³ για το Nagios και την παρακολούθηση δικτύου:

¹ <http://www.nagios.org/>

² http://nagios.sourceforge.net/docs/3_0/

³ <http://www.nagios.org/propaganda/books/>

- The *Nagios Ubuntu Wiki*⁴ page also has more details.

⁴ <https://help.ubuntu.com/community/Nagios>

3. Munin

3.1. Εγκατάσταση

Πριν εγκαταστήσετε το Munin στον *server01*, θα πρέπει να εγκαταστήσετε το *apache2*. Οι προεπιλεγμένες ρυθμίσεις επαρκούν για τη λειτουργία ενός εξυπηρετητή munin. Για περισσότερες πληροφορίες δείτε το *Τμήμα 1, “HTTPD - Apache2 Διακομιστής Ιστού” [200]*.

Καταρχάς, εγκαταστήστε το πακέτο munin στον *server01*. Εισάγετε σε τερματικό:

```
sudo apt-get install munin
```

Τώρα, στον *server02* εγκαταστήστε το πακέτο munin-node:

```
sudo apt-get install munin-node
```

3.2. Ρυθμίσεις

Στον *server01* τροποποιήστε το */etc/munin/munin.conf*, προσθέτοντας τη διεύθυνση IP του *server02*:

```
## First our "normal" host.
[server02]
    address 172.18.100.101
```



Αντικαταστήστε τα *server02* και *172.18.100.101* με το όνομα και τη διεύθυνση IP του δικού σας εξυπηρετητή.

Στη συνέχεια, ρυθμίστε το munin-node στον *server02*. Τροποποιήστε το */etc/munin/munin-node.conf* για να επιτρέψετε την πρόσβαση του *server01*:

```
allow ^172\.\18\.\100\.\100$
```



Αντικαταστήστε το *^172\.\18\.\100\.\100\$* με τη διεύθυνση IP του δικού σας εξυπηρετητή munin.

Τώρα, επανεκκινήστε το munin-node στον *server02* για να ενεργοποιήσετε τις αλλαγές:

```
sudo service munin-node restart
```

Τέλος, από τον περιηγητή σας πηγαίνετε στο *http://server01/munin*. Θα πρέπει να μπορείτε να δείτε συνδέσμους προς κομψά γραφήματα με πληροφορίες των βασικών *προσθέτων του munin* για το δίσκο, το δίκτυο, τις διεργασίες και το σύστημα.



Εφόσον πρόκειται για νέα εγκατάσταση, ίσως χρειαστεί λίγος χρόνος μέχρι να εμφανιστούν κάποιες χρήσιμες πληροφορίες στα γραφήματα.

3.3. Επιπλέον πρόσθετα

Το πακέτο `munin-plugins-extra` περιλαμβάνει ελέγχους απόδοσης για επιπλέον υπηρεσίες. Π.χ., DNS, DHCP, Samba, κτλ. Για να εγκαταστήσετε το πακέτο, εισάγετε από το τερματικό:

```
sudo apt-get install munin-plugins-extra
```

Θυμηθείτε να εγκαταστήσετε το πακέτο τόσο στον εξυπηρετητή όσο και στα κομβικά μηχανήματα (node).

3.4. Αναφορές

- Δείτε τον ιστότοπο του *Munin*⁵ για περισσότερες λεπτομέρειες.
- Συγκεκριμένα, η σελίδα με την *Τεκμηρίωση του Munin*⁶ περιλαμβάνει πληροφορίες σχετικά με επιπλέον πρόσθετα, τη συγγραφή προσθέτων, κτλ.
- Επίσης, κυκλοφορεί ένα βιβλίο της Open Source Press στα Γερμανικά: *Munin Graphisches Netzwerk- und System-Monitoring*⁷.
- Another resource is the *Munin Ubuntu Wiki*⁸ page.

⁵ <http://munin.projects.linpro.no/>

⁶ <http://munin.projects.linpro.no/wiki/Documentation>

⁷ https://www.opensourcepress.de/index.php?26&backPID=178&tt_products=152

⁸ <https://help.ubuntu.com/community/Munin>

Κεφάλαιο 11. Διακομιστές Ιστού

Ένας Διακομιστής Ιστού είναι το λογισμικό που είναι υπεύθυνο για την αποδοχή αιτημάτων HTTP από πελάτες, γνωστά και ως φυλλομετρητές Ιστού, και να στέλνουν απαντήσεις HTTP μαζί με προαιρετικά περιεχόμενα δεδομένων, τα οποία συνήθως είναι Ιστοσελίδες όπως αρχεία HTML και συνδεδεμένα αντικείμενα (εικόνες, κλπ.).

1. HTTPD - Apache2 Διακομιστής Ιστού

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 Mozilla.

Users enter a Uniform Resource Locator (URL) to point to a Web server by means of its Fully Qualified Domain Name (FQDN) and a path to the required resource. For example, to view the home page of the *Ubuntu Web site*¹ a user will enter only the FQDN:

www.ubuntu.com

To view the *community*² sub-page, a user will enter the FQDN followed by a path:

www.ubuntu.com/community

Το πιο κοινό πρωτόκολλο που χρησιμοποιείτε για τη μεταφορά ιστοσελίδων είναι το Πρωτόκολλο Μεταφοράς Υπερκειμένου (Hyper Text Transfer Protocol (HTTP)). Πρωτόκολλα όπως το HTTP πάνω από το Στρώμα Ασφαλούς Υποδοχής (Secure Sockets Layer (HTTPS)), και το Πρωτόκολλο Μεταφοράς Αρχείων (File Transfer Protocol (FTP)), ένα πρωτόκολλο για την αποστολή και λήψη αρχείων, υποστηρίζονται επίσης.

Οι Διακομιστές Ιστού Apache συχνά χρησιμοποιούνται σε συνδυασμό με τη μηχανή βάσης δεδομένων MySQL, τη γλώσσα σεναρίου Προεπεξεργαστή Υπερκειμένου (PHP), και άλλες δημοφιλείς γλώσσες σεναρίου όπως οι Python και Perl. Αυτή η σύνθεση ονομάζεται LAMP (Linux, Apache, MySQL and Perl/Python/PHP) και σχηματίζει μια ισχυρή και αυτοδύναμη πλατφόρμα για την ανάπτυξη εφαρμογών βασισμένες στον Ιστό.

1.1. Εγκατάσταση

Ο διακομιστής ιστού Apache2 είναι διαθέσιμος για Ubuntu Linux. Για να εγκαταστήσετε τον Apache2:

- Σε ένα τερματικό εντολών πληκτρολογήστε την ακόλουθη εντολή:

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

1.2. Ρυθμίσεις

Ο Apache2 ρυθμίζεται τοποθετώντας *οδηγίες* σε απλά αρχεία κειμένου διαμόρφωσης. Αυτές οι *οδηγίες* χωρίζονται μεταξύ των ακόλουθων φακέλων και καταλόγων:

¹ <http://www.ubuntu.com>

² <http://www.ubuntu.com/community>

- *apache2.conf*: το κύριο αρχείο διαμόρφωσης. Περιέχει ρυθμίσεις οι οποίες είναι *καθολικές* για το Apache2.
- *conf.d*: περιέχει αρχεία διαμόρφωσης τα οποία εφαρμόζονται *καθολικά* στο Apache2. Άλλα πακέτα που χρησιμοποιούν τον Apache2 για να εξυπηρετούν περιεχόμενο μπορεί να προσθέσουν αρχεία, ή συνδέσμους, σε αυτόν τον κατάλογο.
- *envvars*: αρχείο στο οποίο ορίζονται η μεταβλητές *περιβάλλοντος* του Apache2.
- *httpd.conf*: historically the main Apache2 configuration file, named after the httpd daemon. Now the file is typically empty, as most configuration options have been moved to the below referenced directories. The file can be used for *user specific* configuration options that globally effect Apache2.
- *mods-available*: αυτός ο κατάλογος περιέχει αρχεία διαμόρφωσης για να φορτώνει *επιλογές* και να τις τροποποιεί. Δεν θα έχουν όλες οι επιλογές συγκεκριμένα αρχεία διαμόρφωσης, όμως.
- *mods-enabled*: κρατάει *συνδέσμους* στα αρχεία του /etc/apache2/mods-available. Όταν ένα αρχείο διαμόρφωσης επιλογής συνδέεται θα ενεργοποιηθεί την επόμενη φορά που θα επανεκκινηθεί ο apache2.
- *ports.conf*: στεγάζει τις οδηγίες που προσδιορίζουν ποιες θύρες ακούει ο Apache2.
- *sites-available*: αυτός ο κατάλογος έχει αρχεία διαμόρφωσης για τους Εικονικούς Κόμβους του Apache2. Οι Εικονικοί Κόμβοι επιτρέπουν στον Apache2 να διαμορφώνεται για πολλαπλούς δικτυακούς τόπους που έχουν διαφορετικές ρυθμίσεις.
- *sites-enabled*: όπως το mods-enabled, το sites-enabled περιέχει συνδέσμους στον κατάλογο /etc/apache2/sites-available. Όμοια, όταν ένα αρχείο διαμόρφωσης στο sites-available συνδέεται, ο δικτυακός τόπος που ρυθμίζετε από αυτό θα ενεργοποιηθεί όταν ο Apache2 επανεκκινηθεί.

Επιπλέον, άλλα αρχεία διαμόρφωσης μπορούν να προστεθούν χρησιμοποιώντας τον κώδικα παραπομπής *Include*, και μπαλαντέρ μπορούν να χρησιμοποιηθούν για να προστεθούν πολλά αρχεία διαμόρφωσης. Οποιοσδήποτε κώδικας παραπομπής μπορεί να χρησιμοποιηθεί σε οποιοδήποτε από αυτά τα αρχεία διαμόρφωσης. Οι αλλαγές στο κύριο αρχείο διαμόρφωσης αναγνωρίζονται από τον Apache2 όταν ενεργοποιείται ή επανεκκινείται.

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. Βασικές Ρυθμίσεις

Αυτή η ενότητα εξηγεί τις ουσιώδεις παραμέτρους ρύθμισης του διακομιστή Apache2. Αναφερθείτε στο *Apache2 Documentation*³ για περισσότερες λεπτομέρειες.

³ <http://httpd.apache.org/docs/2.2/>

- Ο Apache2 αποστέλλεται με μία προεπιλεγμένη εικονική φιλική προς τον υπολογιστή ρύθμιση. Έχει ρυθμιστεί με ένα προεπιλεγμένο εικονικό κεντρικό υπολογιστή (χρησιμοποιώντας τον κώδικα παραπομπής *VirtualHost*) ο οποίος μπορεί να τροποποιηθεί ή να χρησιμοποιηθεί όπως είναι εάν έχετε ένα μόνο δικτυακό τόπο, ή να χρησιμοποιηθεί ως πρότυπο για επιπλέον εικονικούς κεντρικούς υπολογιστές εάν έχετε πολλαπλούς δικτυακούς τόπους. Εάν αφεθεί μόνος, ο προεπιλεγμένος κεντρικός υπολογιστής θα λειτουργήσει ως ο προεπιλεγμένος δικτυακός τόπος σας, ή ο δικτυακός τόπος που θα βλέπουν οι χρήστες εάν το URL που εισάγουν δεν ταιριάζει με τον κώδικα παραπομπής *ServerName* κανενός από τους δικτυακούς σας τόπους. Για να τροποποιήσετε τον προεπιλεγμένο εικονικό κεντρικό υπολογιστή, επεξεργαστείτε το αρχείο `/etc/apache2/sites-available/default`.



Οι κώδικες παραπομπής που ορίζονται για έναν εικονικό κεντρικό υπολογιστή απευθύνονται μόνο στον συγκεκριμένο εικονικό κεντρικό υπολογιστή. Εάν ένας κώδικας παραπομπής έχει οριστεί ως *server-wide* και δεν έχει οριστεί στα πλαίσια των ρυθμίσεων του εικονικού κεντρικού υπολογιστή, χρησιμοποιείτε η προεπιλεγμένη ρύθμιση. Για παράδειγμα, μπορείτε να ορίσετε μια διεύθυνση ηλεκτρονικού ταχυδρομείου *Webmaster* και να μην ορίσετε ατομικές διευθύνσεις για κάθε εικονικό κεντρικό υπολογιστή.

Εάν επιθυμείτε να ρυθμίσετε έναν καινούριο εικονικό κεντρικό υπολογιστή ή δικτυακό τόπο, αντιγράψτε αυτό το αρχείο στον ίδιο κατάλογο με όνομα που θα επιλέξετε. Για παράδειγμα:

```
sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/mynewsite
```

Επεξεργαστείτε το καινούριο αρχείο για να ρυθμίσετε τον καινούριο δικτυακό τόπο χρησιμοποιώντας κάποιους από τους κώδικες παραπομπής που περιγράφονται παρακάτω.

- Ο κώδικας παραπομπής *ServerAdmin* προσδιορίζει τη διεύθυνση ηλεκτρονικού ταχυδρομείου του διαχειριστή του διακομιστή. Η προεπιλεγμένη τιμή είναι `webmaster@localhost`. Αυτό θα πρέπει να αλλαχτεί σε μια ηλεκτρονική διεύθυνση ταχυδρομείου που θα παραδοθεί σε εσάς (εάν είστε ο διαχειριστής του διακομιστή). Εάν η ιστοσελίδα σας έχει πρόβλημα, ο Apache2 θα εμφανίσει ένα μήνυμα σφάλματος το οποίο θα περιλαμβάνει τη συγκεκριμένη διεύθυνση στην οποία θα αναφέρετε το πρόβλημα. Βρείτε το συγκεκριμένο κώδικα παραπομπής στο αρχείο ρύθμισης της ιστοσελίδας σας στο `/etc/apache2/sites-available`.
- Ο κώδικας παραπομπής *Listen* ορίζει τη θύρα, και προαιρετικά τη διεύθυνση IP, που θα πρέπει να ακούει ο Apache2. Εάν η διεύθυνση IP δεν έχει οριστεί, ο Apache2 θα ακούει όλες τις IP διευθύνσεις που έχουν εκχωρηθεί στη μηχανή στην οποία τρέχει. Η προεπιλεγμένη τιμή για τον κώδικα παραπομπής *Listen* είναι 80. Αλλάξτε το σε `127.0.0.1:80` ώστε ο Apache2 να ακούει μόνο τη διεπαφή *loopback* ώστε να μην είναι

διαθέσιμος το Διαδίκτυο, στο (για παράδειγμα) 81 για να μην αλλάξει τη θύρα την οποία ακούει, ή να την αφήσει όπως είναι για κανονική λειτουργία. Αυτός ο κώδικας παραπομπής μπορεί να βρεθεί και να αλλαχτεί στο δικό του αρχείου, `/etc/apache2/ports.conf`

- Ο κώδικας παραπομπής *ServerName* είναι προαιρετικός και ορίζει σε τι FQDN θα απαντάει η ιστοσελίδα σας. Ο προεπιλεγμένος εικονικός κεντρικός υπολογιστής δεν έχει κάποιον *ServerName* κώδικα παραπομπής ορισμένο, έτσι θα ανταποκριθεί σε όλες τις αιτήσεις που δεν ταιριάζουν με κάποιο κώδικα παραπομπής *ServerName* άλλου εικονικού κεντρικού υπολογιστή. Εάν έχετε μόλις αποκτήσει το όνομα τομέα `ubunturocks.com` και επιθυμείτε να το φιλοξενήσετε στον διακομιστή Ubuntu σας, η τιμή του κώδικα παραπομπής *ServerName* στο αρχείο ρύθμισης του εικονικού κεντρικού υπολογιστή πρέπει να είναι `ubunturocks.com`. Προσθέστε αυτόν τον κώδικα παραπομπής στο καινούριο αρχείο εικονικού κεντρικού υπολογιστή που δημιουργήσατε προηγουμένως (`/etc/apache2/sites-available/mynewsite`).

Μπορεί επίσης να θέλετε ο δικτυακός σας τόπος να ανταποκρίνεται στο `www.ubunturocks.com`, καθώς πολλοί χρήστες θα θεωρήσουν ότι το πρόθεμα `www` είναι απαραίτητο. Χρησιμοποιείτε τον κώδικα παραπομπής *ServerAlias* για αυτό. Μπορείτε επίσης να χρησιμοποιήσετε μπαλαντέρ στον κώδικα παραπομπής *ServerAlias*.

Για παράδειγμα, η ακόλουθη ρύθμιση θα προκαλέσει τον δικτυακό σας τόπο να ανταποκρίνεται σε κάθε αίτημα τομέα που τελειώνει σε `.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`, as specified in `/etc/apache2/sites-available/default`. If desired, change this value in your site's virtual host file, and remember to create that directory if necessary!

Ενεργοποιήστε το *VirtualHost* χρησιμοποιώντας τη λειτουργία `a2ensite` και επανεκκινήστε τον Apache2:

```
sudo a2ensite mynewsite
sudo service apache2 restart
```



Φροντίστε να αντικαταστήσετε το *mynewsite* με ένα πιο περιγραφικό όνομα για τον Εικονικό Κεντρικό Υπολογιστή. Μια μέθοδος είναι να το ονομάσετε το αρχείο όπως ο κώδικας παραπομπής *ServerName* του Εικονικού Κεντρικού Υπολογιστή.

Ομοίως, χρησιμοποιήστε τη λειτουργία `a2dissite` για να απενεργοποιήσετε δικτυακούς τόπους. Αυτό μπορεί να είναι χρήσιμο όταν λύνετε προβλήματα ρύθμισης με πολλαπλούς Εικονικούς Κεντρικούς Υπολογιστές:

```
sudo a2dissite mynewsite
```

sudo service apache2 restart

1.2.2. Αρχικές Ρυθμίσεις

Αυτή η ενότητα εξηγεί τη ρύθμιση των αρχικών ρυθμίσεων του Apache2. Για παράδειγμα, εάν προσθέσετε έναν εικονικό κεντρικό υπολογιστή, οι ρυθμίσεις που επεξεργάζεστε για τον εικονικό κεντρικό υπολογιστή υπερισχύουν για εκείνο τον εικονικό υπολογιστή. Για ένα κώδικα παραπομπής που δεν έχει οριστεί στις ρυθμίσεις του εικονικού υπολογιστή, χρησιμοποιείται η αρχική τιμή.

- Το *DirectoryIndex* είναι η προεπιλεγμένη σελίδα που εξυπηρετείται από έναν διακομιστή όταν ένας χρήστης ζητάει το ευρετήριο ενός καταλόγου προσδιορίζοντας μια κάθετο (/) στο τέλος του ονόματος του καταλόγου.

Για παράδειγμα, όταν ένας χρήστης ζητά τη σελίδα `http://www.example.com/this_directory/`, αυτός ή αυτή θα λάβει είτε τη σελίδα Ευρετηρίου Καταλόγου εάν υπάρχει, μια λίστα καταλόγου παραγμένη από το διακομιστή εάν δεν υπάρχει οι επιλογές του Ευρετηρίου έχουν προσδιοριστεί, ή μια σελίδα Άδεια Απορρίφθηκε εάν τίποτα από τα δύο δεν αληθεύει. Ο διακομιστής θα προσπαθήσει να βρει ένα από τα αρχεία που βρίσκονται στη λίστα του κώδικα παραπομπής *DirectoryIndex* και θα επιστρέψει το πρώτο που θα βρει. Εάν δε βρει κανέναν από αυτά τα αρχεία και εάν το *Options Indexes* έχει οριστεί για αυτόν τον κατάλογο, ο διακομιστής θα παράγει και θα επιστρέψει μια λίστα, σε μορφή HTML, των υποκαταλόγων και των αρχείων του καταλόγου. Η προεπιλεγμένη τιμή, που βρίσκεται στο `/etc/apache2/mods-available/dir.conf` είναι `"index.html index.cgi index.pl index.php index.xhtml index.htm"`. Έτσι, εάν ο Apache2 βρει ένα αρχείο σε έναν κατάλογο που έχει ζητηθεί και ταιριάζει με κάποιο από αυτά τα ονόματα, το πρώτο θα προβληθεί.

- 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.d/localized-error-pages` 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.d/other-vhosts-access-log`. 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).
- Μερικές ρυθμίσεις προσδιορίζονται ανά κατάλογο αντί ανά διακομιστή. Ο *Options* είναι ένας από εκείνους τους κώδικες παραπομπής. Μια στροφή καταλόγου περιλαμβάνεται σε ετικέτες στυλ XML, όπως:

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

Ο κώδικας παραπομπής *Options* μέσα σε μια στροφή Καταλόγου δέχεται μία ή περισσότερες από τις ακόλουθες τιμές (μεταξύ άλλων), χωρισμένες από κενά:

- **ExecCGI** - Επιτρέπει εκτέλεση σεναρίων CGI. Τα σενάρια CGI δεν εκτελούνται εάν αυτή η επιλογή δεν έχει επιλεγεί.



Τα περισσότερα αρχεία δεν πρέπει να εκτελούνται σαν σενάρια CGI. Αυτό θα ήταν πολύ επικίνδυνο. Τα σενάρια CGI θα πρέπει να κρατούνται σε έναν κατάλογο ξεχωριστά από και έξω από το DocumentRoot, και μόνο σε αυτόν τον κατάλογο πρέπει να οριστεί η επιλογή ExecCGI. Αυτή είναι η προεπιλογή, και η προεπιλεγμένη τοποθεσία των σεναρίων CGI είναι /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** - Επιτρέπει περιλήψεις διακομιστή, αλλά απενεργοποιεί τις εντολές *#exec* και *#include* σε σενάρια CGI.
- **Indexes** - Προβάλλει μια μορφοποιημένη λίστα των περιεχομένων του καταλόγου, εάν το *DirectoryIndex* (σαν το index.html) δεν υπάρχει στον ζητούμενο κατάλογο.



Για λόγους ασφαλείας, αυτό δεν θα πρέπει να οριστεί, και σίγουρα δε θα πρέπει να οριστεί στον κατάλογο DocumentRoot. Ενεργοποιήστε αυτή την επιλογή προσεκτικά ανά κατάλογο μόνο εάν είστε σίγουροι ότι θέλετε οι χρήστες να βλέπουν όλα τα περιεχόμενα του καταλόγου.

- **Multiview** - Υποστηρίζει πολλαπλές προβολές διαπραγματεύσιμου περιεχομένου, αυτή η επιλογή είναι απενεργοποιημένη από προεπιλογή για λόγους ασφαλείας. Δείτε το *Apache2 documentation on this option*⁵.
- **SymLinksIfOwnerMatch** - Ακολουθείστε μόνο σθμβολικούς συνδέσμους εάν το αρχείο ή ο κατάλογος στόχος έχει τον ίδιο ιδιοκτήτη με το σύνδεσμο.

1.2.3. Ρυθμίσεις httpd

Αυτή η ενότητα εξηγεί κάποιες βασικές ρυθμίσεις διαμόρφωσης του δαίμονα httpd.

LockFile - Ο κώδικας παραπομπής LockFile ορίζει το μονοπάτι του lockfile που χρησιμοποιείται όταν ο διακομιστής καταρτίζεται είτε με το USE_FCNTL_SERIALIZED_ACCEPT ή με το USE_FLOCK_SERIALIZED_AC. Πρέπει να είναι αποθηκευμένο στον τοπικό δίσκο. Πρέπει να μείνει στις προεπιλεγμένες τιμές εκτός εάν ο κατάλογος του ιστορικού βρίσκεται σε ένα διαμοιρασμένο NFS. Σε αυτή την περίπτωση, η

⁴ <https://help.ubuntu.com/community/ServerSideIncludes>

⁵ http://httpd.apache.org/docs/2.2/mod/mod_negotiation.html#multiviews

προεπιλεγμένη τιμή πρέπει να αλλάξει σε μια τοποθεσία του τοπικού δίσκου και σε έναν κατάλογο που είναι αναγνώσιμος μόνο από τη βάση.

PidFile - Ο κώδικας παραπομπής PidFile ορίζει το αρχείο στο οποίο ο διακομιστής καταγράφει την πρόοδο ID (pid). Αυτό το αρχείο θα πρέπει να είναι αναγνώσιμο από τη βάση. Στις περισσότερες περιπτώσεις, θα πρέπει να αφεθεί στις αρχικές τιμές.

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".



Εκτός εάν ξέρετε ακριβώς τι κάνετε, μην ορίσετε τον κώδικα παραπομπής User στη βάση. Χρησιμοποιώντας τη βάση ως User θα δημιουργήσει μεγάλες τρύπες ασφαλείας για τον διακομιστή Ιστού σας.

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".

1.2.4. Υπομονάδες Apache2

Ο Apache2 είναι ένας σπονδυλωτός διακομιστής. Αυτό σημαίνει ότι μόνο η πιο βασική λειτουργικότητα περιλαμβάνεται στον πυρήνα του διακομιστή. Επιπρόσθετα χαρακτηριστικά είναι διαθέσιμα μέσω υπομονάδων οι οποίες μπορούν να φορτωθούν στον Apache2. Από προεπιλογή, ένα βασικό σύνολο υπομονάδων περιλαμβάνεται στο διακομιστή κατά την σύνταξη. Εάν ο διακομιστής έχει συνταχθεί ώστε να χρησιμοποιεί υπομονάδες φορτωμένες δυναμικά, τότε οι υπομονάδες μπορούν να συνταχθούν ξεχωριστά, και να προστεθούν οποιαδήποτε στιγμή χρησιμοποιώντας τον κώδικα παραπομπής LoadModule. Αλλιώς, ο Apache2 πρέπει να ανασυνταχθεί ώστε να προσθέτει ή να αφαιρεί υπομονάδες.

Το Ubuntu συντάσσει τον Apache2 ώστε να επιτρέπει τη δυναμική φόρτωση υπομονάδων. Οι κώδικες παραπομπής διαμόρφωσης μπορούν να περιληφθούν υπό όρους υπό την παρουσία μιας συγκεκριμένης υπομονάδας περικλείοντάς τους σε ένα μπλοκ *<IfModule>*.

Μπορείτε να εγκαταστήσετε επιπρόσθετες υπομονάδες του Apache2 και να τις χρησιμοποιήσετε με τον διακομιστή Ιστού σας. Για παράδειγμα, τρέξτε την ακόλουθη εντολή από ένα τερματικό εντολών για να εγκαταστήσετε την υπομονάδα *MySQL Authentication*:

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

Δείτε τον κατάλογο `/etc/apache2/mods-available` για επιπλέον υπομονάδες.

Χρησιμοποιείτε τη λειτουργία `a2enmod` για να ενεργοποιήσετε μια υπομονάδα:

```
a2enmod
sudo service apache2 restart
```

Ομοίως, a2dismod θα απενεργοποιήσει μια υπομονάδα:

```
sudo a2dismod auth_mysql
sudo service apache2 restart
```

1.3. Διαμόρφωση HTTPS

Η υπομονάδα mod_ssl προσθέτει ένα σημαντικό χαρακτηριστικό στο διακομιστή Apache2 - την ικανότητα να κρυπτογραφεί επικοινωνίες. Έτσι, όταν ο φυλλομετρητής σας επικοινωνεί χρησιμοποιώντας SSL, το πρόθεμα https:// χρησιμοποιείται στην αρχή του URL στην μπάρα πλοήγησης του φυλλομετρητή.

Η υπομονάδα mod_ssl είναι διαθέσιμη στο πακέτο apache2-common. Εκτελέστε την ακόλουθη εντολή από ένα τερματικό εντολών για να ενεργοποιήσετε την υπομονάδα mod_ssl:

```
sudo a2enmod ssl
```

Υπάρχει ένα προεπιλεγμένο αρχείο διαμόρφωσης HTTPS στο /etc/apache2/sites-available/default-ssl. Για να παρέχει ο Apache2 HTTPS, χρειάζονται επίσης ένα *πιστοποιητικό* και ένα αρχείο *κλειδί*. Η προεπιλεγμένη διαμόρφωση HTTPS θα χρησιμοποιήσει ένα πιστοποιητικό και ένα κλειδί που θα παραχθούν από το πακέτο ssl-cert. Είναι καλά για δοκιμή, αλλά το πιστοποιητικό και το κλειδί που παράχθηκαν αυτόματα πρέπει να αντικατασταθούν από ένα πιστοποιητικό συγκεκριμένο για τον δικτυακό τόπο ή το διακομιστή. Για πληροφορίες στο πως να παράγετε ένα κλειδί και να αποκτήσετε ένα πιστοποιητικό δείτε *Τμήμα 5, “Πιστοποιητικά” [181]*

Για να διαμορφώσετε τον Apache2 για HTTPS, πληκτρολογήστε το ακόλουθο:

```
sudo a2ensite default-ssl
```



Οι κατάλογοι /etc/ssl/certs και /etc/ssl/private είναι οι προεπιλεγμένες τοποθεσίες. Εάν εγκαταστήσετε το πιστοποιητικό και το κλειδί σε άλλο κατάλογο βεβαιωθείτε να αλλάξετε τα SSLCertificateFile και SSLCertificateKeyFile κατάλληλα.

Με τον Apache2 τώρα διαμορφωμένο για HTTPS, επανεκκινήστε την υπηρεσία για να ενεργοποιηθούν οι ρυθμίσεις:

```
sudo service apache2 restart
```



Ανάλογα με τον πως αποκτήσατε το πιστοποιητικό σας ίσως χρειαστεί να εισάγετε ένα συνθηματικό όταν εκκινηθεί ο Apache2.

Μπορείτε να εισέλθετε στις ασφαλείς σελίδες του διακομιστή πληκτρολογώντας `https://your_hostname/url/` στην μπάρα διεύθυνσης του φυλλομετρητή σας.

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` to the group "webmasters".

```
sudo chgrp -R webmasters /var/www
sudo find /var/www -type d -exec chmod g=rwx {} \;
sudo find /var/www -type f -exec chmod g=rws {} \;
```



If access must be granted to more than one group per directory, enable Access Control Lists (ACLs).

1.5. Αναφορές

- Το *Apache2 Documentation*⁶ περιέχει πληροφορίες σε βάθος για τους κώδικες παραπομπής διαμόρφωσης του Apache2. Επίσης, δείτε το πακέτο `apache2-doc` για τα επίσημα αρχεία του Apache2.
- Δείτε την ιστοσελίδα *Mod SSL Documentation*⁷ για περισσότερες πληροφορίες σχετικές με SSL.
- Το *Apache Cookbook*⁸ του O'Reilly είναι ένα καλό μέσο για να πετύχετε συγκεκριμένες διαμορφώσεις για το Apache2.
- Για συγκεκριμένες ερωτήσεις για τον Apache2 για Ubuntu, ρωτήστε στο κανάλι IRC `#ubuntu-server` στο `freenode.net`⁹.
- Συνήθως ενσωματωμένη με την PHP και τη MySQL η σελίδα *Apache MySQL PHP Ubuntu Wiki*¹⁰ είναι μια καλή πηγή.

⁶ <http://httpd.apache.org/docs/2.2/>

⁷ <http://www.modssl.org/docs/>

⁸ <http://oreilly.com/catalog/9780596001919/>

⁹ <http://freenode.net/>

¹⁰ <https://help.ubuntu.com/community/ApacheMySQLPHP>

2. PHP5 - Γλώσσα Σεναρίου

Η PHP είναι μια γλώσσα σεναρίου γενικού σκοπού κατάλληλη για ανάπτυξη Ιστού. Το σενάριο PHP μπορεί να ενσωματωθεί στην HTML. Αυτή η ενότητα εξηγεί πως να εγκαταστήσετε και να διαμορφώσετε την PHP5 σε Σύστημα Ubuntu με τον Apache και την MySQL.

Αυτή η ενότητα υποθέτει πως έχει εγκαταστήσει και διαμορφώσει τον Διακομιστή Ιστού Apache2 και τον Διακομιστή Βάσεως δεδομένων MySQL. Μπορείτε να αναφερθείτε στα τμήματα Apache2 και MySQL σε αυτό το αρχείο για να εγκαταστήσετε και να διαμορφώσετε τον Apache2 και το MySQL αντίστοιχα.

2.1. Εγκατάσταση

The PHP5 is available in Ubuntu Linux. Unlike python and perl, which are installed in the base system, PHP must be added.

- Για να εγκαταστήσετε την PHP5 μπορείτε να πληκτρολογήσετε την ακόλουθη εντολή στο τερματικό εντολών:

```
sudo apt-get install php5 libapache2-mod-php5
```

Μπορείτε να εκτελέσετε PHP5 σενάρια από τη γραμμή εντολών. Για να εκτελέσετε σενάρια PHP5 από τη γραμμή εντολών πρέπει να εγκαταστήσετε το πακέτο php5-cli. Για να το εγκαταστήσετε το php5-cli μπορείτε να πληκτρολογήσετε την ακόλουθη εντολή στο τερματικό εντολών:

```
sudo apt-get install php5-cli
```

Μπορείτε επίσης να εκτελέσετε σενάρια PHP5 χωρίς να εγκαταστήσετε την υπομονάδα PHP5 του Apache. Για να το πετύχετε αυτό, πρέπει να εγκαταστήσετε το πακέτο php5-cgi. Μπορείτε να εκτελέσετε την ακόλουθη εντολή στο τερματικό εντολών για να εγκαταστήσετε το πακέτο php5-cgi:

```
sudo apt-get install php5-cgi
```

Για να χρησιμοποιήσετε MySQL με PHP5 πρέπει να εγκαταστήσετε το πακέτο php5-mysql. Για να εγκαταστήσετε το php5-mysql μπορείτε να πληκτρολογήσετε την ακόλουθη εντολή στο τερματικό εντολών:

```
sudo apt-get install php5-mysql
```

Ομοίως, για να χρησιμοποιήσετε PostgreSQL με PHP5 πρέπει να εγκαταστήσετε το πακέτο `php5-pgsql`. Για να εγκαταστήσετε το `php5-pgsql` μπορείτε να πληκτρολογήσετε την ακόλουθη εντολή στο τερματικό εντολών:

```
sudo apt-get install php5-pgsql
```

2.2. Ρυθμίσεις

Αφού εγκαταστήσετε την PHP5, μπορείτε να εκτελέσετε σενάρια PHP5 από τον φυλλομετρητή ιστού σας. Εάν έχετε εγκαταστήσει το πακέτο `php5-cli`, μπορείτε να εκτελέσετε σενάρια PHP5 από τη γραμμή εντολών.

Από προεπιλογή, ο διακομιστής Ιστού Apache2 είναι διαμορφωμένος να εκτελεί σενάρια PHP5. Με άλλα λόγια, η υπομονάδα PHP5 ενεργοποιείται στον διακομιστή Ιστού Apache2 αυτόματα όταν εγκαθιστάτε την υπομονάδα. Παρακαλώ επαληθεύστε εάν τα αρχεία `/etc/apache2/mods-enabled/php5.conf` και `/etc/apache2/mods-enabled/php5.load` υπάρχουν. Εάν δεν υπάρχουν, μπορείτε να ενεργοποιήσετε την υπομονάδα χρησιμοποιώντας την εντολή **a2enmod**.

Μόλις εγκαταστήσετε τα πακέτα που σχετίζονται με PHP5 και ενεργοποιήσετε την ενότητα PHP5 Apache 2, θα πρέπει να επανεκκινήσετε το διακομιστή διαδικτύου Apache2 για να τρέξει τα σενάρια PHP5. Μπορείτε να εκτελέσετε την ακόλουθη εντολή σε ένα τερματικό εντολών για να κάνετε επανεκκίνηση το διακομιστή διαδικτύου σας:

```
sudo service apache2 restart
```

2.3. Δοκιμή

για να επαληθεύσετε την εγκατάστασή σας, μπορείτε να εκτελέσετε το ακόλουθο σενάριο PHP5 `phpinfo`:

```
<?php
phpinfo();
?>
```

Μπορείτε να αποθηκεύσετε το περιεχόμενο σε ένα αρχείο `phpinfo.php` και να το τοποθετήσετε κάτω από τον κατάλογο **DocumentRoot** του διακομιστή Ιστού Apache2. Όταν υποδείξετε στον φυλλομετρητή σας το `http://hostname/phpinfo.php`, θα εμφανίσει τιμές διαφόρων παραμέτρων διαμόρφωσης PHP5.

2.4. Αναφορές

- Για περισσότερες πληροφορίες σε βάθος δείτε τις βοηθητικές οδηγίες *php.net*¹¹.

¹¹ <http://www.php.net/docs.php>

- Υπάρχει μια πληθώρα βιβλίων για την PHP. Δύο καλά βιβλία από τον O'Reilly είναι τα *Learning PHP 5*¹² και *PHP Cook Book*¹³.
- Επίσης, δείτε τη σελίδα του wiki για *Apache MySQL PHP στο Ubuntu*¹⁴ για περισσότερες πληροφορίες.

¹² <http://oreilly.com/catalog/9780596005603/>

¹³ <http://oreilly.com/catalog/9781565926813/>

¹⁴ <https://help.ubuntu.com/community/ApacheMySQLPHP>

3. Squid - Διακομιστής Διαμεσολαβητή

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. Εγκατάσταση

Σε ένα τερματικό εντολών, πληκτρολογήστε την ακόλουθη εντολή για να εγκαταστήσετε το διακομιστή Squid:

```
sudo apt-get install squid3
```

3.2. Ρυθμίσεις

Squid is configured by editing the directives contained within the `/etc/squid3/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/squid3/squid.conf /etc/squid3/squid.conf.original  
sudo chmod a-w /etc/squid3/squid.conf.original
```

- Για να ορίσετε τον διακομιστή Squid να ακούει τη θύρα TCP 8888 αντί για την προεπιλεγμένη θύρα TCP 3128, αλλάξτε τον κώδικα παραπομπής `http_port`:

```
http_port 8888
```

- Αλλάξτε τον κώδικα παραπομπής `visible_hostname` ώστε να δώσετε στον διακομιστή Squid ένα συγκεκριμένο όνομα. Αυτό το όνομα κεντρικού υπολογιστή δεν πρέπει να είναι απαραίτητα το όνομα του κεντρικού υπολογιστή. Σε αυτό το παράδειγμα ορίζεται σε *weezie*

```
visible_hostname weezie
```

- Χρησιμοποιώντας τον έλεγχο πρόσβασης Squid, μπορείτε να διαμορφώσετε υπηρεσίες Διαδικτύου που έχουν διαμεσολαβητή το Squid ώστε να είναι διαθέσιμες μόνο σε χρήστες με συγκεκριμένες IP διευθύνσεις. Για παράδειγμα, θα επεξηγήσουμε την πρόσβαση από χρήστες του υποδικτύου 192.168.42.0/24 μόνο:

Add the following to the **bottom** of the ACL section of your `/etc/squid3/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/squid3/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/squid3/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/squid3/squid.conf` file:

```
http_access allow biz_network biz_hours
```



After making changes to the `/etc/squid3/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 service squid3 restart
```

3.3. Αναφορές

*Ιστοσελίδα Squid*¹⁵

*Σελίδα Ubuntu Wiki Squid*¹⁶.

¹⁵ <http://www.squid-cache.org/>

¹⁶ <https://help.ubuntu.com/community/Squid>

4. Ruby on Rails

Το Ruby on Rails είναι ένα πλαίσιο ιστού ανοιχτού κώδικα για την ανάπτυξη εφαρμογών ιστού με βάση δεδομένων. Είναι βελτιστοποιημένο για την ανεκτή παραγωγικότητα του προγραμματιστή καθώς επιτρέπει τον προγραμματιστή να γράψει κώδικα ευνοώντας τη συνήθεια αντί την διαμόρφωση.

4.1. Εγκατάσταση

Πριν εγκαταστήσετε το Rails θα πρέπει να εγκαταστήσετε τα Apache και MySQL. Για να εγκαταστήσετε το πακέτο Apache, παρακαλώ αναφερθείτε στο *Τμήμα 1, “HTTPD - Apache2 Διακομιστής Ιστού” [200]*. Για οδηγίες για το πως να εγκαταστήσετε το MySQL αναφερθείτε στο *Τμήμα 1, “MySQL” [222]*.

Αφού έχετε εγκαταστήσει τα πακέτα Apache και MySQL, είστε έτοιμοι να εγκαταστήσετε το πακέτο Ruby on Rails.

Για να εγκαταστήσετε τα βασικά πακέτα Ruby και το Ruby on Rails, μπορείτε να πληκτρολογήσετε την ακόλουθη εντολή σε ένα τερματικό εντολών:

```
sudo apt-get install rails
```

4.2. Ρυθμίσεις

τροποποιήστε το αρχείο διαμόρφωσης `/etc/apache2/sites-available/default` για να εγκαταστήσετε τον τομέα.

Το πρώτο πράγμα που πρέπει να αλλάξετε είναι ο κώδικας παραπομπής *DocumentRoot*:

```
DocumentRoot /path/to/rails/application/public
```

Μετά, αλλάξτε τον κώδικα παραπομπής `<Directory "/path/to/rails/application/public">` :

```
<Directory "/path/to/rails/application/public">
  Options Indexes FollowSymLinks MultiViews ExecCGI
  AllowOverride All
  Order allow,deny
  allow from all
  AddHandler cgi-script .cgi
</Directory>
```

Πρέπει επίσης να ενεργοποιήσετε την υπομονάδα `mod_rewrite` για τον Apache. Για να ενεργοποιήσετε την υπομονάδα `mod_rewrite`, παρακαλώ πληκτρολογήστε την ακόλουθη εντολή σε ένα τερματικό εντολών:

sudo a2enmod rewrite

Τέλος, θα χρειαστεί να αλλάξετε την κυριότητα των καταλόγων `/path/to/rails/application/public` και `/path/to/rails/application/tmp` στον χρήστη που χρησιμοποιείται για να εκτελεί τη διεργασία Apache:

sudo chown -R www-data:www-data /path/to/rails/application/public

sudo chown -R www-data:www-data /path/to/rails/application/tmp

Αυτό είναι! Τώρα έχετε το Διακομιστή σας έτοιμο για την εφαρμογή Ruby on Rails:

4.3. Αναφορές

- Δείτε την ιστοσελίδα *Ruby on Rails*¹⁷ για περισσότερες πληροφορίες.
- Επίσης το *Agile Development with Rails*¹⁸ είναι μια ένας καλός πόρος.
- Άλλη τοποθεσία για περισσότερες πληροφορίες είναι η σελίδα *Ruby on Rails Ubuntu Wiki*¹⁹.

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

Το Apache Tomcat είναι ένα δοχείο ιστού που σας επιτρέπει να εξυπηρετείται εφαρμογές ιστού Java Servlets και JSP (Java Server Pages)

The Tomcat 6.0 packages in Ubuntu support two different ways of running Tomcat. You can install them as a classic unique system-wide instance, that will be started at boot time will run as the tomcat6 unprivileged user. But you can also deploy private instances that will run with your own user rights, and that you should start and stop by yourself. This second way is particularly useful in a development server context where multiple users need to test on their own private Tomcat instances.

5.1. Εγκατάσταση για όλο το σύστημα

Για να εγκαταστήσετε το διακομιστή Tomcat, μπορείτε να εισάγετε την ακόλουθη εντολή στο τερματικό εντολών:

```
sudo apt-get install tomcat6
```

Αυτό θα εγκαταστήσει το διακομιστή Tomcat με μόνο μια εφαρμογή ιστού ROOT που προβάλει μια απλή σελίδα "Λειτουργεί" από προεπιλογή.

5.2. Ρυθμίσεις

Τα αρχεία διαμόρφωσης του Tomcat μπορούν να βρεθούν στο `/etc/tomcat6`. Μόνο λίγες κοινές αλλαγές διαμόρφωσης θα περιγραφούν εδώ, παρακαλώ δείτε το *Tomcat 6.0 documentation*²⁰ για περισσότερα.

5.2.1. Αλλαγή προεπιλεγμένων θυρών

Από προεπιλογή το Tomcat 6.0 τρέχει έναν συζευκτήρα HTTP στη θύρα 8080 και έναν συζευκτήρα AJP στη θύρα 8009. Ίσως θέλετε να αλλάξετε τις προεπιλεγμένες θύρες για να αποφύγετε σύγκρουση με έναν άλλο διακομιστή του συστήματος. Αυτό γίνεται αλλάζοντας τις ακόλουθες γραμμές στο `/etc/tomcat6/server.xml`:

```
<Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
...
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

5.2.2. Αλλαγή του JVM που χρησιμοποιείται

Από προεπιλογή το Tomcat θα τρέξει κατά προτίμηση με το OpenJDK-6, μετά θα δοκιμάσει το Sun's JVM, μετά θα δοκιμάσει κάποια άλλα JVMs. Εάν έχετε πολλαπλά

²⁰ <http://tomcat.apache.org/tomcat-6.0-doc/index.html>

JVMs εγκατεστημένα, μπορείτε να ορίσετε ποια θέλετε να χρησιμοποιηθούν ορίζοντας το `JAVA_HOME` στο `/etc/default/tomcat6`:

```
JAVA_HOME=/usr/lib/jvm/java-6-sun
```

5.2.3. Δήλωση χρηστών και ρόλων

Ονόματα χρηστών, κωδικοί και ρόλοι (Ομάδες) μπορούν να προσδιοριστούν κεντρικά σε ένα δοχείο Servlet. Στο Tomcat 6.0 αυτό γίνεται στο αρχείο `/etc/tomcat6/tomcat-users.xml`:

```
<role rolename="admin"/>
<user username="tomcat" password="s3cret" roles="admin"/>
```

5.3. Χρήση των πρότυπων εφαρμογών ιστού Tomcat

Το Tomcat αποστέλλεται με εφαρμογές ιστού που μπορείτε να εγκαταστήσετε για σκοπούς τεκμηρίωσης, διαχείρισης ή δοκιμαστικούς.

5.3.1. Τεκμηρίωση Tomcat

Το πακέτο `tomcat6-docs` περιέχει τις βοηθητικές οδηγίες του Tomcat 6.0, δομημένες σαν εφαρμογή ιστού στην οποία μπορείτε να έχετε πρόσβαση από προεπιλογή στο `http://yourserver:8080/docs`. Μπορείτε να το εγκαταστήσετε πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολών:

```
sudo apt-get install tomcat6-docs
```

5.3.2. Εφαρμογές ιστού διαχείρισης Tomcat

Το πακέτο `tomcat6-admin` περιέχει δύο εφαρμογές ιστού οι οποίες μπορούν να χρησιμοποιηθούν για να διαχειριστείτε το διακομιστή Tomcat χρησιμοποιώντας μια διεπαφή διαδικτύου. Μπορείτε να τις εγκαταστήσετε πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολών:

```
sudo apt-get install tomcat6-admin
```

Το πρώτο είναι η εφαρμογή ιστού *manager*, την οποία μπορείτε να βρείτε από προεπιλογή στο `http://yourserver:8080/manager/html`. Πρωτίστως χρησιμοποιείται για τη λήψη κατάστασης διακομιστή και για την επανεκκίνηση εφαρμογών ιστού.



Η πρόσβαση στην εφαρμογή *manager* προστατεύεται από προεπιλογή: πρέπει να ορίσετε έναν χρήστη με ρόλο "manager" στο `/etc/tomcat6/tomcat-users.xml` πριν μπορέσετε να αποκτήσετε πρόσβαση.

Η δεύτερη είναι η εφαρμογή ιστού *host-manager*, την οποία μπορείτε να βρείτε από προεπιλογή στο `http://yourserver:8080/host-manager/html`. Μπορεί να χρησιμοποιηθεί για να δημιουργήσετε εικονικούς κεντρικούς υπολογιστές δυναμικά.



Η πρόσβαση στην εφαρμογή *host-manager* προστατεύεται επίσης από προεπιλογή: πρέπει να ορίσετε έναν χρήστη με ρόλο "admin" στο `/etc/tomcat6/tomcat-users.xml` πριν μπορέσετε να αποκτήσετε πρόσβαση.

Για λόγους ασφαλείας, ο χρήστης `tomcat6` δεν μπορεί να επεξεργαστεί τον κατάλογο `/etc/tomcat6` από προεπιλογή. Μερικά χαρακτηριστικά σε αυτές τις εφαρμογές ιστού `admin` (ανάπτυξη εφαρμογής, δημιουργία εικονικού υπολογιστή) χρειάζονται άδεια επεξεργασίας για να έχουν πρόσβαση στον συγκεκριμένο κατάλογο. Εάν θέλετε να χρησιμοποιήσετε αυτά τα χαρακτηριστικά εκτελέστε το ακόλουθο, για να δώσετε στους χρήστες της ομάδας `tomcat6` τα κατάλληλα δικαιώματα:

```
sudo chgrp -R tomcat6 /etc/tomcat6
sudo chmod -R g+w /etc/tomcat6
```

5.3.3. Παραδείγματα εφαρμογών ιστού Tomcat

Το πακέτο `tomcat6-examples` περιλαμβάνει δύο εφαρμογές ιστού που μπορούν να χρησιμοποιηθούν για να ελεγχθούν ή να επιδείξουν Servlets και JSP χαρακτηριστικά, και που μπορείτε να τα βρείτε στο `http://yourserver:8080/examples`. Μπορείτε να τα εγκαταστήσετε πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολών:

```
sudo apt-get install tomcat6-examples
```

5.4. Χρήση ιδιωτικών στιγμιότυπων

Το Tomcat χρησιμοποιείται πολύ στην ανάπτυξη και τον έλεγχο σεναρίων όπου η χρησιμοποίηση ενός στιγμιότυπου για όλο το σύστημα δεν πληροί τις απαιτήσεις πολλών χρηστών σε ένα μόνο σύστημα. Τα πακέτα του Tomcat 6.0 στο Ubuntu έχουν εργαλεία για να σας βοηθήσουν να αναπτύξετε τα δικά σας στιγμιότυπα προσανατολισμένα στο χρήστη, επιτρέποντας σε κάθε χρήστη του συστήματος (χωρίς δικαιώματα βάσης) να εκτελούν ξεχωριστά ιδιωτικά στιγμιότυπα ενώ χρησιμοποιούν ακόμα τις βιβλιοθήκες συστήματος.



Είναι δυνατό να εκτελείτε το στιγμιότυπο για όλο το σύστημα παράλληλα με ιδιωτικά στιγμιότυπα, εφόσον δε χρησιμοποιούν τις ίδιες TCP πύλες.

5.4.1. Εγκατάσταση υποστήριξης ιδιωτικών στιγμιότυπων

Μπορείτε να εγκαταστήσετε οτιδήποτε απαραίτητο για να εκτελέσετε ιδιωτικά σενάρια πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολών:

```
sudo apt-get install tomcat6-user
```

5.4.2. Δημιουργία ιδιωτικού στιγμιότυπου

Μπορείτε να δημιουργήσετε έναν κατάλογο ιδιωτικών στιγμιότυπων πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολών:

tomcat6-instance-create my-instance

Αυτό θα δημιουργήσει έναν νέο κατάλογο `my-instance` με όλους τους απαραίτητους υποκαταλόγους και σενάρια. Μπορείτε για παράδειγμα να εγκαταστήσετε τις κοινές βιβλιοθήκες σας στον υποκατάλογο `lib/` και να αναπτύξετε τις εφαρμογές ιστού στον υποκατάλογο `webapps/`. Καμία εφαρμογή ιστού δεν αναπτύσσεται από προεπιλογή.

5.4.3. Ρύθμιση των ιδιωτικών στιγμιότυπών σας

Θα βρείτε τα κλασικά αρχεία διαμόρφωσης του Tomcat για τα ιδιωτικό στιγμιότυπό σας στον υποκατάλογο `conf/`. Θα πρέπει για παράδειγμα σίγουρα να επεξεργαστείτε το αρχείο `conf/server.xml` για να αλλάξετε τις προεπιλεγμένες θύρες που χρησιμοποιούνται από το ιδιωτικό στιγμιότυπο Tomcat για να αποφύγετε σύγκρουση με άλλα στιγμιότυπα που μπορεί να εκτελούνται.

5.4.4. Εκκίνηση/Τερματισμός του ιδιωτικού στιγμιότυπού σας

Μπορείτε να εκκινήσετε το ιδιωτικό σας στιγμιότυπο πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολών (υποθέτοντας ότι το στιγμιότυπό σας βρίσκεται στον κατάλογο `my-instance`):

my-instance/bin/startup.sh



Συστήνεται να κοιτάξετε τον υποκατάλογο `logs/` για σφάλματα. Εάν έχετε σφάλμα *java.net.BindException: Address already in use<null>:8080*, σημαίνει ότι η θύρα που χρησιμοποιείται είναι ήδη πιασμένη και ότι πρέπει να την αλλάξετε.

Μπορείτε να τερματίσετε το ιδιωτικό σας στιγμιότυπο πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολών (υποθέτοντας ότι το στιγμιότυπό σας βρίσκεται στον κατάλογο `my-instance`):

my-instance

5.5. Αναφορές

- Δείτε την ιστοσελίδα *Apache Tomcat*²¹ για περισσότερες πληροφορίες.
- το *Tomcat: The Definitive Guide*²² είναι ένας καλός πόρος για τη δημιουργία εφαρμογών ιστού με το Tomcat.
- Για επιπλέον βιβλία δείτε λίστα στη σελίδα *Tomcat Books*²³.
- Επίσης, δείτε τη σελίδα *Ubuntu Wiki Apache Tomcat*²⁴.

²¹ <http://tomcat.apache.org/>

²² <http://oreilly.com/catalog/9780596003180/>

²³ <http://wiki.apache.org/tomcat/Tomcat/Books>

²⁴ <https://help.ubuntu.com/community/ApacheTomcat5>

Κεφάλαιο 12. Βάσεις δεδομένων

Το Ubuntu παρέχει δύο δημοφιλείς εξυπηρετητές βάσεων δεδομένων. Είναι οι:

- MySQL™
- PostgreSQL

Είναι διαθέσιμοι στο κύριο αποθετήριο. Αυτή η ενότητα εξηγεί πώς να εγκαταστήσετε και να ρυθμίσετε αυτούς τους εξυπηρετητές βάσεων δεδομένων.

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. Εγκατάσταση

Για να εγκαταστήσετε το MySQL, εκτελέστε την ακόλουθη εντολή σε ένα τερματικό:

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



As of Ubuntu 12.04, MySQL 5.5 is installed by default. Whilst this is 100% compatible with MySQL 5.1 should you need to install 5.1 (for example to be a slave to other MySQL 5.1 servers) you can install the `mysql-server-5.1` package instead.

During the installation process you will be prompted to enter a password for the MySQL root user.

Μόλις η εγκατάσταση ολοκληρωθεί, ο εξυπηρετητής MySQL θα πρέπει να εκκινηθεί αυτόματα. Μπορείτε να εκτελέσετε την παρακάτω εντολή σε ένα τερματικό για να ελέγξετε εάν ο εξυπηρετητής MySQL εκτελείται: ````````````````````

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

Όταν εκτελείτε αυτή την εντολή, θα πρέπει να δείτε τις ακόλουθες γραμμές ή κάτι παρόμοιο:

```
tcp    0    0 localhost:mysql    *.*                LISTEN    2556/mysqld
```

Αν ο εξυπηρετητής δεν εκτελείται σωστά, μπορείτε να πληκτρολογήσετε την παρακάτω εντολή για να τον εκκινήσετε:

```
sudo service mysql restart
```

1.2. Ρυθμίσεις

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
```



Αντικαταστήστε το 192.168.0.5 με την κατάλληλη διεύθυνση.

After making a change to `/etc/mysql/my.cnf` the MySQL daemon will need to be restarted:

```
sudo service mysql restart
```

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

¹ <http://www.mysqlperformanceblog.com/2006/06/17/using-myisam-in-production/>

² <http://en.wikipedia.org/wiki/ACID>

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 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 service mysql stop
```

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:

³ <http://tools.percona.com/members/wizard>

```
sudo rm -rf /var/lib/mysql/*
sudo mysql_install_db
sudo chown -R mysql: /var/lib/mysql
sudo service mysql start
```

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-get 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.

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-get 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. Πόροι

- Δείτε την *Αρχική σελίδα του MySQL*⁴ για περισσότερες πληροφορίες.
- 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.
- The *Apache MySQL PHP Ubuntu Wiki*⁷ page also has useful information.

⁴ <http://www.mysql.com/>

⁵ <http://dev.mysql.com/doc/>

⁶ <http://www.informit.com/store/product.aspx?isbn=0768664128>

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. Εγκατάσταση

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

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

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

2.2. Ρυθμίσεις

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. PostgreSQL configuration files are stored in the `/etc/postgresql/<version>/main` directory. For example, if you install PostgreSQL 9.1, the configuration files are stored in the `/etc/postgresql/9.1/main` directory.



To configure *ident* authentication, add entries to the `/etc/postgresql/9.1/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/9.1/main/postgresql.conf`

Εντοπίστε τη γραμμή `#listen_addresses = 'localhost'` και αλλάξτε την σε:

```
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.

⁸ <http://www.postgresql.org/docs/9.1/static/admin.html>

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:

```
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 'ο_κωδικός_σας';
```

After configuring the password, edit the file `/etc/postgresql/9.1/main/pg_hba.conf` to use *MD5* authentication with the *postgres* user:

```
local all postgres md5
```

Τέλος, θα πρέπει να επανεκκινήσετε την υπηρεσία PostgreSQL για να αρχικοποιηθούν οι νέες ρυθμίσεις. Σε ένα τερματικό πληκτρολογήστε το παρακάτω για να επανεκκινήσετε την PostgreSQL:

```
sudo service postgresql restart
```



The above configuration is not complete by any means. Please refer *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-get install postgresql-client  
psql -h postgres.example.com -U postgres -W
```



Replace the domain name with your actual server domain name.

2.3. Αντίγραφα ασφαλείας

PostgreSQL databases should be backed up regularly. Refer to the *the PostgreSQL Administrator's Guide*¹⁰ for different approaches.

⁹ <http://www.postgresql.org/docs/9.1/static/admin.html>

¹⁰ <http://www.postgresql.org/docs/9.1/static/backup.html>

2.4. Πόροι

- As mentioned above the *the PostgreSQL Administrator's Guide*¹¹ is an excellent resource. The guide is also available in the postgresql-doc-9.1 package. Execute the following in a terminal to install the package:

```
sudo apt-get install postgresql-doc-9.1
```

To view the guide enter **file:///usr/share/doc/postgresql-doc-9.1/html/index.html** into the address bar of your browser.

- Για γενικές πληροφορίες σχετικά με την SQL δείτε το *Using SQL Special Edition*¹² από τον Rafe Colburn.
- Also, see the *PostgreSQL Ubuntu Wiki*¹³ page for more information.

¹¹ <http://www.postgresql.org/docs/9.1/static/admin.html>

¹² <http://www.informit.com/store/product.aspx?isbn=0768664128>

¹³ <https://help.ubuntu.com/community/PostgreSQL>

Κεφάλαιο 13. Εφαρμογές LAMP

1. Επισκόπηση

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:

- Σε ένα τερματικό εντολών πληκτρολογήστε την ακόλουθη εντολή:

```
sudo tasksel install lamp-server
```

After installing it you'll be able to install most *LAMP* applications in this way:

- Λήψη ενός αρχείου που περιέχει τα πηγαία αρχεία της εφαρμογής.
- Αποσυμπίεση του αρχείου, συνήθως σε έναν κατάλογο προσβάσιμο από κάποιον εξυπηρετητή ιστού.
- Depending on where the source was extracted, configure a web server to serve the files.
- Ρύθμιση της εφαρμογής για να συνδεθεί με τη βάση δεδομένων.
- Εκτέλεση κάποιου σεναρίου εντολών, ή περιήγηση σε κάποια σελίδα της εφαρμογής, για την εγκατάσταση της βάσης δεδομένων που χρειάζεται η εφαρμογή.
- Μόλις τα παραπάνω βήματα, ή παρόμοια βήματα, ολοκληρωθούν, θα είστε έτοιμοι να ξεκινήσετε να χρησιμοποιείτε την εφαρμογή.

Ένα μειονέκτημα αυτής της προσέγγισης είναι πως τα αρχεία της εφαρμογής δεν τοποθετούνται στο σύστημα αρχείων με κάποιον τυπικό τρόπο, πράγμα που μπορεί να προκαλέσει σύγχυση ως προς το πού έχει εγκατασταθεί η εφαρμογή. Ένα ακόμη μεγαλύτερο μειονέκτημα είναι η αναβάθμιση της εφαρμογής. Όταν μια νέα έκδοση κυκλοφορήσει, η ίδια διαδικασία που χρησιμοποιήθηκε για την εγκατάσταση της εφαρμογής θα χρειαστεί για να εφαρμοστούν οι ενημερώσεις.

Ευτυχώς, μια σειρά εφαρμογών *LAMP* είναι ήδη σε πακέτα για το Ubuntu και είναι διαθέσιμες για εγκατάσταση με τον ίδιο τρόπο όπως οι μη-LAMP εφαρμογές. Ωστόσο, ανάλογα την εφαρμογή, κάποια επιπλέον βήματα ρύθμισης και εγκατάστασης μπορεί να χρειαστούν.

This section covers how to install some *LAMP* applications.

2. Moin Moin

Το MoinMoin είναι μια μηχανή Wiki υλοποιημένη σε Python, βασισμένη στη μηχανή Wiki PikiPiki και υπό την άδεια GNU GPL.

2.1. Εγκατάσταση

Για να εγκαταστήσετε το MoinMoin, εκτελέστε την ακόλουθη εντολή στη γραμμή εντολών:

```
sudo apt-get install python-moinmoin
```

Θα πρέπει επίσης να εγκαταστήσετε τον εξυπηρετητή ιστού apache2. Για να εγκαταστήσετε τον εξυπηρετητή ιστού apache2, παρακαλούμε αναφερθείτε στην υπο-ενότητα *Τμήμα 1.1, Εγκατάσταση [200]* της ενότητας *Τμήμα 1, HTTPD - Apache2 Διακομιστής Ιστού [200]*.

2.2. Ρυθμίσεις

Για να ρυθμίσετε την πρώτη σας εφαρμογή Wiki, παρακαλούμε εκτελέστε το ακόλουθο σύνολο εντολών. Ας υποθέσουμε πως δημιουργείτε ένα Wiki με όνομα *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
```

Τώρα θα πρέπει να ρυθμίσετε το MoinMoin για να εντοπίσει το νέο σας Wiki: *mywiki*. Για να ρυθμίσετε το MoinMoin, ανοίξτε το αρχείο `/etc/moin/mywiki.py` και αλλάξτε την παρακάτω γραμμή:

```
data_dir = '/org/mywiki/data'
```

σε

```
data_dir = '/usr/share/moin/mywiki/data'
```

Επίσης, κάτω από την επιλογή *data_dir* προσθέστε το *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.



Αν έχετε ονομάσει το Wiki σας ως *my_wiki_name* θα πρέπει να προσθέσετε μια γραμμή `“("my_wiki_name", r".*")”` στο αρχείο `/etc/moin/farmconfig.py` μετά από τη γραμμή `“("mywiki", r".*")”`.

Μόλις ρυθμίσετε το MoinMoin για να εντοπίσει την πρώτη σας εφαρμογή Wiki *mywiki*, θα πρέπει να ρυθμίσετε το `apache2` και να το ετοιμάσετε για την εφαρμογή σας Wiki.

Θα πρέπει να προσθέσετε τις ακόλουθες γραμμές στο αρχείο `/etc/apache2/sites-available/default` μέσα στην κατηγορία `“<VirtualHost *>”`:

```
### moin
ScriptAlias /mywiki "/usr/share/moin/mywiki/moin.cgi"
alias /moin_static193 "/usr/share/moin/htdocs"
<Directory /usr/share/moin/htdocs>
Order allow,deny
allow from all
</Directory>
### end moin
```

Μόλις ρυθμίσετε τον εξυπηρετητή ιστού `apache2` και τον κάνετε διαθέσιμο για την εφαρμογή σας Wiki, θα πρέπει να τον επανεκκινήσετε. Μπορείτε να εκτελέσετε την ακόλουθη εντολή για να επανεκκινήσετε τον εξυπηρετητή ιστού `apache2`:

```
sudo service apache2 restart
```

2.3. Έλεγχος

Μπορείτε να ελέγξετε την εφαρμογή Wiki και να δείτε αν λειτουργεί πηγαίνοντας με το πρόγραμμα περιήγησής σας στο παρακάτω URL:

`http://localhost/mywiki`

Για περισσότερες πληροφορίες παρακαλούμε επισκεφθείτε τον ιστότοπο του *MoinMoin*¹.

2.4. Αναφορές

- Για περισσότερες πληροφορίες δείτε το *Wiki του moinmoin*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. MediaWiki

Το MediaWiki είναι λογισμικό Wiki, γραμμένο στη γλώσσα PHP. Μπορεί να χρησιμοποιήσει είτε το MySQL ή το PostgreSQL ως σύστημα διαχείρισης βάσεων δεδομένων.

3.1. Εγκατάσταση

Πριν εγκαταστήσετε το MediaWiki θα πρέπει επίσης να εγκαταστήσετε το Apache2, τη γλώσσα προγραμματισμού PHP5 και ένα σύστημα διαχείρισης βάσεων δεδομένων. Το MySQL ή το PostgreSQL είναι τα πιο κοινά· επιλέξτε ένα με βάση τις ανάγκες σας. Παρακαλούμε αναφερθείτε στις αντίστοιχες ενότητες σε αυτό το εγχειρίδιο για οδηγίες εγκατάστασης.

Για να εγκαταστήσετε το MediaWiki, εκτελέστε την ακόλουθη εντολή στη γραμμή εντολών:

```
sudo apt-get install mediawiki php5-gd
```

Για επιπλέον λειτουργίες του MediaWiki δείτε το πακέτο mediawiki-extensions.

3.2. Ρυθμίσεις

Το αρχείο ρύθμισης του Apache για το MediaWiki είναι εγκατεστημένο στον κατάλογο `/etc/apache2/conf.d/`. Θα πρέπει να αποσχολιάσετε την ακόλουθη γραμμή σε αυτό το αρχείο για να αποκτήσετε πρόσβαση στην εφαρμογή MediaWiki.

```
# Alias /mediawiki /var/lib/mediawiki
```

Αφού αποσχολιάσετε την παραπάνω γραμμή, επανεκκινήστε τον εξυπηρετητή Apache και αποκτήστε πρόσβαση στο MediaWiki με το παρακάτω url:

```
http://localhost/mediawiki/config/index.php
```



Παρακαλούμε διαβάστε την ενότητα `“Checking environment...”` σε αυτή τη σελίδα. Θα μπορείτε να διορθώνετε πολλά προβλήματα διαβάζοντας προσεκτικά αυτή την ενότητα.

Once the configuration is complete, you should copy the `LocalSettings.php` file to `/etc/mediawiki` directory:

```
sudo mv /var/lib/mediawiki/config/LocalSettings.php /etc/mediawiki/
```

You may also want to edit `/etc/mediawiki/LocalSettings.php` in order to set the memory limit (disabled by default):

```
ini_set( 'memory_limit', '64M' );
```

3.3. Επεκτάσεις

Οι επεκτάσεις προσθέτουν νέες λειτουργίες και βελτιώσεις στην εφαρμογή MediaWiki. Οι επεκτάσεις δίνουν στους διαχειριστές και στους τελικούς χρήστες τη δυνατότητα να προσαρμόσουν το MediaWiki στις απαιτήσεις τους.

Μπορείτε να κάνετε λήψη επεκτάσεων του MediaWiki ως συμπιεσμένο αρχείο ή από το αποθετήριο Subversion. Θα πρέπει να τις αντιγράψετε στον κατάλογο `/var/lib/mediawiki/extensions`. Επίσης, θα πρέπει να προσθέσετε την ακόλουθη γραμμή στο τέλος του αρχείου `/etc/mediawiki/LocalSettings.php`.

```
require_once "$IP/extensions/ΌνομαΕπέκτασης/ΌνομαΕπέκτασης.php";
```

3.4. Αναφορές

- Για περισσότερες πληροφορίες, παρακαλούμε αναφερθείτε στον ιστότοπο του *MediaWiki*⁴
- Ο *Οδηγός του MediaWiki για διαχειριστές*⁵ περιέχει πλήθος πληροφοριών για νέους διαχειριστές MediaWiki.
- Also, the *Ubuntu Wiki MediaWiki*⁶ page is a good resource.

⁴ <http://www.mediawiki.org>

⁵ <http://www.packtpub.com/Mediawiki/book>

⁶ <https://help.ubuntu.com/community/MediaWiki>

4. phpMyAdmin

Το phpMyAdmin είναι μια εφαρμογή LAMP γραμμένη ειδικά για τη διαχείριση εξυπηρετητών MySQL. Γραμμένο σε PHP και προσβάσιμο μέσω ενός περιηγητή ιστοσελίδων, το phpMyAdmin προσφέρει ένα γραφικό περιβάλλον για εργασίες διαχείρισης βάσεων δεδομένων.

4.1. Εγκατάσταση

Πριν εγκαταστήσετε το phpMyAdmin θα χρειαστείτε πρόσβαση σε μια βάση δεδομένων MySQL είτε στον ίδιο υπολογιστή που είναι εγκατεστημένο το phpMyAdmin, ή σε έναν υπολογιστή προσβάσιμο μέσω δικτύου. Για περισσότερες πληροφορίες δείτε εδώ: *Τμήμα 1, “MySQL” [222]*. Σε ένα τερματικό πληκτρολογήστε:

```
sudo apt-get install phpmyadmin
```

Στο τερματικό επιλέξτε ποιος εξυπηρετητής ιστού θα ρυθμιστεί για το phpMyAdmin. Το υπόλοιπο αυτής της ενότητας θα χρησιμοποιεί το Apache2 για εξυπηρετητή ιστού.

Σε έναν περιηγητή πηγαίνετε στο *http://όνομα_εξυπηρετητή/phpmyadmin*, αντικαθιστώντας το *όνομα_εξυπηρετητή* με το πραγματικό όνομα του εξυπηρετητή. Στη σελίδα εισόδου, πληκτρολογήστε *root* για *όνομα χρήστη*, ή κάποιον άλλο χρήστη MySQL, αν έχετε κάνει κάποια ρύθμιση, και πληκτρολογήστε τον κωδικό πρόσβασης MySQL του χρήστη.

Μόλις συνδεθείτε, μπορείτε να επαναφέρετε τον κωδικό του *root*, αν χρειάζεται, να δημιουργήσετε χρήστες, να δημιουργήσετε/διαγράψετε βάσεις δεδομένων και πίνακες, κτλ.

4.2. Ρυθμίσεις

Τα αρχεία ρύθμισης του phpMyAdmin βρίσκονται στο */etc/phpmyadmin*. Το κύριο αρχείο ρυθμίσεων είναι το */etc/phpmyadmin/config.inc.php*. Αυτό το αρχείο περιέχει ρυθμίσεις που ισχύουν για ολόκληρο το phpMyAdmin.

Για να χρησιμοποιήσετε το phpMyAdmin για να διαχειριστείτε μια βάση δεδομένων MySQL που φιλοξενείται σε έναν άλλον εξυπηρετητή, ρυθμίστε τα ακόλουθα στο */etc/phpmyadmin/config.inc.php*:

```
$cfg['Servers'][$i]['host'] = 'db_server';
```



Αντικαταστήστε το *db_server* με το πραγματικό όνομα ή τη διεύθυνση IP του απομακρυσμένου εξυπηρετητή βάσεων δεδομένων. Επίσης, σιγουρευτείτε πως ο υπολογιστής που είναι εγκατεστημένο το phpMyAdmin έχει δικαιώματα πρόσβασης στην απομακρυσμένη βάση δεδομένων.

Μόλις το ρυθμίσετε, αποσυνδεθείτε από το phpMyAdmin και συνδεθείτε ξανά, και θα πρέπει να έχετε πρόσβαση στο νέο εξυπηρετητή.

Τα αρχεία `config.header.inc.php` και `config.footer.inc.php` χρησιμοποιούνται για την προσθήκη κεφαλίδας και υποσέλιδου HTML στο phpMyAdmin.

Ένα άλλο σημαντικό αρχείο ρυθμίσεων είναι το `/etc/phpmyadmin/apache.conf`, αυτό το αρχείο είναι συμβολικός σύνδεσμος στο `/etc/apache2/conf.d/phpmyadmin.conf` και χρησιμοποιείται για τη ρύθμιση του Apache2 ώστε να παρέχει το site του phpMyAdmin. Το αρχείο περιέχει οδηγίες για την φόρτωση της PHP, για δικαιώματα καταλόγων, κτλ. Για περισσότερες πληροφορίες σχετικά με τη ρύθμιση του Apache2 δείτε εδώ: *Τμήμα 1, “HTTPD - Apache2 Διακομιστής Ιστού” [200]*.

4.3. Αναφορές

- Η τεκμηρίωση του phpMyAdmin εγκαθίσταται μαζί με το πακέτο και μπορεί να βρεθεί από τον σύνδεσμο *Τεκμηρίωση του phpMyAdmin* (ένα ερωτηματικό με ένα πλαίσιο γύρω του), κάτω από το λογότυπο του phpMyAdmin. Η επίσημη τεκμηρίωση μπορεί επίσης να βρεθεί στον ιστότοπο του *phpMyAdmin*⁷.
- Επίσης, το *Mastering phpMyAdmin*⁸ είναι μια πολύ καλή πηγή.
- A third resource is the *phpMyAdmin Ubuntu Wiki*⁹ page.

⁷ http://www.phpmyadmin.net/home_page/docs.php

⁸ <http://www.packtpub.com/phpmyadmin-3rd-edition/book>

⁹ <https://help.ubuntu.com/community/phpMyAdmin>

5. WordPress

WordPress is a blog tool, publishing platform and CMS implemented in PHP and licensed under the GNU GPLv2.

5.1. Εγκατάσταση

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

```
sudo apt-get install wordpress
```

You should also install apache2 web server and mysql server. For installing apache2 web server, please refer to *Τμήμα 1.1, “Εγκατάσταση” [200]* sub-section in *Τμήμα 1, “HTTPD - Apache2 Διακομιστής Ιστού” [200]* section. For installing mysql server, please refer to *Τμήμα 1.1, “Εγκατάσταση” [222]* sub-section in *Τμήμα 1, “MySQL” [222]* section.

5.2. Ρυθμίσεις

For configuring your first WordPress application, configure an apache site. Open `/etc/apache2/sites-available/wordpress` and write the following lines:

```
Alias /blog /usr/share/wordpress
Alias /blog/wp-content /var/lib/wordpress/wp-content
<Directory /usr/share/wordpress>
    Options FollowSymLinks
    AllowOverride Limit Options FileInfo
    DirectoryIndex index.php
    Order allow,deny
    Allow from all
</Directory>
<Directory /var/lib/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 service apache2 restart

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', '/var/lib/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.

5.3. Αναφορές

- *WordPress.org Codex*¹⁰
- *Ubuntu Wiki WordPress*¹¹

¹⁰ <https://codex.wordpress.org/>

¹¹ <https://help.ubuntu.com/community/WordPress>

Κεφάλαιο 14. Εξυπηρετητές αρχείων

Αν έχετε περισσότερους από έναν υπολογιστές σε ένα δίκτυο. Κάποια στιγμή, πιθανώς θα χρειαστείτε να ανταλλάξετε αρχεία μεταξύ τους. Σε αυτή την ενότητα, καλύπτουμε την εγκατάσταση και τη ρύθμιση για FTP, NFS και CUPS.

1. Εξυπηρετητής FTP

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 *Κεφάλαιο 6, Απομακρυσμένη Διαχείριση [84]* 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.

Η πρόσβαση σε έναν εξυπηρετητή FTP μπορεί να επιτευχθεί με δύο τρόπους:

- Ανώνυμη
- Πιστοποιημένη

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 - Εγκατάσταση εξυπηρετητή FTP

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

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

1.2. Ρύθμιση ανώνυμου FTP

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
```

Αφού κάνετε την αλλαγή, επανεκκινήστε το `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. Ρύθμιση FTP με πιστοποίηση χρηστών

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
```

Τώρα επανεκκινήστε το `vsftpd`:

```
sudo restart vsftpd
```

Τώρα, όταν οι χρήστες του συστήματος συνδέονται στο FTP, θα ξεκινούν στους *αρχικούς καταλόγους* τους, όπου μπορούν να κάνουν λήψη, αποστολή, δημιουργία καταλόγων, κτλ.

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
```



Η ενεργοποίηση της ανώνυμης αποστολής FTP μπορεί να είναι ακραίος κίνδυνος ασφαλείας. Είναι καλύτερα να μην ενεργοποιήσετε την ανώνυμη αποστολή σε εξυπηρετητές στους οποίους είναι δυνατή η πρόσβαση απευθείας από το διαδίκτυο.

Το αρχείο ρυθμίσεων αποτελείται από πολλές παραμέτρους ρύθμισης. Οι πληροφορίες για κάθε παράμετρο είναι διαθέσιμες στο αρχείο ρυθμίσεων. Εναλλακτικά, μπορείτε να αναφερθείτε στη σελίδα `man` - **man 5 vsftpd.conf** - για λεπτομέρειες για κάθε παράμετρο.

1.4. Ασφάλιση του FTP

Υπάρχουν επιλογές στο `/etc/vsftpd.conf` που βοηθάνε στο να κάνετε το `vsftpd` πιο ασφαλές. Για παράδειγμα οι χρήστες μπορούν να περιοριστούν στους αρχικούς τους καταλόγους αν αποσχολιάσετε το:

```
chroot_local_user=YES
```

Μπορείτε επίσης να περιορίσετε μόνο μια συγκεκριμένη λίστα χρηστών στους αρχικούς τους καταλόγους:

```
chroot_list_enable=YES  
chroot_list_file=/etc/vsftpd.chroot_list
```

Αφού αποσχολιάσετε τις παραπάνω επιλογές, δημιουργήστε ένα αρχείο `/etc/vsftpd.chroot_list` που περιέχει μια λίστα χρηστών - έναν σε κάθε γραμμή. Μετά επανεκκινήστε το `vsftpd`:

sudo restart vsftpd

Επίσης το αρχείο `/etc/ftpusers` είναι μια λίστα χρηστών στους οποίους *δεν επιτρέπεται* η πρόσβαση FTP. Η προεπιλεγμένη λίστα περιέχει τους χρήστες `root`, `daemon`, `nobody`, κτλ. Για να απενεργοποιήσετε την πρόσβαση FTP σε επιπλέον χρήστες, απλά προσθέστε τους στη λίστα.

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.

Για να ρυθμίσετε το *FTPS*, επεξεργαστείτε το αρχείο `/etc/vsftpd.conf` και στο τέλος του προσθέστε:

```
ssl_enable=Yes
```

Επίσης, παρατηρήστε τις επιλογές σχετικά με το πιστοποιητικό και το κλειδί:

```
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 *Τμήμα 5, “Πιστοποιητικά” [181]*.

Τώρα επανεκκινήστε το `vsftpd`, και οι μη-ανώνυμοι χρήστες θα είναι αναγκασμένοι να χρησιμοποιούν το *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: έγκυρα κελύφη εισόδου
/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
```

Αυτό είναι απαραίτητο επειδή, από προεπιλογή το `vsftpd` χρησιμοποιεί το PAM για πιστοποίηση και το αρχείο ρυθμίσεων `/etc/pam.d/vsftpd` περιέχει το παρακάτω:

```
auth required pam_shells.so
```

Το άρθρωμα PAM *shells* περιορίζει την πρόσβαση στα κελύφη που υπάρχουν στο αρχείο `/etc/shells`.

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. Αναφορές

- Δείτε τον *ιστότοπο του vsftpd*¹ για περισσότερες πληροφορίες.
- 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/raring/en/man5/vsftpd.conf.5.html>

2. Σύστημα Αρχείων Δικτύου (NFS)

Το NFS επιτρέπει σε ένα σύστημα να μοιραστεί καταλόγους και αρχεία με άλλαθ μέσω ενός δικτύου. Με τη χρήση του NFS, οι χρήστες και τα προγράμματα μπορούν να έχουν πρόσβαση σε αρχεία που βρίσκονται σε απομακρυσμένα συστήματα σχεδόν σα να ήταν τοπικά αρχεία.

Κάποια από τα πιο αξιοσημείωτα πλεονεκτήματα που προσφέρει το NFS είναι:

- Οι τοπικοί σταθμοί εργασίας χρησιμοποιούν λιγότερο χώρο στο δίσκο επειδή τα δεδομένα που χρησιμοποιούνται συχνά, μπορούν να αποθηκευτούν σε ένα μηχάνημα και να παραμείνουν ακόμη προσβάσιμα σε άλλους μέσω του δικτύου.
- Δεν χρειάζεται οι χρήστες να έχουν ξεχωριστούς αρχικούς καταλόγους σε κάθε μηχάνημα του δικτύου. Οι αρχικοί κατάλογοι μπορούν να τοποθετηθούν στον εξυπηρετητή NFS και να είναι διαθέσιμοι μέσω του δικτύου.
- Οι συσκευές αποθήκευσης όπως οι συσκευές δισκέτας, CDROM και USB μπορούν να χρησιμοποιηθούν από άλλα μηχανήματα στο δίκτυο. Αυτό μπορεί να μειώσει τον αριθμό των αφαιρούμενων συσκευών που υπάρχουν στο δίκτυο.

2.1. Εγκατάσταση

Σε ένα τερματικό πληκτρολογήστε την ακόλουθη εντολή για να εγκαταστήσετε τον εξυπηρετητή NFS:

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

2.2. Ρυθμίσεις

Μπορείτε να ρυθμίσετε τους καταλόγους που θα εξαχθούν προσθέτοντάς τους στο αρχείο `/etc/exports`. Για παράδειγμα:

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

Μπορείτε να αντικαταστήσετε το `*` με μια από τις μορφές ονόματος υπολογιστή. Κάντε την καταχώρηση του ονόματος υπολογιστή όσο πιο συγκεκριμένη γίνεται ώστε να μην είναι δυνατή η πρόσβαση του πόρου NFS από ανεπιθύμητα συστήματα.

Για να εκκινήσετε τον εξυπηρετητή NFS, μπορείτε να εκτελέσετε την παρακάτω εντολή σε ένα τερματικό:

```
sudo service nfs-kernel-server start
```

2.3. Ρύθμιση πελάτη NFS

Χρησιμοποιήστε την εντολή `mount` για να προσαρτήσετε έναν κοινόχρηστο κατάλογο NFS από ένα άλλο μηχάνημα, πληκτρολογώντας μια εντολή παρόμοια με την ακόλουθη σε ένα τερματικό:

```
sudo mount example.hostname.com:/ubuntu /local/ubuntu
```



Ο κατάλογος προσάρτησης `/local/ubuntu` πρέπει να υπάρχει. Δεν πρέπει να υπάρχουν αρχεία ή υποκατάλογοι στον κατάλογο `/local/ubuntu`.

Ένας εναλλακτικός τρόπος για να προσαρτήσετε έναν κοινόχρηστο κατάλογο από ένα άλλο μηχάνημα είναι να προσθέσετε μια γραμμή στο αρχείο `/etc/fstab`. Αυτή η γραμμή πρέπει να αναφέρει το όνομα του εξυπηρετητή NFS, τον κατάλογο στον εξυπηρετητή που εξάγεται και τον κατάλογο στο τοπικό μηχάνημα στον οποίο θα προσαρτηθεί ο κοινόχρηστος κατάλογος.

Η γενική σύνταξη για τη γραμμή στο αρχείο `/etc/fstab` είναι ως εξής:

```
example.hostname.com:/ubuntu /local/ubuntu nfs rsize=8192,wsiz=8192,timeo=14,intr
```

Αν έχετε πρόβλημα με την προσάρτηση ενός κοινόχρηστου καταλόγου NFS, σιγουρευτείτε πως το πακέτο `nfs-common` είναι εγκατεστημένο στον πελάτη σας. Για να εγκαταστήσετε το `nfs-common`, πληκτρολογήστε την ακόλουθη εντολή στο τερματικό:

```
sudo apt-get install nfs-common
```

2.4. Αναφορές

*Linux NFS faq*³

*Ubuntu Wiki NFS Howto*⁴

³ <http://nfs.sourceforge.net/>

⁴ <https://help.ubuntu.com/community/NFSv4Howto>

3. Αρχικοποιητής iSCSI

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-get 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:sl7b92030000520000-2
```



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. Αναφορές

*Open-iSCSI Website*⁵

*Debian Open-iSCSI page*⁶

⁵ <http://www.open-iscsi.org/>

⁶ <http://wiki.debian.org/SAN/iSCSI/open-iscsi>

4. CUPS - Εξυπηρετητής εκτυπώσεων

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. Εγκατάσταση

Για να εγκαταστήσετε το CUPS στον υπολογιστή σας, απλά χρησιμοποιήστε το `sudo` με την εντολή `apt-get` και δώστε τα πακέτα προς εγκατάσταση ως πρώτη παράμετρο. Μια ολοκληρωμένη εγκατάσταση CUPS έχει πολλές εξαρτήσεις πακέτων, αλλά μπορούν όλες να δοθούν στην ίδια εντολή. Πληκτρολογήστε το παρακάτω σε ένα τερματικό για να εγκαταστήσετε το CUPS:

```
sudo apt-get install cups
```

Μόλις πιστοποιηθείτε με τον κωδικό πρόσβασης του χρήστη σας, τα πακέτα θα πρέπει να ληφθούν και να εγκατασταθούν χωρίς σφάλματα. Μετά το πέρας της εγκατάστασης, ο εξυπηρετητής CUPS θα εκκινηθεί αυτόματα.

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. Ρυθμίσεις

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.



Πριν επεξεργαστείτε το αρχείο ρυθμίσεων, θα πρέπει να δημιουργήσετε ένα αντίγραφο του αρχικού αρχείου και να το προστατέψετε από εγγραφή, ώστε να

έχετε τις αρχικές ρυθμίσεις ως αναφορά και να τις επαναχρησιμοποιείτε όπως χρειάζεται.

Αντιγράψτε το αρχείο `/etc/cups/cupsd.conf` και προστατέψτε το από εγγραφή με τις παρακάτω εντολές, σε ένα τερματικό:

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

- **ServerAdmin:** Για να ρυθμίσετε την διεύθυνση email του καθορισμένου διαχειριστή του εξυπηρετητή CUPS, απλά επεξεργαστείτε το αρχείο ρυθμίσεων `/etc/cups/cupsd.conf` με τον επεξεργαστή κειμένου που προτιμάτε, και προσθέστε ή επεξεργαστείτε την γραμμή *ServerAdmin* αναλόγως. Για παράδειγμα, αν είσαστε εσείς ο διαχειριστής του εξυπηρετητή CUPS και η διεύθυνση e-mail σας είναι 'bjoy@somebigco.com', τότε θα τροποποιούσατε τη γραμμή *ServerAdmin* ως εξής:

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

- **Listen:** Από προεπιλογή στο Ubuntu, η εγκατάσταση του εξυπηρετητή CUPS αναμένει για συνδέσεις μόνο στην διεπαφή loopback στην διεύθυνση IP `127.0.0.1`. Για να κάνετε τον εξυπηρετητή CUPS να αναμένει για συνδέσεις σε μία διεύθυνση IP μιας πραγματικής δικτυακής συσκευής, πρέπει να ορίσετε είτε ένα όνομα, την διεύθυνση IP, ή προαιρετικά, ένα ζευγάρι διεύθυνσης IP/θύρας μέσω της προσθήκης μιας οδηγίας *Listen*. Για παράδειγμα, αν ο εξυπηρετητής σας CUPS βρίσκεται σε ένα τοπικό δίκτυο στην διεύθυνση IP `192.168.10.250` και θέλετε να τον κάνετε προσβάσιμο στα άλλα συστήματα σε αυτό το υποδίκτυο, μπορείτε να επεξεργαστείτε το `/etc/cups/cupsd.conf` και να προσθέσετε μια οδηγία *Listen*, όπως:

```
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)
```

Στο παραπάνω παράδειγμα, μπορείτε να σχολιάσετε ή να αφαιρέσετε την αναφορά στη διεύθυνση Loopback (`127.0.0.1`) αν δεν επιθυμείτε το cupsd να αναμένει για συνδέσεις σε αυτή την διεπαφή, αλλά θα προτιμούσατε να αναμένει μόνο στις διεπαφές Ethernet του τοπικού δικτύου (LAN). Για να ενεργοποιήσετε την αναμονή για συνδέσεις σε όλες τις δικτυακές διεπαφές για τις οποίες έχει δεσμευτεί ένα συγκεκριμένο όνομα, συμπεριλαμβανομένης της Loopback, μπορείτε να δημιουργήσετε μία καταχώρηση *Listen* για το όνομα *socrates* όπως:

```
Listen socrates:631 # Αναμονή για συνδέσεις σε όλες τις διεπαφές για το όνομα «socrates»
```

ή παραλείποντας την οδηγία *Listen* και χρησιμοποιώντας την *Port*, όπως:

Port 631 # Αναμονή για συνδέσεις στην θύρα 631 σε όλες τις διεπαφές

Για περισσότερα παραδείγματα οδηγιών ρύθμισης στο αρχείο ρυθμίσεων του εξυπηρετητή CUPS, δείτε την σχετική σελίδα εγχειριδίου του συστήματος πληκτρολογώντας την παρακάτω εντολή σε ένα τερματικό:

man cupsd.conf



Όποτε κάνετε αλλαγές στο αρχείο ρυθμίσεων `/etc/cups/cupsd.conf`, θα χρειάζεται να επανεκκινείτε τον εξυπηρετητή CUPS πληκτρολογώντας την ακόλουθη εντολή σε ένα τερματικό:

sudo service cups restart

4.3. Περιβάλλον ιστού



Το CUPS μπορεί να ρυθμίζεται και να παρακολουθείται μέσω ενός περιβάλλοντος ιστού, που από προεπιλογή είναι διαθέσιμο στο `http://localhost:631/admin`. Το περιβάλλον ιστού μπορεί να χρησιμοποιηθεί για να πραγματοποιούνται όλες οι εργασίες διαχείρισης του εκτυπωτή.

Για να πραγματοποιήσετε διαχειριστικές εργασίες μέσω του περιβάλλοντος ιστού, θα πρέπει είτε να έχετε τον λογαριασμό `root` ενεργοποιημένο στον εξυπηρετητή σας, ή να πιστοποιηθείτε ως κάποιος χρήστης της ομάδας `lpadmin`. Για λόγους ασφαλείας, το CUPS δεν θα πιστοποιήσει κάποιον χρήστη που δεν έχει κωδικό πρόσβασης.

Για να προσθέσετε έναν χρήστη στην ομάδα `lpadmin`, εκτελέστε στο τερματικό:

sudo usermod -aG lpadmin όνομα_χρήστη

Περαιτέρω τεκμηρίωση είναι διαθέσιμη στην καρτέλα *Τεκμηρίωση/Βοήθεια* του περιβάλλοντος ιστού.

4.4. Αναφορές

*Ιστότοπος του CUPS*⁷

*Debian Open-iSCSI page*⁸

⁷ <http://www.cups.org/>

⁸ <http://wiki.debian.org/SAN/iSCSI/open-iscsi>

Κεφάλαιο 15. Υπηρεσίες Ηλ. Αλληλογραφίας

Η διαδικασία διαβίβασης ενός email από ένα άτομο σε άλλο μέσω του Διαδικτύου ή άλλου δικτύου απαιτεί τη συνεργασία πολλών διαφορετικών συστημάτων. Καθένα από αυτά τα συστήματα θα πρέπει να έχει ρυθμιστεί κατάλληλα προκειμένου να λειτουργήσει σωστά η διαδικασία. Ο αποστολέας χρησιμοποιεί έναν *Mail User Agent* (Πράκτορα Χρήστη Αλληλογραφίας - MUA), ή πελάτη email, για την αποστολή του μηνύματος μέσω ενός ή περισσότερων *Mail Transfer Agents* (Πρακτόρων Μεταφοράς Αλληλογραφίας - MTA), ο τελευταίος των οποίων παραδίδει το μήνυμα στον *Mail Delivery Agent* (Πράκτορα Παράδοσης Αλληλογραφίας - MDA). Ο τελευταίος το παραδίδει στην ταχυδρομική θυρίδα του παραλήπτη, από όπου ανακτάται από τον πελάτη email του παραλήπτη, συνήθως μέσω εξυπηρετητή POP3 ή IMAP.

1. Postfix

Το Postfix είναι ο προεπιλεγμένος Mail Transfer Agent (MTA) του Ubuntu. Φιλοδοξεί να είναι γρήγορος, ευδιαχείριστος και ασφαλής. Είναι συμβατός με τον MTA sendmail. Σε αυτή την ενότητα περιγράφεται η εγκατάσταση και ρύθμιση του postfix. Επίσης, περιγράφεται η χρήση του ως εξυπηρετητή SMTP με χρήση ασφαλούς σύνδεσης (για την ασφαλή αποστολή email).



Αυτός ο οδηγός δεν καλύπτει την εγκατάσταση *Εικονικών τομέων (Virtual Domains)* για το Postfix. Για πληροφορίες σχετικά με τους εικονικούς τομείς και άλλες προχωρημένες δυνατότητες, δείτε το *Τμήμα 1.7.4, “Αναφορές” [263]*.

1.1. Εγκατάσταση

Για να εγκαταστήσετε το postfix εκτελέστε την ακόλουθη εντολή:

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

Απλά πατήστε enter όποτε εμφανίζονται ερωτήσεις. Στο επόμενο στάδιο θα κάνετε λεπτομερέστερες ρυθμίσεις

1.2. Βασικές ρυθμίσεις

Για να ρυθμίσετε το postfix εκτελέστε την ακόλουθη εντολή:

```
sudo dpkg-reconfigure postfix
```

Θα εμφανιστεί η διεπαφή χρήστη. Σε κάθε οθόνη επιλέξτε τις ακόλουθες τιμές:

- Internet Site
- mail.example.com
- steve
- mail.example.com, localhost.localdomain, localhost
- Όχι
- 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.0.0/24
- 0
- +
- all



Αντικαταστήστε το mail.example.com με τον τομέα για το οποίο θα αποδέχεστε email. Επίσης, το 192.168.0.0/24 με το δίκτυο και το εύρος (class range) του δικού σας εξυπηρετητή email, και το steve με το κατάλληλο όνομα χρήστη.

Τώρα είναι η κατάλληλη στιγμή να αποφασίσετε τη μορφή της ταχυδρομικής θυρίδας (mailbox) που θα χρησιμοποιήσετε. Η προεπιλογή του Postfix είναι το **mbox**. Αντί να

τροποποιήσετε απευθείας το αρχείο ρυθμίσεων, μπορείτε να χρησιμοποιήσετε την εντολή **postconf** για να ρυθμίσετε όλες τις παραμέτρους του postfix. Οι παράμετροι βρίσκονται αποθηκευμένες στο αρχείο `/etc/postfix/main.cf`. Αργότερα, αν επιθυμείτε να τροποποιήσετε μια συγκεκριμένη παράμετρο, μπορείτε είτε να τρέξετε την εντολή, είτε να κάνετε την αλλαγή απευθείας στο αρχείο.

Για να ρυθμίσετε τη μορφή της ταχυδρομικής θυρίδας ως **Maildir** εκτελέστε:

```
sudo postconf -e 'home_mailbox = Maildir/'
```



Έτσι, τα νέα μηνύματα θα τοποθετούνται στο `/home/όνομαχρήστη/Maildir`. Θα πρέπει να ρυθμίσετε το Mail Delivery Agent (MDA) ώστε να χρησιμοποιεί την ίδια διαδρομή.

1.3. Πιστοποίηση SMTP

Το SMTP-AUTH επιτρέπει σε πελάτες να ταυτοποιούνται μέσω ενός μηχανισμού πιστοποίησης (SASL). Θα πρέπει να χρησιμοποιείται Transport Layer Security (TLS) για την κρυπτογράφηση της διαδικασίας πιστοποίησης. Μετά την πιστοποίηση, ο εξυπηρετητής SMTP θα επιτρέπει στον πελάτη να διαβιβάζει email.

1. Ρυθμίστε το Postfix ώστε να χρησιμοποιεί SMTP-AUTH μέσω SASL (Dovecot SASL):

```
sudo postconf -e 'smtpd_sasl_type = dovecot'
sudo postconf -e 'smtpd_sasl_path = private/auth-client'
sudo postconf -e 'smtpd_sasl_local_domain ='
sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
sudo postconf -e 'broken_sasl_auth_clients = yes'
sudo postconf -e 'smtpd_sasl_auth_enable = yes'
sudo postconf -e 'smtpd_recipient_restrictions = \
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
```



Το `smtpd_sasl_path` είναι μια σχετική διαδρομή που καθορίζεται σε σχέση με τον κατάλογο ουράς του Postfix.

2. Next, generate or obtain a digital certificate for TLS. See *Τμήμα 5, “Πιστοποιητικά” [181]* for details. This example also uses a Certificate Authority (CA). For information on generating a CA certificate see *Τμήμα 5.5, “Αρχή Πιστοποίησης” [184]*.



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 certificates 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 *Τμήμα 5.3, “Δημιουργία ενός Πιστοποιητικού Υπογεγραμμένου από εσάς” [183]* for more details.

3. Αφού αποκτήσετε πιστοποιητικό, ρυθμίστε το Postfix έτσι ώστε να παρέχει κρυπτογράφηση TLS τόσο για τα εισερχόμενα όσο και για τα εξερχόμενα μηνύματα:

```
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 *Τμήμα 5, “Πιστοποιητικά” [181]*.



Μετά την εκτέλεση όλων αυτών των εντολών, το Postfix θα έχει ρυθμιστεί για χρήση του SMTP-AUTH και θα έχει δημιουργηθεί και ένα πιστοποιητικό με τη δική σας υπογραφή για την κρυπτογράφηση TLS.

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
```

Η αρχική ρύθμιση του postfix έχει ολοκληρωθεί. Εκτελέστε την ακόλουθη εντολή για να επανεκκινήσετε την υπηρεσία postfix:

sudo service postfix restart

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. Ρύθμιση του SASL

Το Postfix υποστηρίζει δύο υλοποιήσεις του SASL, τις Cyrus SASL και Dovecot SASL. Για να ενεργοποιήσετε το Dovecot SASL, θα πρέπει να εγκαταστήσετε το πακέτο `dovecot-common`. Από το τερματικό, δίνετε:

sudo apt-get install dovecot-common

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 =
```

¹ <http://www.ietf.org/rfc/rfc2554.txt>

² <http://www.ietf.org/rfc/rfc2222.txt>

```
#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
```

Αφού ολοκληρώσετε τη ρύθμιση του Dovecot, επανεκκινήστε το δίνοντας:

```
sudo service dovecot restart
```

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.

Για να εγκαταστήσετε το πακέτο από το τερματικό, εισάγετε:

```
sudo apt-get install mail-stack-delivery
```

Θα πρέπει πλέον να διαθέτετε ένα λειτουργικό εξυπηρετητή email, αλλά υπάρχουν και κάποιες ακόμη επιλογές που ίσως σας ενδιαφέρουν. Π.χ., το πακέτο χρησιμοποιεί το πιστοποιητικό και το κλειδί του πακέτου `ssl-cert`, και σε ένα περιβάλλον παραγωγής θα έπρεπε να χρησιμοποιείτε πιστοποιητικό και κλειδί που έχουν δημιουργηθεί για το συγκεκριμένο σύστημα. Δείτε το *Τμήμα 5, Πιστοποιητικά*; [181] για περισσότερες λεπτομέρειες.

Αφού αποκτήσετε ένα προσωποποιημένο πιστοποιητικό και κλειδί για το σύστημα, τροποποιήστε τις ακόλουθες επιλογές στο `/etc/postfix/main.cf`:

```
smtpd_tls_cert_file = /etc/ssl/certs/ssl-mail.pem  
smtpd_tls_key_file = /etc/ssl/private/ssl-mail.key
```

Τώρα, επανεκκινήστε το Postfix:

```
sudo service postfix restart
```

1.6. Δοκιμή

Η ρύθμιση του SMTP-AUTH έχει ολοκληρωθεί. Τώρα μπορείτε να τη δοκιμάσετε.

Για να ελέγξετε αν λειτουργούν σωστά τα SMTP-AUTH και TLS, εκτελέστε την ακόλουθη εντολή:

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

Αφού συνδεθείτε στον εξυπηρετητή postfix, πληκτρολογήστε:

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

Αν εμφανιστούν, μεταξύ άλλων, οι ακόλουθες γραμμές, τότε όλα λειτουργούν απρόσκοπτα. Πληκτρολογήστε **quit** για έξοδο.

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

1.7. Επίλυση Προβλημάτων

Σε αυτή την ενότητα περιγράφονται ορισμένοι κοινοί τρόποι εντοπισμού της αιτίας σε περίπτωση που προκύψουν προβλήματα.

1.7.1. Παράκαμψη του chroot

Το πακέτο postfix του Ubuntu εγκαθίσταται από προεπιλογή σε περιβάλλον *chroot* για λόγους ασφαλείας. Αυτό μπορεί να περιπλέξει τη διαδικασία εντοπισμού προβλημάτων.

Για να απενεργοποιήσετε το chroot, βρείτε την ακόλουθη γραμμή στο αρχείο ρυθμίσεων `/etc/postfix/master.cf`:

```
smtp inet n - - - - smtpd
```

και τροποποιήστε την ως εξής:

```
smtp inet n - n - - smtpd
```

Θα πρέπει να επανεκκινήσετε το Postfix για να χρησιμοποιήσετε τις ρυθμίσεις. Από το τερματικό, δίνετε:

```
sudo service postfix restart
```

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. Αρχεία καταγραφών (Log)

Το Postfix αποστέλλει όλα τα μηνύματα καταγραφών στο `/var/log/mail.log`. Ωστόσο, επειδή τα μηνύματα σφαλμάτων και προειδοποιήσεων είναι εύκολο να χαθούν ανάμεσα στα κανονικά μηνύματα, καταγράφονται και στα αρχεία `/var/log/mail.err` και `/var/log/mail.warn`, αντιστοίχως.

Για να παρακολουθείτε σε πραγματικό χρόνο τα μηνύματα των καταγραφών, μπορείτε να χρησιμοποιήσετε την εντολή `tail -f`:

```
tail -f /var/log/mail.err
```

Το επίπεδο λεπτομέρειας των καταγραφών μπορεί να αυξηθεί. Παρακάτω αναφέρονται ορισμένες ρυθμίσεις που επιτρέπουν την αύξηση της λεπτομέρειας των καταγραφών σε ορισμένους από τους τομείς που καλύφθηκαν παραπάνω.

- Για να αυξήσετε το επίπεδο καταγραφής της δραστηριότητας *TLS*, χρησιμοποιήστε τιμές από 1 έως 4 για την επιλογή `smtpd_tls_loglevel`.

```
sudo postconf -e 'smtpd_tls_loglevel = 4'
```

- Αν αντιμετωπίζετε προβλήματα στην αποστολή ή λήψη ηλ. ταχυδρομείου από συγκεκριμένο τομέα, μπορείτε να προσθέσετε τον τομέα στην παράμετρο `debug_peer_list`.

```
sudo postconf -e 'debug_peer_list = problem.domain'
```

- Μπορείτε να αυξήσετε τη λεπτομέρεια ενημέρωσης (verbosity) οποιασδήποτε υπηρεσίας Postfix τροποποιώντας το αρχείο `/etc/postfix/master.cf` και προσθέτοντας ένα `-v` στο τέλος της αντίστοιχης εγγραφής. Π.χ., για την εγγραφή *smtp*:

```
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 service postfix reload**

- 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 service dovecot reload**.



Ορισμένες από τις παραπάνω αλλαγές μπορεί να οδηγήσουν σε δραματική αύξηση των πληροφοριών που θα αποθηκεύονται στα αρχεία καταγραφών. Θυμηθείτε να επιστρέψετε στα προηγούμενα επίπεδα καταγραφών αφού επιλύσετε το πρόβλημα. Και φυσικά, επανεκκινήστε την κατάλληλη υπηρεσία για να εφαρμοστούν οι αλλαγές στις ρυθμίσεις.

1.7.4. Αναφορές

Η διαχείριση ενός εξυπηρετητή Postfix μπορεί να αποδειχθεί ιδιαίτερα πολύπλοκη διαδικασία. Ίσως χρειαστεί να απευθυνθείτε στην κοινότητα του Ubuntu για πιο εξειδικευμένη βοήθεια.

Ένα καλό μέρος για να ζητήσετε βοήθεια για το Postfix και να ενταχθείτε στην κοινότητα του Ubuntu Server είναι το κανάλι IRC *#ubuntu-server* στο *freenode*³. Επίσης, μπορείτε να δημοσιεύσετε μήνυμα σε ένα από τα *διαδικτυακά φόρουμ*⁴.

Για εις βάθος εξερεύνηση του Postfix οι ειδικοί του Ubuntu συνιστούν το: *Βιβλίο του Postfix*⁵.

Τέλος, ο ιστότοπος του *Postfix*⁶ περιέχει επίσης καλή τεκμηρίωση όλων των διαθέσιμων ρυθμίσεων.

³ <http://freenode.net>

⁴ <http://www.ubuntu.com/support/community/webforums>

⁵ <http://www.postfix-book.com/>

⁶ <http://www.postfix.org/documentation.html>

Also, the *Ubuntu Wiki Postfix*⁷ page has more information.

⁷ <https://help.ubuntu.com/community/Postfix>

2. Exim4

Το Exim4 είναι ένας ακόμη Message Transfer Agent (MTA), που αναπτύχθηκε από το Πανεπιστήμιο του Cambridge για χρήση σε συστήματα Unix συνδεδεμένα στο διαδίκτυο. Το Exim μπορεί να εγκατασταθεί στη θέση του sendmail, αν και οι ρυθμίσεις του exim διαφέρουν αρκετά από αυτές του sendmail.

2.1. Εγκατάσταση

Για να εγκαταστήσετε το exim4, εκτελέστε την ακόλουθη εντολή:

```
sudo apt-get install exim4
```

2.2. Ρυθμίσεις

Για να ρυθμίσετε το Exim4 εκτελέστε την ακόλουθη εντολή:

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

Θα εμφανιστεί η διεπαφή χρήστη. Η διεπαφή χρήστη σας επιτρέπει να ρυθμίσετε πολλές παραμέτρους. Π.χ., στο Exim4 οι ρυθμίσεις είναι κατανεμημένες σε διάφορα αρχεία. Αν θέλετε να τις συγκεντρώσετε σε ένα μόνο αρχείο, μπορείτε να το επιλέξετε από τη διεπαφή χρήστη.

All the parameters you configure in the user interface are stored in `/etc/exim4/update-exim4.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
```

Το κεντρικό αρχείο ρυθμίσεων δημιουργείται και αποθηκεύεται στο `/var/lib/exim4/config.autogenerated`.



Μην προσπαθήσετε ποτέ να τροποποιήσετε μόνοι σας το κεντρικό αρχείο ρυθμίσεων `/var/lib/exim4/config.autogenerated`. Ενημερώνεται αυτόματα όποτε εκτελείτε την εντολή **update-exim4.conf**

Μπορείτε να εκτελέσετε την ακόλουθη εντολή για να ξεκινήσετε την υπηρεσία Exim4.

```
sudo service exim4 start
```

2.3. Πιστοποίηση SMTP

Αυτή η ενότητα περιγράφει τη ρύθμιση του Exim4 ώστε να χρησιμοποιεί το SMTP-AUTH με τα TLS και SASL.

Το πρώτο βήμα είναι η δημιουργία ενός πιστοποιητικού για χρήση με το TLS. Από το τερματικό, δίνετε:

```
sudo /usr/share/doc/exim4-base/examples/exim-gencert
```

Τώρα θα πρέπει να ρυθμίσετε το Exim4 για χρήση με το TLS, τροποποιώντας το `/etc/exim4/conf.d/main/03_exim4-config_tlsoptions` και προσθέτοντας τα εξής:

```
MAIN_TLS_ENABLE = yes
```

Στη συνέχεια θα πρέπει να ρυθμίσετε το Exim4 ώστε να χρησιμοποιεί το `saslauthd` για πιστοποίηση. Τροποποιήστε το `/etc/exim4/conf.d/auth/30_exim4-config_examples` και αφαιρέστε τα σχόλια μπροστά από τις ενότητες `plain_saslauthd_server` και `login_saslauthd_server`.

```
plain_saslauthd_server:
driver = plaintext
public_name = PLAIN
server_condition = ${if saslauthd{${auth2}${auth3}}{1}{0}}
server_set_id = $auth2
server_prompts = :
.ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
server_advertise_condition = ${if eq{${tls_cipher}}{}}{*}}
.endif
#
login_saslauthd_server:
driver = plaintext
public_name = LOGIN
server_prompts = "Username:: : Password::"
# να μην αποστέλλονται οι κωδικοί πρόσβασης του συστήματος μέσω μη κρυπτογραφημένων συνδέσεων
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/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
```

Τέλος, ενημερώστε τις ρυθμίσεις του Exim4 επανεκκινώντας την υπηρεσία:


```
sudo update-exim4.conf
sudo service exim4 restart
```

2.4. Ρύθμιση του SASL

Αυτή η ενότητα περιγράφει τη διαδικασία ρύθμισης του `saslauthd` ώστε αυτό να αναλάβει την πιστοποίηση για το Exim4.

Το πρώτο βήμα είναι η εγκατάσταση του πακέτου `sasl2-bin`. Από το τερματικό, δίνετε:

```
sudo apt-get install sasl2-bin
```

Για να ρυθμίσετε το `saslauthd` τροποποιήστε το αρχείο ρυθμίσεων `/etc/default/saslauthd` και αντικαταστήστε το `START=no` με:

```
START=yes
```

Στη συνέχεια, ο χρήστης *Debian-exim* θα πρέπει να συμπεριληφθεί στην ομάδα *sasl*, για να μπορεί το Exim4 να χρησιμοποιεί την υπηρεσία `saslauthd`:

```
sudo adduser Debian-exim sasl
```

Τώρα, εκκινήστε την υπηρεσία `saslauthd`:

```
sudo service saslauthd start
```

Πλέον, το Exim4 έχει ρυθμιστεί για χρήση του SMTP-AUTH με πιστοποίηση TLS και SASL.

2.5. Αναφορές

- Ανατρέξτε στο *exim.org*⁸ για περισσότερες λεπτομέρειες.
- Επίσης, διατίθεται και το *Βιβλίο του Exim4*⁹.
- 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. Εξυηρητητής Dovecot

Το Dovecot είναι Mail Delivery Agent, γραμμένος με πρώτο γνώμονα την ασφάλεια. Υποστηρίζει τις κυριότερες μορφές ταχυδρομικής θυρίδας: mbox και Maildir. Σε αυτή την ενότητα περιγράφεται η ρύθμισή του ως εξυηρητητή imap ή pop3.

3.1. Εγκατάσταση

Για να εγκαταστήσετε το dovecot, εισάγετε την ακόλουθη εντολή στο τερματικό:

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

3.2. Ρυθμίσεις

Για να ρυθμίσετε το dovecot, μπορείτε να τροποποιήσετε το αρχείο `/etc/dovecot/dovecot.conf`. Μπορείτε να επιλέξετε το πρωτόκολλο που θα χρησιμοποιείται: pop3, pop3s (ασφαλές pop3), imap και imaps (ασφαλές imap). Η περιγραφή αυτών των πρωτοκόλλων υπερβαίνει το αντικείμενο του παρόντος οδηγού. Για περισσότερες λεπτομέρειες μπορείτε να ανατρέξετε στα άρθρα της Βικιπαίδειας για το POP3¹¹ και το IMAP¹².

Τα IMAPS και POP3S είναι περισσότερο ασφαλή από τα απλά IMAP και POP3 γιατί χρησιμοποιούν κρυπτογράφηση SSL για τη σύνδεση. Αφού επιλέξετε πρωτόκολλο, τροποποιήστε την ακόλουθη γραμμή στο αρχείο `/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 # (για το maildir)
```

ή

```
mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u # (για το mbox)
```



Αν ο τύπος ταχυδρομικής θυρίδας σας ήταν διαφορετικός, θα πρέπει να ρυθμίσετε τον Mail Transport Agent (MTA) για να μεταφέρει την εισερχόμενη αλληλογραφία στον νέο τύπο.

¹¹ <http://en.wikipedia.org/wiki/POP3>

¹² http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

¹³ <http://wiki2.dovecot.org/MailboxFormat>

Αφού ολοκληρώσετε τη ρύθμιση του dovecot, επανεκκινήστε την υπηρεσία dovecot για να το δοκιμάσετε:

sudo service dovecot restart

Ακόμη, αν έχετε ενεργοποιημένο το imap, ή το pop3, μπορείτε να προσπαθήσετε να κάνετε είσοδο με τις εντολές **telnet localhost pop3** ή **telnet localhost imap2**. Αν εμφανιστεί κάτι παρόμοιο με το παρακάτω, η εγκατάσταση έχει ολοκληρωθεί επιτυχώς:

```
bhuvan@rainbow:~$ telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^'.
+OK Dovecot ready.
```

3.3. Ρύθμιση του Dovecot SSL

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 *Τμήμα 5, “Πιστοποιητικά” [181]* 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. Ρύθμιση τείχους προστασίας για εξυπηρετητή ηλ. αλληλογραφίας

Για να έχετε πρόσβαση στον εξυπηρετητή ηλ. αλληλογραφίας από άλλο υπολογιστή, θα πρέπει να ρυθμίσετε το τείχος προστασίας (firewall) σας ώστε να δέχεται συνδέσεις προς τον εξυπηρετητή, στις απαραίτητες θύρες.

3.5. Αναφορές

- Ανατρέξτε στον *ιστότοπο του Dovecot*¹⁴ για περισσότερες πληροφορίες.
- Also, the *Dovecot Ubuntu Wiki*¹⁵ page has more details.

¹⁴ <http://www.dovecot.org/>

¹⁵ <https://help.ubuntu.com/community/Dovecot>

4. Mailman

Το Mailman είναι ένα πρόγραμμα ανοιχτού κώδικα για τη διαχείριση συζητήσεων ηλ. αλληλογραφίας και λιστών ηλ. ενημέρωσης (e-newsletter). Πολλές λίστες ηλ. ταχυδρομείου ανοιχτού κώδικα (συμπεριλαμβανομένων και όλων των λιστών ηλ. ταχυδρομείου του *Ubuntu*¹⁶) χρησιμοποιούν το Mailman. Πρόκειται για ισχυρό λογισμικό, εύκολο στην εγκατάσταση και τη συντήρηση.

4.1. Εγκατάσταση

Το Mailman παρέχει μια διεπαφή Ιστού για τους διαχειριστές και τους χρήστες, και χρησιμοποιεί εξωτερικό εξυπηρετητή για την αποστολή και λήψη email. Συνεργάζεται άψογα με τους παρακάτω εξυπηρετητές email:

- Postfix
- Exim
- Sendmail
- Qmail

Θα εξετάσουμε τη διαδικασία εγκατάστασης και ρύθμισης του Mailman με χρήση του εξυπηρετητή Ιστού Apache και, είτε του εξυπηρετητή email Postfix, είτε του Exim. Αν επιθυμείτε να εγκαταστήσετε το Mailman χρησιμοποιώντας διαφορετικό εξυπηρετητή email, παρακαλούμε ανατρέξτε στην ενότητα Αναφορές.



Θα πρέπει να εγκαταστήσετε μόνο έναν εξυπηρετητή email, και το Postfix είναι ο προεπιλεγμένος Mail Transfer Agent του Ubuntu.

4.1.1. Apache2

To install apache2 you refer to *Τμήμα 1.1, “Εγκατάσταση” [200]* for details.

4.1.2. Postfix

Για οδηγίες σχετικά με την εγκατάσταση και ρύθμιση του Postfix δείτε το *Τμήμα 1, “Postfix” [256]*

4.1.3. Exim4

Για την εγκατάσταση του Exim4 δείτε το *Τμήμα 2, “Exim4” [265]*.

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:

¹⁶ <http://lists.ubuntu.com>

```
dc_use_split_config='true'
```

4.1.4. Mailman

Για να εγκαταστήσετε το Mailman, εισάγετε την ακόλουθη εντολή στο τερματικό:

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

Αντιγράφει τα αρχεία της εγκατάστασης στον κατάλογο `/var/lib/mailman`. Εγκαθιστά τα σενάρια εντολών CGI στον κατάλογο `/usr/lib/cgi-bin/mailman`. Δημιουργεί το χρήστη `linux list`. Δημιουργεί την ομάδα `linux list`. Η διεργασία του `mailman` ανήκει σε αυτόν το χρήστη.

4.2. Ρυθμίσεις

Σε αυτή την ενότητα υποθέτουμε ότι έχετε ήδη εγκαταστήσει επιτυχώς τα `mailman`, `apache2` και το `postfix` ή το `exim4`. Τώρα απομένει μόνο η ρύθμισή τους.

4.2.1. Apache2

Το Mailman συμπεριλαμβάνει ένα αρχείο-υπόδειγμα ρύθμισης του Apache, το `/etc/mailman/apache.conf`. Για να μπορέσει το Apache να χρησιμοποιήσει τις ρυθμίσεις του, το αρχείο θα πρέπει να αντιγραφεί στο `/etc/apache2/sites-available`:

```
sudo cp /etc/mailman/apache.conf /etc/apache2/sites-available/mailman.conf
```

Έτσι, δημιουργείται ένα νέο *Εικονικό Σύστημα (VirtualHost)* Apache για τον ιστότοπο διαχείρισης του Mailman. Τώρα, μπορείτε να ενεργοποιήσετε τις νέες ρυθμίσεις και να επανεκκινήσετε το Apache:

```
sudo a2ensite mailman.conf  
sudo service apache2 restart
```

Το Mailman χρησιμοποιεί το `apache2` για τα σενάρια εντολών CGI. Τα σενάρια CGI του `mailman` CGI βρίσκονται στον κατάλογο `/usr/lib/cgi-bin/mailman`. Άρα, η διεύθυνση url του `mailman` θα είναι `http://hostname/cgi-bin/mailman/`. Αν θέλετε να αλλάξετε αυτή τη συμπεριφορά μπορείτε να τροποποιήσετε το αρχείο `/etc/apache2/sites-available/mailman.conf`.

4.2.2. Postfix

Για να ενσωματώσουμε και το `Postfix`, θα συσχετίσουμε τον τομέα `lists.example.com` με τις λίστες ταχυδρομείου. Αντικαταστήστε το `lists.example.com` με τον τομέα της επιλογής σας.

Μπορείτε να χρησιμοποιήσετε την εντολή `postconf` για να προσθέσετε τις απαραίτητες ρυθμίσεις στο `/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'
```

Στο `/etc/postfix/master.cf` επαληθεύστε προσεκτικά ότι διαθέτετε τον ακόλουθο μεταφορέα (transport):

```
mailman unix - n n - - pipe
 flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
 ${nexthop} ${user}
```

Καλεί το σενάριο *postfix-to-mailman.py* όποτε η λίστα λαμβάνει ένα email.

Συσχετίστε τον τομέα `lists.example.com` με τον μεταφορέα του Mailman μέσω του χάρτη μεταφοράς (transport map). Τροποποιήστε το αρχείο `/etc/postfix/transport`:

```
lists.example.com mailman:
```

Τώρα, ζητήστε από το Postfix να δημιουργήσει το χάρτη μεταφοράς, δίνοντας από το τερματικό:

```
sudo postmap -v /etc/postfix/transport
```

Τέλος, επανεκκινήστε το Postfix για να ενεργοποιήσετε τις νέες ρυθμίσεις:

```
sudo service postfix restart
```

4.2.3. Exim4

Αφού εγκατασταθεί το Exim4, μπορείτε να εκκινήσετε τον εξυπηρετητή Exim με την ακόλουθη εντολή:

```
sudo service exim4 start
```

Για να επιτρέψετε στο mailman να συνεργαστεί με το Exim4, θα χρειαστεί να ρυθμίσετε κατάλληλα το Exim4. Όπως αναφέρθηκε προηγουμένως, η προεπιλογή του Exim4 είναι να χρησιμοποιεί πολλαπλά αρχεία ρυθμίσεων διαφορετικών τύπων. Για περισσότερες λεπτομέρειες, δείτε τον ιστότοπο του *Exim*¹⁷. Για το mailman, θα πρέπει να προσθέσουμε ένα νέο αρχείο ρυθμίσεων στους ακόλουθους τύπους ρυθμίσεων:

- Main (Κύριος)
- Transport (Μεταφορέας)
- Router (Δρομολογητής)

Το Exim δημιουργεί ένα κεντρικό αρχείο ρυθμίσεων, ταξινομώντας όλα αυτά τα επιμέρους αρχεία ρυθμίσεων. Άρα, η σειρά αυτών των αρχείων παίζει καθοριστικό ρόλο.

¹⁷ <http://www.exim.org>

4.2.4. Main (Κύριος)

Όλα τα αρχεία ρυθμίσεων που ανήκουν στον τύπο main αποθηκεύονται στον κατάλογο /etc/exim4/conf.d/main/. Μπορείτε να προσθέσετε τα παρακάτω σε ένα νέο αρχείο, με όνομα 04_exim4-config_mailman:

```
# start
# Ο αρχικός κατάλογος της εγκατάστασης του Mailman -- δηλαδή ο κατάλογος με
# το πρόθεμα Mailman.
# Στο Ubuntu θα έπρεπε να είναι "/var/lib/mailman"
# Συνήθως, ταυτίζεται με το ~mailman
MM_HOME=/var/lib/mailman
#
# Χρήστης και ομάδα για το Mailman, θα πρέπει να ταυτίζεται με την τιμή του --with-mail-gid
# στο σενάριο ρύθμισης του Mailman. Η τιμή του κανονικά είναι "mailman"
MM_UID=list
MM_GID=list
#
# Τομείς όπου βρίσκονται οι λίστες σας - λίστα διαχωρισμένη με άνω κάτω τελεία
# Ίσως σας ενδιαφέρει να τους προσθέσετε και στο local_domains
domainlist mm_domains=hostname.com
#
# -----
#
# Αυτές οι τιμές προκύπτουν από τις παραπάνω τιμές. Δε χρειάζονται
# επεξεργασία εκτός αν έχετε μπλέξει την εγκατάστασή σας του mailman
#
# Η διαδρομή του σεναρίου-περιβλήματος mail του Mailman
MM_WRAP=MM_HOME/mail/mailman
#
# Η διαδρομή του αρχείου ρυθμίσεων των λιστών (απαραίτητο αρχείο
# για την επαλήθευση των διευθύνσεων των λιστών)
MM_LISTCHK=MM_HOME/lists/${lc::$local_part}/config.pck
# end
```

4.2.5. Transport (Μεταφορέας)

Όλα τα αρχεία ρυθμίσεων που ανήκουν στον τύπο transport αποθηκεύονται στον κατάλογο /etc/exim4/conf.d/transport/. Μπορείτε να προσθέσετε τα παρακάτω σε ένα νέο αρχείο, με όνομα 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 (Δρομολογητής)

Όλα τα αρχεία ρυθμίσεων που ανήκουν στον τύπο router αποθηκεύονται στον κατάλογο /etc/exim4/conf.d/router/. Μπορείτε να προσθέσετε τα παρακάτω σε ένα νέο αρχείο, με όνομα 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
```



Τα αρχεία ρυθμίσεων main και transport μπορούν να τοποθετηθούν με οποιαδήποτε σειρά. Ωστόσο, η σειρά των αρχείων ρυθμίσεων router πρέπει να είναι η ίδια. Το αρχείο αυτό πρέπει να βρίσκεται πριν από το αρχείο 200_exim4-config_primary. Αυτά τα δύο αρχεία ρυθμίσεων περιέχουν τον ίδιο τύπο πληροφοριών. Το πρώτο αρχείο υπερισχύει. Για περισσότερες λεπτομέρειες, δείτε την ενότητα Αναφορές.

4.2.7. Mailman

Αφού εγκατασταθεί το mailman, μπορείτε να το εκτελέσετε με την ακόλουθη εντολή:

```
sudo service mailman start
```

Αφού εγκατασταθεί το mailman, θα πρέπει να δημιουργήσετε την προεπιλεγμένη λίστα ταχυδρομείου. Εκτελέστε την ακόλουθη εντολή:

```
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:

```
## λίστα ταχυδρομείου mailman
```

```
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...

#

Έχουμε ρυθμίσει το Postfix ή το Exim4 ώστε να αναγνωρίζουν όλα τα email του mailman. Άρα, δεν είναι υποχρεωτικό να προσθέσουμε νέες εγγραφές στο `/etc/aliases`. Αν έχετε κάνει αλλαγές στα αρχεία ρυθμίσεων, φροντίστε να επανεκκινήσετε τις αντίστοιχες υπηρεσίες πριν προχωρήσετε στην επόμενη ενότητα.



Το Exim4 δεν χρησιμοποιεί τα παραπάνω ψευδώνυμα (alias) για την προώθηση email στο Mailman, γιατί χρησιμοποιεί τη μέθοδο *ανακάλυψης (discover)*. Για να απενεργοποιήσετε τα ψευδώνυμα κατά τη δημιουργία της λίστας, μπορείτε να προσθέσετε τη γραμμή `MTA=None` στο αρχείο ρυθμίσεων του Mailman, `/etc/mailman/mm_cfg.py`.

4.3. Διαχείριση

Υποθέτουμε ότι η εγκατάστασή σας διαθέτει τις προεπιλεγμένες ρυθμίσεις. Τα σενάρια cgi του mailman βρίσκονται στον κατάλογο `/usr/lib/cgi-bin/mailman/`. Το Mailman παρέχει ένα εργαλείο διαχείρισης μέσω Ιστού. Για να αποκτήσετε πρόσβαση στη σελίδα, εισάγετε την ακόλουθη διεύθυνση στον περιηγητή σας:

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

Η προεπιλεγμένη λίστα ταχυδρομείου, η *mailman*, εμφανίζεται στην οθόνη. Αν κάνετε κλικ στο όνομά της, θα σας ζητηθεί ο κωδικός πιστοποίησής σας. Αν εισάγετε το σωστό κωδικό, θα σας δοθεί η δυνατότητα να αλλάξετε τις ρυθμίσεις διαχείρισης αυτής της λίστας.

Μπορείτε να δημιουργήσετε νέα λίστα ταχυδρομείου χρησιμοποιώντας το εργαλείο της γραμμής εντολών (`/usr/sbin/newlist`). Εναλλακτικά, μπορείτε να δημιουργήσετε νέα λίστα ταχυδρομείου χρησιμοποιώντας τη διεπαφή Ιστού.

4.4. Χρήστες

Το Mailman παρέχει μία διεπαφή ιστού για τους χρήστες. Για να αποκτήσετε πρόσβαση στη σελίδα, εισάγετε την ακόλουθη διεύθυνση στον περιηγητή σας:

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

Η προεπιλεγμένη λίστα ταχυδρομείου, η *mailman*, εμφανίζεται στην οθόνη. Αν κάνετε κλικ στο όνομά της, θα εμφανιστεί η φόρμα εγγραφής συνδρομητή. Μπορείτε να εισάγετε τη διεύθυνση email σας, το όνομά σας (προαιρετικά) και τον κωδικό σας για να εγγραφείτε

συνδρομητής. Στη συνέχεια, θα σας σταλεί μία πρόσκληση μέσω email. Μπορείτε να ακολουθήσετε τις οδηγίες στην πρόσκληση για να ολοκληρώσετε την εγγραφή σας.

4.5. Αναφορές

*GNU Mailman - Εγχειρίδιο εγκατάστασης*¹⁸

*HOWTO - Συνδυασμός Exim 4 και Mailman 2.1*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. Φίλτρα ηλ. αλληλογραφίας

Σήμερα, ένα από τα σημαντικότερα προβλήματα του email είναι τα μαζικά ανεπίκλητα email (Unsolicited Bulk Email). Γνωστά και ως SPAM, αυτά τα μηνύματα ενδέχεται να περιέχουν ιούς ή άλλα είδη κακόβουλου λογισμικού. Σύμφωνα με ορισμένες πηγές, αυτά τα μηνύματα αποτελούν την πλειονότητα των email που διακινούνται στο Διαδίκτυο.

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.

- Το Amavisd-new είναι ένα πρόγραμμα-περίβλημα που μπορεί να καλεί διάφορα άλλα προγράμματα φιλτραρίσματος περιεχομένου, για εντοπισμό σπαμ, ιών, κτλ.
- Το Spamassassin χρησιμοποιεί διάφορους μηχανισμούς για να φιλτράρει την ηλ. αλληλογραφία με βάση το περιεχόμενο των μηνυμάτων.
- Το ClamAV είναι μία αντιική εφαρμογή ανοιχτού κώδικα.
- opendkim implements a Sendmail Mail Filter (Milter) for the DomainKeys Identified Mail (DKIM) standard.
- Το python-policyd-spf επιτρέπει ελέγχους Sender Policy Framework (SPF) με χρήση του Postfix.

Δείτε πώς συνδυάζονται όλα μαζί:

- Το μήνυμα email γίνεται δεκτό από το Postfix.
- The message is passed through any external filters opendkim and python-policyd-spf in this case.
- Το Amavisd-new προχωρεί σε επεξεργασία του μηνύματος.
- Χρησιμοποιείται το ClamAV για τη σάρωση του μηνύματος. Αν το μήνυμα περιέχει ιό, το Postfix απορρίπτει το μήνυμα.
- Στη συνέχεια, τα "καθαρά" μηνύματα αναλύονται από το Spamassassin για να διαπιστωθεί αν είναι σπαμ. Τέλος, το Spamassassin προσθέτει γραμμές X-Header, επιτρέποντας στο Amavisd-new να συνεχίσει την επεξεργασία του μηνύματος.

Π.χ., αν ένα μήνυμα έχει βαθμολογία σπαμ πάνω από πενήντα, το μήνυμα μπορεί να αφαιρεθεί από την ουρά και να μη χρειαστεί ποτέ να ενοχλήσει τον παραλήπτη. Ένας άλλος τρόπος προσέγγισης των ύποπτων μηνυμάτων είναι η αποστολή τους στον Mail User Agent (MUA), έτσι ώστε ο χρήστης να τα χειριστεί όπως επιθυμεί.

5.1. Εγκατάσταση

Δείτε το *Τμήμα 1, “Postfix” [256]* για οδηγίες εγκατάστασης και ρύθμισης του Postfix.

Για να εγκαταστήσετε τις υπόλοιπες εφαρμογές εισάγετε τα ακόλουθα στο τερματικό:

```
sudo apt-get install amavisd-new spamassassin clamav-daemon
sudo apt-get install opendkim postfix-policyd-spf-python
```

Υπάρχουν ορισμένα προαιρετικά πακέτα, συμπληρωματικά του Spamassassin, για καλύτερη προστασία από τα σπαμ:

```
sudo apt-get install pyzor razor
```

Πέρα από τις κύριες εφαρμογές φιλτραρίσματος, για ορισμένα συνημμένα απαιτούνται και εργαλεία συμπίεσης:

```
sudo apt-get 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-get update** before trying to install again.

5.2. Ρυθμίσεις

Τώρα, κάντε τις απαραίτητες ρυθμίσεις για να επιτρέψετε τη συνεργασία όλων των εργαλείων στο φιλτράρισμα του email.

5.2.1. ClamAV

Η προεπιλεγμένη συμπεριφορά του ClamAV καλύπτει τις ανάγκες μας. Για περισσότερες επιλογές ρύθμισης του ClamAV, ανατρέξτε στα αρχεία ρυθμίσεων στο `/etc/clamav`.

Προσθέστε το χρήστη *clamav* στην ομάδα *amavis*, έτσι ώστε το Amavisd-new να διαθέτει πρόσβαση για τη σάρωση αρχείων:

```
sudo adduser clamav amavis
sudo adduser amavis clamav
```

5.2.2. Spamassassin

Το Spamassassin εντοπίζει αυτόματα και χρησιμοποιεί τα διάφορα προαιρετικά εργαλεία. Άρα, δεν απαιτείται ρύθμιση των pyzor και razor.

Τροποποιήστε το `/etc/default/spamassassin` για να ενεργοποιήσετε την υπηρεσία Spamassassin. Αλλάξτε το `ENABLED=0` σε:

ENABLED=1

Τώρα, εκκινήστε την υπηρεσία:

sudo service spamassassin start

5.2.3. Amavisd-new

Καταρχάς, ενεργοποιήστε τον εντοπισμό σπαμ και ιών του Amavisd-new, τροποποιώντας το αρχείο `/etc/amavis/conf.d/15-content_filter_mode`:

```
use strict;
```

```
# Μπορείτε να τροποποιήσετε το αρχείο για να επανενεργοποιήσετε τον έλεγχο  
# για σπαμ μέσω spamassassin, καθώς και τον εντοπισμό ιών.
```

```
#  
# Προεπιλεγμένη λειτουργία αντιϊικού ελέγχου  
# Αφαιρέστε τα σχόλια από τις δύο παρακάτω γραμμές για να την ενεργοποιήσετε  
#
```

```
@bypass_virus_checks_maps = (  
  \bypass_virus_checks, \bypass_virus_checks_acl, \bypass_virus_checks_re);
```

```
#  
# Προεπιλεγμένη λειτουργία ελέγχου για σπαμ  
# Αφαιρέστε τα σχόλια από τις δύο παρακάτω γραμμές για να την ενεργοποιήσετε  
#
```

```
@bypass_spam_checks_maps = (  
  \bypass_spam_checks, \bypass_spam_checks_acl, \bypass_spam_checks_re);
```

```
1; # διασφάλιση ορισμένης επιστροφής
```

Η επιστροφή των μηνυμάτων σπαμ στον αποστολέα μπορεί να αποδειχθεί κακή ιδέα, καθώς η διεύθυνση αποστολέα συχνά είναι πλαστή. Μπορείτε να τροποποιήσετε το `/etc/amavis/conf.d/20-debian_defaults` και να ορίσετε το `$final_spam_destiny` ως `D_DISCARD` (διαγραφή) αντί για `D_BOUNCE` (επιστροφή), ως εξής:

```
$final_spam_destiny = D_DISCARD;
```

Επιπροσθέτως, μπορείτε να προσαρμόσετε τις ακόλουθες επιλογές, ώστε να σημειώνονται περισσότερα μηνύματα ως σπαμ:

```
$sa_tag_level_deflt = -999; # προσθήκη κεφαλίδων πληροφόρησης σπαμ από αυτό το επίπεδο και πάνω  
$sa_tag2_level_deflt = 6.0; # προσθήκη κεφαλίδων 'spam detected' (εντοπίστηκε σπαμ) σε αυτό το επίπεδο  
$sa_kill_level_deflt = 21.0; # εκκίνηση ενεργειών αποφυγής σπαμ
```

```
$sa_dsn_cutoff_level = 4; # επίπεδο σπαμ πάνω από το οποίο δεν αποστέλλεται DSN
```

Αν το *όνομα* του εξυπηρετητή είναι διαφορετικό από την εγγραφή MX του τομέα, ίσως χρειαστεί να ορίσετε χειροκίνητα την επιλογή *\$myhostname*. Επιπλέον, αν ο εξυπηρετητής λαμβάνει email για πολλαπλούς τομείς, θα πρέπει να προσαρμοστεί κατάλληλα η επιλογή *@local_domains_acl*. Τροποποιήστε το αρχείο */etc/amavis/conf.d/50-user*:

```
$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(.);
```

Αφού ολοκληρωθεί η ρύθμιση, το Amavisd-new θα πρέπει να εκκινηθεί εκ νέου:

```
sudo service amavis restart
```

5.2.3.1. Λευκή λίστα DKIM

Το Amavisd-new μπορεί να ρυθμιστεί έτσι ώστε να προσθέτει αυτόματα στη *Λευκή λίστα* τις διευθύνσεις που προέρχονται από τομείς με έγκυρα κλειδιά τομέα (domain keys). Το αρχείο */etc/amavis/conf.d/40-policy_banks* περιέχει ορισμένους προκαθορισμένους τομείς.

Υπάρχουν διάφοροι τρόποι ρύθμισης της λευκής λίστας για ένα τομέα:

- *'example.com' => 'WHITELIST'*; προσθέτει στη λευκή λίστα όλες τις διευθύνσεις του τομέα "example.com".
- *'.example.com' => 'WHITELIST'*; προσθέτει στη λευκή λίστα όλες τις διευθύνσεις των υποτομέων του "example.com" που διαθέτουν έγκυρη υπογραφή.
- *'.example.com/@example.com' => 'WHITELIST'*; προσθέτει στη λευκή λίστα τους υποτομείς του "example.com" που χρησιμοποιούν την υπογραφή του γονικού τομέα *example.com*.
- *'./@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 service amavis restart
```



Σε αυτές τις περιπτώσεις, από τη στιγμή που ένας τομέας προστίθεται στη λευκή λίστα, τα μηνύματά του δεν φιλτράρονται καθόλου για σπαμ ή ιούς. Εσείς αποφασίζετε αν αυτή είναι η συμπεριφορά που επιθυμείτε για τον τομέα.

5.2.4. Postfix

Για το συνδυασμό με το Postfix, εισάγετε τα ακόλουθα στο τερματικό:

```
sudo postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'
```

Τώρα, τροποποιήστε το `/etc/postfix/master.cf` και προσθέστε τα ακόλουθα στο τέλος του αρχείου:

```
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
```

Επίσης, προσθέστε τις ακόλουθες δύο γραμμές αμέσως μετά την υπηρεσία μεταφοράς *"pickup"*:

```
-o content_filter=
-o receive_override_options=no_header_body_checks
```

Έτσι, τα μηνύματα που δημιουργούνται για την υποβολή αναφορών για σπαμ δε θα χαρακτηρίζονται ως σπαμ.

Τώρα επανεκκινήστε το Postfix:

```
sudo service postfix restart
```

Θα ενεργοποιηθεί το φιλτράρισμα του περιεχομένου για τον εντοπισμό σπαμ και ιων.

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. Δοκιμή

Καταρχάς, ελέγξτε ότι το SMTP του Amavisd-new αφουγκράζεται:

```
telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.
220 [127.0.0.1] ESMTP amavisd-new service ready
^]
```

Στην κεφαλίδα των μηνυμάτων που έχουν περάσει από το φίλτρο περιεχομένου θα πρέπει να εμφανίζονται τα:

```
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:
```



Η δική σας έξοδος μπορεί να διαφέρει, αλλά το σημαντικό είναι να υπάρχουν οι εγγραφές *X-Virus-Scanned* και *X-Spam-Status*.

5.4. Επίλυση Προβλημάτων

Ο καλύτερος τρόπος να καταλάβετε γιατί κάτι δεν πάει καλά σε περίπτωση προβλήματος είναι να ελέγξετε τα αρχεία καταγραφών.

- Για πληροφορίες σχετικά με τις καταγραφές του Postfix δείτε την ενότητα *Τμήμα 1.7, “Επίλυση Προβλημάτων” [261]*.
- Το Amavisd-new χρησιμοποιεί το Syslog για να αποστέλλει μηνύματα στο `/var/log/mail.log`. Το επίπεδο λεπτομέρειάς τους μπορεί να αυξηθεί αν προστεθεί η επιλογή *\$log_level* στο `/etc/amavis/conf.d/50-user`, και οριστεί η τιμή της μεταξύ 1 και 5.


```
$log_level = 2;
```



Όταν αυξάνεται το επίπεδο καταγραφών του Amavisd-new, αυξάνεται και το επίπεδο καταγραφών του Spamassassin.

- Το επίπεδο καταγραφών του ClamAV μπορεί να αυξηθεί αν τροποποιηθεί το `/etc/clamav/clamd.conf` με προσθήκη της ακόλουθης επιλογής:

```
LogVerbose true
```

Η προεπιλογή του ClamAV είναι να αποστέλλει τις καταγραφές στο `/var/log/clamav/clamav.log`.



Μετά την αλλαγή των ρυθμίσεων για τις καταγραφές μιας εφαρμογής, θυμηθείτε να επανεκκινήσετε την υπηρεσία για να ενεργοποιήσετε τις νέες ρυθμίσεις. Επίσης, όταν επιλύσετε το πρόβλημά σας, καλό θα ήταν να επαναφέρετε τις φυσιολογικές ρυθμίσεις των καταγραφών.

5.5. Αναφορές

Για περισσότερες πληροφορίες σχετικά με τη χρήση φίλτρων email δείτε τους ακόλουθους συνδέσμους:

- *Τεκμηρίωση Amavisd-new*²¹
- *ClamAV Documentation*²² and *ClamAV Wiki*²³
- *Spamassassin Wiki*²⁴
- *Ιστοσελίδα Pyzor*²⁵
- *Ιστοσελίδα Razor*²⁶
- *DKIM.org*²⁷
- *Postfix Amavis New*²⁸

Επίσης, ρωτήστε ελεύθερα στο κανάλι IRC `#ubuntu-server` στο *freenode*²⁹.

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/>

²⁷ <http://dkim.org/>

²⁸ <https://help.ubuntu.com/community/PostfixAmavisNew>

²⁹ <http://freenode.net>

Κεφάλαιο 16. Εφαρμογές συζήτησης

1. Επισκόπηση

Σε αυτή την ενότητα, θα συζητήσουμε πώς να εγκαταστήσετε και να ρυθμίσετε έναν εξυπηρετητή IRC, τον ircd-irc2. Θα συζητήσουμε επίσης πώς να εγκαταστήσετε και να ρυθμίσετε το Jabber, έναν εξυπηρετητή άμεσης ανταλλαγής μηνυμάτων.

2. Εξυπηρετητής IRC

Το αποθετήριο του Ubuntu έχει πολλούς εξυπηρετητές Internet Relay Chat. Αυτή η ενότητα εξηγεί πώς να εγκαταστήσετε και να ρυθμίσετε τον πρώτο εξυπηρετητή IRC, τον `ircd-irc2`.

2.1. Εγκατάσταση

Για να εγκαταστήσετε το `ircd-irc2`, εκτελέστε την παρακάτω εντολή στο τερματικό:

```
sudo apt-get install ircd-irc2
```

Τα αρχεία ρυθμίσεων είναι αποθηκευμένα στον κατάλογο `/etc/ircd`. Τα έγγραφα είναι διαθέσιμα στον κατάλογο `/usr/share/doc/ircd-irc2`.

2.2. Ρυθμίσεις

Οι ρυθμίσεις του IRC μπορούν να γίνουν στο αρχείο ρυθμίσεων `/etc/ircd/ircd.conf`. Σε αυτό το αρχείο μπορείτε να ορίσετε το όνομα τομέα του IRC τροποποιώντας την ακόλουθη γραμμή:

```
M:irc.localhost::Debian ircd default configuration::000A
```

Παρακαλούμε σιγουρευτείτε πως προσθέσατε ψευδώνυμα (aliases) DNS για το όνομα τομέα του IRC. Για παράδειγμα, αν ορίσατε το `irc.livecipher.com` ως το όνομα τομέα του IRC, παρακαλούμε σιγουρευτείτε πως το `irc.livecipher.com` είναι επιλύσιμο στον εξυπηρετητή ονομάτων τομέα (DNS) σας. Το όνομα τομέα του IRC δεν θα πρέπει να είναι το ίδιο με το όνομα του υπολογιστή.

The IRC admin details can be configured by editing the following line:

```
A:Organization, IRC dept.:Daemon <ircd@example.irc.org>;Client Server::IRCnet:
```

Θα πρέπει να προσθέσετε συγκεκριμένες γραμμές για την ρύθμιση της λίστας των θυρών IRC στις οποίες θα αναμένονται συνδέσεις, να ρυθμίσετε τα πιστοποιητικά των διαχειριστών, να ρυθμίσετε την πιστοποίηση πελατών, κτλ. Για λεπτομέρειες, παρακαλούμε αναφερθείτε στο παράδειγμα αρχείου ρυθμίσεων `/usr/share/doc/ircd-irc2/ircd.conf.example.gz`.

Το λογότυπο του IRC που θα εμφανίζεται στον πελάτη IRC, όταν ο χρήστης συνδέεται στον εξυπηρετητή, μπορεί να οριστεί στο αρχείο `/etc/ircd/ircd.motd`.

Αφού κάνετε τις απαραίτητες αλλαγές στο αρχείο ρυθμίσεων, μπορείτε να επανεκκινήσετε τον εξυπηρετητή IRC χρησιμοποιώντας την ακόλουθη εντολή:

```
sudo service ircd-irc2 restart
```

2.3. Αναφορές

Μπορεί επίσης να σας ενδιαφέρει να ρίξετε μια ματιά σε άλλες υπηρεσίες IRC που είναι διαθέσιμες στο αποθετήριο του Ubuntu. Συμπεριλαμβανομένων και των `ircd-ircu` και `ircd-hybrid`.

- Αναφερθείτε στο *FAQ του IRCD*¹ για περισσότερες λεπτομέρειες για τον εξυπηρετητή IRC.

¹ http://www.irc.org/tech_docs/ircnet/faq.html

3. Εξυπηρετητής άμεσης ανταλλαγής μηνυμάτων Jabber

Το *Jabber*, ένα δημοφιλές πρωτόκολλο ανταλλαγής άμεσων μηνυμάτων, βασίζεται στο XMPP, ένα ανοιχτό πρότυπο για ανταλλαγή άμεσων μηνυμάτων και χρησιμοποιείται από πολλές δημοφιλείς εφαρμογές. Αυτή η ενότητα καλύπτει τη ρύθμιση ενός εξυπηρετητή *Jabberd 2* σε ένα τοπικό δίκτυο (LAN). Αυτές οι ρυθμίσεις μπορούν επίσης να προσαρμοστούν για να παρέχονται υπηρεσίες ανταλλαγής μηνυμάτων σε χρήστες σε όλο το διαδίκτυο.

3.1. Εγκατάσταση

Για να εγκαταστήσετε το *jabberd2*, πληκτρολογήστε σε ένα τερματικό:

```
sudo apt-get install jabberd2
```

3.2. Ρυθμίσεις

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 user authentication.

Πρώτα, επεξεργαστείτε το `/etc/jabberd2/sm.xml` αλλάζοντας το:

```
<id>jabber.example.com</id>
```



Αντικαταστήστε το *jabber.example.com* με το όνομα, ή κάποιο άλλο αναγνωριστικό, του εξυπηρετητή σας.

Τώρα, στην ενότητα `<storage>`, αλλάξτε το `<driver>` σε:

```
<driver>db</driver>
```

Μετά, επεξεργαστείτε το `/etc/jabberd2/c2s.xml` και στην ενότητα `<local>`, αλλάξτε το:

```
<id>jabber.example.com</id>
```

Και στην ενότητα `<authreg>`, τροποποιήστε την ενότητα `<module>` σε:

```
<module>db</module>
```

Τέλος, επανεκκινήστε το *jabberd2* για να ενεργοποιηθούν οι νέες ρυθμίσεις:

```
sudo service jabberd2 restart
```

Τώρα θα πρέπει να μπορείτε να συνδεθείτε στον εξυπηρετητή χρησιμοποιώντας έναν πελάτη Jabber όπως το Pidgin για παράδειγμα.



Το πλεονέκτημα του να χρησιμοποιείτε Berkeley DB για τα δεδομένα των χρηστών είναι πως αφού ρυθμιστεί, δεν χρειάζεται περαιτέρω συντήρηση. Αν χρειάζεστε περισσότερο έλεγχο στους λογαριασμούς και στα πιστοποιητικά των χρηστών, συνιστάται να χρησιμοποιήσετε κάποια άλλη μέθοδο πιστοποίησης.

3.3. Αναφορές

- Ο ιστότοπος του *Jabberd2*² περιέχει περισσότερες λεπτομέρειες για τη ρύθμιση του 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>

Κεφάλαιο 17. Σύστημα Ελέγχου Έκδοσης

Ο έλεγχος Έκδοσης είναι η τέχνη του να ελέγχετε αλλαγές στις πληροφορίες. Είναι εδώ και καιρό ένα κρίσιμο εργαλείο για προγραμματιστές, που τυπικά περνούν το χρόνο τους κάνοντας μικρές αλλαγές σε λογισμικό και μετά αναιρώντας τις την επόμενη μέρα. Αλλά η χρησιμότητα του λογισμικού ελέγχου εκδόσεως επεκτείνεται πέρα από τα σύνορα του κόσμου ανάπτυξης. Όπου μπορείτε να βρείτε ανθρώπους που χρησιμοποιούν υπολογιστές για να διαχειρίζονται πληροφορίες που αλλάζουν συχνά, υπάρχει χώρος για το έλεγχο έκδοσης.

1. Bazaar

Το Bazaar είναι μια καινούρια έκδοση του συστήματος ελέγχου έκδοσης που χορηγείται από την Canonical, τη διαφημιστική εταιρία πίσω από το Ubuntu. Σε αντίθεση με τα Subversion και CVS που υποστηρίζουν μόνο ένα κεντρικό μοντέλο αποθετηρίου, το Bazaar υποστηρίζει επίσης *διανεμόμενο έλεγχο έκδοσης*, δίνοντας τη δυνατότητα πιο αποτελεσματικής διαδικασίας. Συγκεκριμένα, το Bazaar είναι σχεδιασμένο να μεγιστοποιεί το επίπεδο συμμετοχής στην κοινότητα σε έργα ανοιχτού κώδικα.

1.1. Εγκατάσταση

Σε ένα τερματικό εντολών, πληκτρολογήστε την ακόλουθη εντολή για να εγκαταστήσετε το bzt:

```
sudo apt-get install bzt
```

1.2. Ρυθμίσεις

Για να συστήσετε τον εαυτό σας στο bzt, χρησιμοποιείτε την εντολή *whoami* έτσι:

```
$ bzt whoami 'Joe Doe <joe.doe@gmail.com>'
```

1.3. Μαθαίνοντας

Το Bazaar έρχεται με βοηθητικές οδηγίες εγκατεστημένες εξορισμού στο `/usr/share/doc/bzt/html`. Το εγχειρίδιο οδηγιών είναι ένα καλό μέρος να ξεκινήσετε. Η εντολή *bzt* έρχεται επίσης με ενσωματωμένη βοήθεια:

```
$ bzt help
```

Για να μάθετε περισσότερα για την εντολή *foo*:

```
$ bzt help foo
```

1.4. Ενσωμάτωση Εκκινητή

Ενώ είναι ιδιαίτερα χρήσιμο σαν ένα αυτόνομο σύστημα, το Bazaar καλή, προαιρετική ενσωμάτωση με το *Launchpad*¹, τη συνεργατική ανάπτυξη συστήματος που χρησιμοποιείται από την Canonical και την ευρύτερη κοινότητα ανοιχτού κώδικα για να διαχειριστεί και να επεκτείνει το Ubuntu. Για πληροφορίες στο πως μπορεί το Bazaar να χρησιμοποιηθεί με το Launchpad για να συνεργαστούν σε ένα έργο ανοιχτού κώδικα, δείτε το <http://bazaar-vcs.org/LaunchpadIntegration>².

¹ <https://launchpad.net/>

² <http://bazaar-vcs.org/LaunchpadIntegration/>

2. Subversion

Το Subversion είναι μία έκδοση ανοικτού κώδικα του συστήματος ελέγχου έκδοσης. Χρησιμοποιώντας το Subversion, μπορείτε να καταγράψετε το ιστορικό αρχείων πηγής και αρχείων. Διαχειρίζεται αρχεία και καταλόγους σε πάροδο χρόνου. Ένα δέντρο αρχείων τοποθετείτε σε ένα κεντρικό αποθετήριο. Το αποθετήριο είναι σαν ένας κανονικός διακομιστής αρχείων, με τη διαφορά ότι θυμάται κάθε αλλαγή που έγινε σε αρχεία και καταλόγους.

2.1. Εγκατάσταση

Για να έχετε πρόσβαση στο αποθετήριο του Subversion χρησιμοποιώντας πρωτόκολλο HTTP, πρέπει να εγκαταστήσετε και να διαμορφώσετε έναν διακομιστή ιστού. Ο Apache2 έχει αποδειχτεί ότι δουλεύει με το Subversion. Παρακαλώ αναφερθείτε στην υπο ενότητα HTTP στην ενότητα Apache2 για να εγκαταστήσετε και να διαμορφώσετε τον Apache2. Για να έχετε πρόσβαση στο αποθετήριο του Subversion χρησιμοποιώντας πρωτόκολλο HTTPS, πρέπει να εγκαταστήσετε και να διαμορφώσετε ένα ψηφιακό πιστοποιητικό στον διακομιστή ιστού Apache 2. Παρακαλώ αναφερθείτε στην υπο ενότητα HTTPS στην ενότητα Apache2 για να εγκαταστήσετε και να διαμορφώσετε το ψηφιακό πιστοποιητικό.

Για να εγκαταστήσετε το Subversion, εκτελέστε την ακόλουθη εντολή από ένα τερματικό εντολών:

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

2.2. Διαμόρφωση Διακομιστή

Αυτό το βήμα υποθέτει ότι έχετε εγκαταστήσει πακέτα που αναφέρθηκαν νωρίτερα στο σύστημά σας. Αυτή η ενότητα εξηγεί πως να δημιουργήσετε ένα αποθετήριο Subversion και να έχετε πρόσβαση στο έργο.

2.2.1. Δημιουργία Αποθετηρίου Subversion

Το αποθετήριο Subversion μπορεί να δημιουργηθεί χρησιμοποιώντας την ακόλουθη εντολή από ένα τερματικό εντολών:

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

2.2.2. Εισαγωγή Αρχείων

Αφού δημιουργήσετε ένα αποθετήριο μπορείτε να εισάγετε αρχεία στο αποθετήριο. Για να εισάγετε έναν κατάλογο, εισάγετε τα ακόλουθα από ένα τερματικό εντολών:

```
svn import /path/to/import/directory file:///path/to/repos/project
```

2.3. Μέθοδοι Πρόσβασης

Μπορείτε να έχετε πρόσβαση (ελέγξετε) τα αποθετήρια Subversion μέσω πολλών διαφορετικών μεθόδων --στον τοπικό δίσκο, ή μέσω διάφορων πρωτοκόλλων δικτύου. Μια τοποθεσία αποθετηρίου, όμως, είναι πάντα ένα URL. Ο πίνακας εξηγεί πως διαφορετικά σχέδια URL αντιδρούν στις διαθέσιμες μεθόδους πρόσβασης.

Πίνακας 17.1. Μέθοδοι Πρόσβασης

Σχήμα	Μέθοδος Πρόσβασης
file://	απευθείας πρόσβαση σε αποθετήριο (στον τοπικό δίσκο)
http://	Πρόσβαση μέσω πρωτοκόλλου WebDAV σε διακομιστή δικτύου Subversion-aware Apache2
https://	Όμοια με http://, αλλά με κρυπτογράφηση SSL
svn://	Πρόσβαση μέσω προσαρμοσμένου πρωτοκόλλου σε έναν διακομιστή svnserve
svn+ssh://	Όμοια με svn://, αλλά μέσω ενός τούνελ SSH

Σε αυτή την ενότητα, θα δούμε πως να διαμορφώσουμε το Subversion για όλες αυτές τις μεθόδους πρόσβασης. Εδώ, καλύπτουμε τα βασικά. Για περισσότερες ειδικές λεπτομέρειες χρήσης, αναφερθείτε στο *svn book*³.

2.3.1. Απευθείας πρόσβαση σε αποθετήριο (file://)

Αυτή είναι η πιο απλή μέθοδος πρόσβασης. Δεν απαιτεί καμία διαδικασία διακομιστή Subversion να εκτελείται. Αυτή η μέθοδος πρόσβασης, αν πληκτρολογηθεί σε ένα τερματικό εντολών, είναι όπως ακολουθεί:

```
svn co file:///path/to/repos/project
```

ή

```
svn co file://localhost/path/to/repos/project
```



Εάν δεν προσδιορίσετε το όνομα κεντρικού υπολογιστή, υπάρχουν τρεις κάθετοι (///) -- δύο για το πρωτόκολλο (αρχείο, σε αυτή την περίπτωση) και η πρώτη κάθετος στο μονοπάτι. Εάν προσδιορίσετε το όνομα κεντρικού υπολογιστή, πρέπει να χρησιμοποιήσετε δύο καθέτους (//).

Τα δικαιώματα του αποθετηρίου εξαρτώνται από τα δικαιώματα του συστήματος αρχείων. Εάν ο χρήστης έχει δικαιώματα ανάγνωσης/επεξεργασίας, μπορεί να ελέγξει και να παραδώσει στο αποθετήριο.

³ <http://svnbook.red-bean.com/>

2.3.2. Πρόσβαση μέσω πρωτοκόλλου WebDAV (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/default`, or another VirtualHost file:

```
<Location /svn>
DAV svn
SVNPath /home/svn
AuthType Basic
AuthName "Your repository name"
AuthUserFile /etc/subversion/passwd
Require valid-user
</Location>
```



Το παραπάνω απόσπασμα διαμόρφωσης υποθέτει ότι τα αποθέματα Subversion είναι δημιουργημένα στον κατάλογο `/home/svn/` χρησιμοποιώντας την εντολή **svnadmin**. Μπορούν να είναι προσβάσιμα χρησιμοποιώντας το url **http://hostname/svn/repos_name**.

Για να εισάγετε ή να παραδώσετε αρχεία στο αποθετήριο Subversion μέσω HTTP, το αποθετήριο θα πρέπει να ανήκει σε ένα χρήστη HTTP. Σε συστήματα Ubuntu, κανονικά ο χρήστης HTTP είναι **www-data**. Για να αλλάξετε την ιδιοκτησία των αρχείων του αποθετηρίου πληκτρολογήστε την ακόλουθη εντολή από ένα τερματικό εντολών:

```
sudo chown -R www-data:www-data /path/to/repos
```



Αλλάζοντας την ιδιοκτησία του αποθετηρίου σαν **www-data** δε θα μπορείτε να εισάγετε και να παραδίνετε αρχεία στο αποθετήριο εκτελώντας την εντολή **svn import file:///** ως οποιοσδήποτε χρήστης του **www-data**.

Μετά, πρέπει να δημιουργήσετε ένα αρχείο `/etc/subversion/passwd` που θα περιέχει λεπτομέρειες ταυτοποίησης χρήστη. Για να δημιουργήσετε ένα αρχείο χρησιμοποιήστε την ακόλουθη εντολή σε ένα τερματικό εντολών (η οποία θα δημιουργήσει το αρχείο και θα προσθέσει τον πρώτο χρήστη):

```
sudo htpasswd -c /etc/subversion/passwd user_name
```

Για να προσθέσετε επιπλέον χρήστες παραλείψτε την επιλογή `"-c"` καθώς αυτή η επιλογή αντικαθιστά το παλιό αρχείο. Αντί αυτής χρησιμοποιείτε αυτή τη μορφή:

```
sudo htpasswd /etc/subversion/passwd user_name
```

Αυτή η εντολή θα σας ζητήσει να εισάγετε τον κωδικό. Όταν εισάγετε τον κωδικό, ο χρήστης προστίθεται. Τώρα, για να έχετε πρόσβαση στο αποθετήριο μπορείτε να εκτελέσετε την ακόλουθη εντολή:

svn co http://servername/svn



Ο κωδικός μεταδίδεται σαν απλό κείμενο. Εάν ανησυχείτε για κατασκόπηση κωδικού, συνίσταται να χρησιμοποιήσετε κρυπτογράφηση SSL. Για λεπτομέρειες, παρακαλώ αναφερθείτε στην επόμενη ενότητα.

2.3.3. Πρόσβαση μέσω πρωτοκόλλου WebDAV με κρυπτογράφηση SSL (https://)

Πρόσβαση σε ένα αποθετήριο Subversion μέσω πρωτοκόλλου WebDAV με κρυπτογράφηση SSL (https://) είναι παρόμοια με του http:// εκτός του ότι πρέπει να εγκαταστήσετε και να διαμορφώσετε το ψηφιακό πιστοποιητικό στο διακομιστή ιστού Apache2. Για να χρησιμοποιήσετε SSL με Subversion προσθέστε την παραπάνω διαμόρφωση Apache2 στο /etc/apache2/sites-available/default-ssl. Για περισσότερες πληροφορίες στο πως να στήσετε τον Apache2 με SSL δείτε *Τμήμα 1.3, “Διαμόρφωση HTTPS” [207]*.

Μπορείτε να εγκαταστήσετε ψηφιακά πιστοποιητικά που έχουν εκδοθεί από μια αρχή υπογραφής. Εναλλακτικά, μπορείτε να εγκαταστήσετε τα δικά σας αυτο υπογεγραμμένα πιστοποιητικά.

Αυτό το βήμα υποθέτει ότι έχετε εγκαταστήσει και διαμορφώσει ένα ψηφιακό πιστοποιητικό στο διακομιστή ιστού σας Apache2. Τώρα, για να έχετε πρόσβαση στο αποθετήριο Subversion, παρακαλώ αναφερθείτε στην παραπάνω ενότητα! Οι μέθοδοι πρόσβασης είναι ακριβώς ίδιες, εκτός από το πρωτόκολλο. Πρέπει να χρησιμοποιήσετε https:// για να έχετε πρόσβαση στο αποθετήριο.

2.3.4. Πρόσβαση μέσω προσαρμοσμένου πρωτοκόλλου (svn://)

Όταν δημιουργηθεί το αποθετήριο Subversion, μπορείτε να διαμορφώσετε τον έλεγχο πρόσβασης. Μπορείτε να επεξεργαστείτε το αρχείο /path/to/repos/project/conf/svnserve.conf για να διαμορφώσετε τον έλεγχο πρόσβασης. Για παράδειγμα, για να προσδιορίσετε αυθεντικότητα, μπορείτε να διαγράψετε τα σχόλια των ακόλουθων γραμμών στο αρχείο διαμόρφωσης:

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

Αφού διαγράψετε τα σχόλια στις παραπάνω γραμμές, μπορείτε να διατηρήσετε τη λίστα χρηστών στο αρχείο passwd. Έτσι, επεξεργαστείτε το αρχείο passwd στον ίδιο κατάλογο και προσθέστε τον καινούριο χρήστη. Η σύνταξη είναι όπως ακολούθως:

```
username = password
```

Για περισσότερες λεπτομέρειες, παρακαλώ αναφερθείτε στο αρχείο.

Τώρα, για πρόσβαση του Subversion μέσω του προσαρμοσμένου πρωτοκόλλου svn://, είτε από την ίδια μηχανή ή από διαφορετική, μπορείτε να εκτελέσετε το svnserver χρησιμοποιώντας την εντολή svnserve. Η σύνταξη είναι όπως ακολούθως:

```
$ svnserve -d --foreground -r /path/to/repos
# -d -- κατάσταση δαίμονα
# --foreground -- εκτέλεση στο προσκήνιο (χρήσιμο για αποσφαλμάτωση)
# -r -- ρίζα του καταλόγου για εξυπηρέτηση
```

Για περισσότερες λεπτομέρειες χρήσης, παρακαλώ αναφερθείτε στο:
`$ svnserve --help`

Όταν εκτελέσετε αυτή την εντολή, το Subversion αρχίζει να ακούει στην προεπιλεγμένη θύρα (3690). Για να έχετε πρόσβαση στο αποθετήριο του έργου, πρέπει να εκτελέσετε την ακόλουθη εντολή από ένα τερματικό εντολών:

```
svn co svn://hostname/project project --username user_name
```

Βάση της διαμόρφωσης του διακομιστή, ζητάει κωδικό. Όταν πιστοποιήσετε την ταυτότητά σας, ελέγχει τον κώδικα από το αποθετήριο Subversion. Για να συγχρονίσετε το αποθετήριο του έργου με το τοπικό αντίγραφο, μπορείτε να εκτελέσετε την υπο-εντολή **update**. Η σύνταξη της εντολής, αν πληκτρολογηθεί σε ένα τερματικό, είναι όπως ακολουθεί:

```
cd project_dir ; svn update
```

Για περισσότερες λεπτομέρειες για το πως να χρησιμοποιήσετε κάθε υπο-εντολή Subversion, μπορείτε να αναφερθείτε στο εγχειρίδιο. Για παράδειγμα, για να μάθετε περισσότερα για την εντολή `co` (checkout) παρακαλώ εκτελέστε την ακόλουθη εντολή από ένα τερματικό εντολών:

```
svn co help
```

2.3.5. Πρόσβαση μέσω προσαρμοσμένου πρωτοκόλλου με κρυπτογράφηση SSL (svn+ssh://)

Η διαμόρφωση και η διαδικασία διακομιστή είναι ίδιες με τη μέθοδο `svn://`. Για λεπτομέρειες, παρακαλώ αναφερθείτε στην παραπάνω ενότητα. Αυτό το βήμα υποθέτει ότι έχετε ακολουθήσει τα παραπάνω βήματα και έχετε εκκινήσει τον διακομιστή Subversion χρησιμοποιώντας την εντολή `svnserve command`.

Επίσης υποτίθεται ότι ο διακομιστής `ssh` εκτελείται σε εκείνη τη μηχανή και ότι επιτρέπει εισερχόμενες συνδέσεις. Για να το επιβεβαιώσετε, παρακαλώ δοκιμάστε να συνδεθείτε σε εκείνη τη μηχανή χρησιμοποιώντας `ssh`. Εάν μπορείτε να συνδεθείτε όλα είναι τέλεια. Εάν δεν μπορείτε να συνδεθείτε, παρακαλώ διευθετήστε το πριν συνεχίσετε παρακάτω.

Το πρωτόκολλο `svn+ssh://` χρησιμοποιείται για πρόσβαση στο αποθετήριο Subversion χρησιμοποιώντας SSL κρυπτογράφηση. Τα δεδομένα μεταφοράς είναι κρυπτογραφημένα χρησιμοποιώντας αυτή τη μέθοδο. Για να έχετε πρόσβαση στο αποθετήριο του έργου (για παράδειγμα με `checkout`), πρέπει να χρησιμοποιήσετε τη σύνταξη της ακόλουθης εντολής:

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



Πρέπει να χρησιμοποιήσετε το πλήρες μονοπάτι (/path/to/repos/project) για να έχετε πρόσβαση στο αποθετήριο Subversion χρησιμοποιώντας αυτή τη μέθοδο πρόσβασης.

Βάση της διαμόρφωσης του διακομιστή, ζητάει κωδικό. Πρέπει να εισάγετε τον κωδικό που χρησιμοποιείτε για να εισέλθετε μέσω ssh. Μόλις πιστοποιήσετε την ταυτότητά σας, ελέγχει τον κώδικα από το αποθετήριο Subversion.

3. Διακομιστής CVS

Το CVS είναι ένα σύστημα ελέγχου έκδοσης. Μπορείτε να το χρησιμοποιείτε για να καταγράφετε το ιστορικό αρχείων πηγής.

3.1. Εγκατάσταση

Για να εγκαταστήσετε το CVS, εκτελέστε την ακόλουθη εντολή από το τερματικό εντολών:

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

Αφού εγκαταστήσετε το cvs, πρέπει να εγκαταστήσετε το xinetd για να εκκινείτε/τερματίζετε το διακομιστή cvs. Όταν σας ζητηθεί, εισάγετε την ακόλουθη εντολή για να εγκαταστήσετε το xinetd:

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

3.2. Ρυθμίσεις

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

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

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

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



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

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

sudo service xinetd restart

Μπορείτε να επιβεβαιώσετε ότι ο διακομιστής CVS εκτελείτε χρησιμοποιώντας την ακόλουθη εντολή:

sudo netstat -tap | grep cvs

Όταν εκτελείτε αυτή την εντολή, θα πρέπει να δείτε τις ακόλουθες γραμμές ή κάτι παρόμοιο:

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

Από εδώ μπορείτε να συνεχίσετε να προσθέσετε χρήστες, να προσθέσετε καινούρια έργα, και να διαχειριστείτε το διακομιστή CVS.



Το CVS επιτρέπει στο χρήστη να εισάγει χρήστες ανεξάρτητα από την υποκείμενη εγκατάσταση λειτουργικού συστήματος. Πιθανόν ο πιο εύκολος τρόπος είναι να χρησιμοποιήσετε Χρήστες Linux για CVS, παρόλο που έχει πιθανά θέματα ασφαλείας. Παρακαλώ αναφερθείτε στο εγχειρίδιο CVS για λεπτομέρειες.

3.3. Προσθήκη Έργων

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

cd your/project

**cvs -d :pserver:username@hostname.com:/srv/cvs import -m **
"Importing my project to CVS repository" . new_project start



Μπορείτε να χρησιμοποιήσετε τη μεταβλητή περιβάλλοντος CVSROOT για να αποθηκεύσετε τον κατάλογο βάσης CVS. Όταν εξάγετε της μεταβλητή περιβάλλοντος CVSROOT, μπορείτε να αποφύγετε τη χρήση της επιλογής -d στην παραπάνω εντολή cvs.

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



When you add a new project, the CVS user you use must have write access to the CVS repository (/srv/cvs). By default, the src group has write access to the CVS repository. So, you can add the user to this group, and he can then add and manage projects in the CVS repository.

4. Αναφορές

*Κεντρική Σελίδα Bazaar*⁴

*Εκκινητής*⁵

*Κεντρική Σελίδα Subversion*⁶

*Βιβλίο Subversion*⁷

*Εγχειρίδιο CVS*⁸

*Easy Bazaar Ubuntu Wiki page*⁹

*Ubuntu Wiki Subversion page*¹⁰

⁴ <http://bazaar.canonical.com/en/>

⁵ <https://launchpad.net/>

⁶ <http://subversion.tigris.org/>

⁷ <http://svnbook.red-bean.com/>

⁸ http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs_toc.html

⁹ <https://help.ubuntu.com/community/EasyBazaar>

¹⁰ <https://help.ubuntu.com/community/Subversion>

Κεφάλαιο 18. Samba

Τα δίκτυα υπολογιστών συχνά αποτελούνται από διαφορετικά συστήματα, και ενώ ένα λειτουργικό δίκτυο που αποτελείται εξολοκλήρου από υπολογιστές desktop και server Ubuntu θα ήταν σίγουρα διασκεδαστικό, μερικά περιβάλλοντα δικτύων πρέπει να αποτελούνται από συστήματα Ubuntu και Microsoft®Windows® που εργάζονται αρμονικά μαζί. Αυτό το τμήμα του οδηγού Ubuntu Server εισάγει αρχές και εργαλεία που χρησιμοποιούνται για τη ρύθμιση του Ubuntu Server για κοινή χρήση των πόρων του δικτύου με Windows υπολογιστές.

1. Εισαγωγή

Η επιτυχημένη δικτύωση του Ubuntu συστήματός σας με πελάτες Windows περιλαμβάνει την παροχή και την ενσωμάτωση με τις υπηρεσίες που είναι κοινές στα Windows περιβάλλοντα. Οι εν λόγω υπηρεσίες βοηθούν την ανταλλαγή δεδομένων και πληροφοριών σχετικά με τους υπολογιστές και τους χρήστες που συμμετέχουν στο δίκτυο, και μπορούν να ταξινομηθούν σε τρεις μεγάλες κατηγορίες λειτουργιών:

- **Υπηρεσία Διαμοίρασης Αρχείου και Εκτυπωτή.** Χρησιμοποίηση του πρωτοκόλλου Server Message Block (SMB) για τη διευκόλυνση της ανταλλαγής αρχείων, φακέλων, τόμων, καθώς και την από κοινού χρήση των εκτυπωτών σε όλο το δίκτυο.
- **Υπηρεσίες Καταλόγου.** Κοινή χρήση πληροφοριών ζωτικής σημασίας σχετικά με τους υπολογιστές και τους χρήστες του δικτύου με τεχνολογίες όπως το πρωτόκολλο Lightweight Directory Access (LDAP) και το Microsoft Active Directory®.
- **Πιστοποίηση και Πρόσβαση.** Καθιέρωση της ταυτότητας ενός χρήστη ή υπολογιστή του δικτύου και καθορισμός της πληροφορίας ο υπολογιστής ή ο χρήστης επιτρέπεται να έχει πρόσβαση χρησιμοποιώντας αρχές και τεχνολογίες όπως άδειες αρχείων, πολιτικές ομάδων, και την υπηρεσία ελέγχου ταυτότητας Kerberos.

Ευτυχώς, το Ubuntu σύστημά σας μπορεί να παρέχει όλες αυτές τις εγκαταστάσεις για να τους πελάτες των Windows και να μοιράζει πόρους δικτύου μεταξύ τους. Ένα από τα κύρια κομμάτια του λογισμικού που περιλαμβάνει το σύστημα Ubuntu για τη δικτύωση των Windows είναι η σουίτα Samba του server εφαρμογών και εργαλείων SMB.

Αυτό το τμήμα του Οδηγού Ubuntu Server θα εισαγάγει ορισμένες από τις συνήθειες περιπτώσεις χρήσης Samba, και πώς να εγκαταστήσετε και να ρυθμίσετε τα απαραίτητα πακέτα. Πρόσθετες λεπτομερές βοηθητικές οδηγίες και πληροφορίες για το Samba μπορούν να βρεθούν στο *Samba website*¹.

¹ <http://www.samba.org>

2. File Server

Ένας από τους πιο σύνηθες τρόπους να δικτυωθούν υπολογιστές Ubuntu και Windows είναι να ρυθμιστεί το Samba ως Διακομιστής Αρχείου. Αυτή η ενότητα καλύπτει τη δημιουργία ενός Samba διακομιστή για τη κοινή χρήση αρχείων με πελάτες Windows.

Ο διακομιστής θα ρυθμιστεί ώστε να μοιράζει αρχεία με κάθε πελάτη του δικτύου χωρίς να ζητάει κωδικό πρόσβασης. Εάν το περιβάλλον σας απαιτεί πιο αυστηρό Έλεγχο Εισόδου βλ. *Τμήμα 4, “Securing File and Print Server” [308]*

2.1. Εγκατάσταση

Το πρώτο βήμα είναι να εγκαταστήσετε το πακέτο samba. Από ένα τερματικό εντολών πληκτρολογήστε:

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

Αυτό είναι όλο, είστε τώρα έτοιμη να ρυθμίσετε το Samba να διαμοιράζει αρχεία.

2.2. Ρυθμίσεις

Το κύριο αρχείο ρύθμισης του Samba βρίσκεται στο `/etc/samba/smb.conf`. Το αρχικό αρχείο ρυθμίσεων έχει ένα σημαντικό αριθμό παρατηρήσεων, προκειμένου να τεκμηριώσει διάφορες οδηγίες διαμόρφωσης.



Δεν περιλαμβάνονται όλες οι διαθέσιμες επιλογές στο αρχικό αρχείο ρυθμίσεων. Βλέπε τη σελίδα `smb.confman` ή *Samba HOWTO Collection*² για περισσότερες πληροφορίες.

1. Πρώτον, επεξεργαστείτε τα ακόλουθα ζεύγη κλειδιών / τιμών στον τομέα `[global]` του `/etc/samba/smb.conf`:

```
workgroup = EXAMPLE
...
security = user
```

Η παράμετρος `security` είναι πιο κάτω στον τομέα `[global]`, και σχολιάζετε με προεπιλογή. Επίσης, αλλάξτε το `EXAMPLE` ώστε να ταιριάζει καλύτερα με το περιβάλλον σας.

2. Δημιουργήστε ένα κενό τμήμα στο κάτω μέρος του αρχείου, ή διαγράψτε το σχόλιο κάποιου από τα παραδείγματα, για να μοιράζεται ο κατάλογος.

```
[share]
comment = Ubuntu File Server Share
```

² <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/>

```
path = /srv/samba/share
browsable = yes
guest ok = yes
read only = no
create mask = 0755
```

- *comment*: μια μικρή περιγραφή του διαμοιραζόμενου. Ρυθμίστε το ώστε να ταιριάζει στις ανάγκες σας.
- *path*: το μονοπάτι του καταλόγου που θέλετε να διαμοιράσετε.

Αυτό το παράδειγμα χρησιμοποιεί `/srv/samba/sharename` επειδή, σύμφωνα με το *Filesystem Hierarchy Standard (FHS)*, `/srv`³ εκεί πρέπει να εξυπηρετούνται πληροφορίες σχετικές με site. Τεχνικώς τα διαμοιραζόμενα του Samba μπορούν να τοποθετηθούν οπουδήποτε στο σύστημα αρχείων αρκεί τα δικαιώματα να είναι σωστά, αλλά συνίσταται τήρηση των προτύπων.

- *browsable*: επιτρέπει στους πελάτες των Windows να περιηγηθούν τον κοινόχρηστο κατάλογο χρησιμοποιώντας το Windows Explorer.
 - *guest ok*: επιτρέπει στους πελάτες να συνδεθούν στα κοινόχρηστα χωρίς να παρέχουν έναν κωδικό.
 - *read only*: καθορίζει εάν το διαμοιραζόμενο είναι μόνο για ανάγνωση ή αν παρέχονται προνόμια επεξεργασίας. Τα προνόμια επεξεργασίας παρέχονται μόνο όταν η τιμή είναι *όχι*, όπως φαίνεται σε αυτό το παράδειγμα. Εάν η τιμή είναι *ναι*, τότε η πρόσβαση στο διαμοιραζόμενο είναι μόνο για ανάγνωση.
 - *create mask*: καθορίζει τις άδειες που θα έχουν τα καινούρια αρχεία όταν δημιουργηθούν.
3. Τώρα που το Samba έχει ρυθμιστεί, ο κατάλογος πρέπει να δημιουργηθεί και η άδειες να αλλαχτούν. Από ένα τερματικό πληκτρολογείτε:

```
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. Τέλος, επανεκκινήστε των υπηρεσιών του samba για να ενεργοποιηθούν οι νέες ρυθμίσεις:

```
sudo restart smbd
sudo restart nmbd
```



Για άλλη μια φορά, η ανωτέρω ρύθμιση δίνει πρόσβαση σε κάθε πελάτη του τοπικού δικτύου. Για μια πιο ασφαλή ρύθμιση βλ. *Τμήμα 4, «Securing File and Print Server»*; [308].

³ <http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM>

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.

Για να δημιουργήσετε επιπλέον διαμοιραζόμενα απλά δημιουργήστε καινούρια τμήματα *[dir]* στο */etc/samba/smb.conf*, και επανεκκινήστε το *Samba*. Απλά σιγουρευτείτε ότι ο κατάλογος που θέλετε να μοιραστείτε υπάρχει και οι άδειες είναι σωστές.



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. Πόροι

- Για διαμορφώσεις του Samba σε βάθος δείτε το *Samba HOWTO Collection*⁴
- Ο οδηγός είναι επίσης διαθέσιμος σε *έντυπη μορφή*⁵.
- *Χρησιμοποιώντας το Samba*⁶ του O'Reilly είναι άλλη μια καλή παραπομπή.
- Η σελίδα wiki του *Ubuntu για το Samba*⁷.

⁴ <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/>

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. Διακομιστής Εκτύπωσης

Μια άλλη κοινή χρήση του Samba είναι η διαμόρφωσή του ώστε να διαμοιράζει εγκατεστημένους εκτυπωτές είτε τοπικά είτε μέσω του διαδικτύου, σε έναν διακομιστή Ubuntu. Παρόμοια με το *Τμήμα 2, “File Server” [303]* αυτό το τμήμα θα διαμορφώσει το Samba ώστε να επιτρέπει σε κάθε πελάτη στο τοπικό δίκτυο να χρησιμοποιεί τους εγκατεστημένους εκτυπωτές χωρίς να ζητά όνομα χρήστη και κωδικό πρόσβασης.

Για μια πιο ασφαλή διαμόρφωση βλ. *Τμήμα 4, “Securing File and Print Server” [308]*.

3.1. Εγκατάσταση

Πριν εγκαταστήσετε και διαμορφώσετε το Samba είναι καλό να έχετε ήδη μια λειτουργική εγκατάσταση CUPS. Δείτε *Τμήμα 4, “CUPS - Εξυπηρετητής Εκτυπώσεων” [252]* για λεπτομέρειες.

Για να εγκαταστήσετε το πακέτο samba, από ένα τερματικό πληκτρολογήστε:

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

3.2. Ρυθμίσεις

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
```

Στο τμήμα *[printers]* αλλάξτε την επιλογή *επισκέπτες* σε *yes*:

```
browsable = yes
guest ok = yes
```

Μετά την επεξεργασία του `smb.conf` επανεκκινήστε το Samba:

```
sudo restart smbd
sudo restart nmbd
```

Η προεπιλεγμένη ρύθμιση του Samba θα διαμοιράσει αυτόματα τους εγκατεστημένους εκτυπωτές. Απλά εγκαταστήστε τοπικά τον εκτυπωτή στους πελάτες των Windows.

3.3. Πόροι

- Για διαμορφώσεις του Samba σε βάθος δείτε το *Samba HOWTO Collection*⁸
- Ο οδηγός είναι επίσης διαθέσιμος σε *έντυπη μορφή*⁹.
- *Χρησιμοποιώντας το Samba*¹⁰ του O'Reilly είναι άλλη μια καλή παραπομπή.
- Επίσης δείτε το *CUPS Website*¹¹ για περισσότερες πληροφορίες για τη διαμόρφωση CUPS.
- Η σελίδα wiki του *Ubuntu για το Samba*¹².

⁸ <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/>

⁹ <http://www.amazon.com/exec/obidos/tg/detail/-/0131882228>

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. Καταστάσεις Ασφάλειας Samba

Υπάρχουν δύο επίπεδα ασφάλειας διαθέσιμα στο πρωτόκολλο δικτύου Common Internet Filesystem (CIFS) *user-level* και *share-level*. Η εκτέλεση της *security mode* του Samba επιτρέπει μεγαλύτερη ευελιξία, παρέχοντας τέσσερις τρόπους εφαρμογής ασφάλειας επιπέδου-χρήστη και έναν τρόπο εφαρμογής επιπέδου-διαμοιρασμού:

- *security = user*: απαιτεί από τους πελάτες να παρέχουν ένα όνομα χρήστη και κωδικό πρόσβασης για να συνδεθούν στα διαμοιραζόμενα. Οι λογαριασμοί χρηστών του Samba είναι διαφορετικοί από τους λογαριασμούς συστήματος, αλλά το πακέτο `libram-smbrpass` θα συγχρονίσει τους χρήστες και τους κωδικούς συστήματος με τη βάση δεδομένων χρηστών του Samba.
- *security = domain*: αυτή η κατάσταση επιτρέπει στο διακομιστή του Samba να εμφανίζεται στους πελάτες των Windows σαν Πρωτεύον Ελεγκτής Τομέα (Primary Domain Controller (PDC)), Εφεδρικός Ελεγκτής Τομέα (Backup Domain Controller (BDC)), ή Τμήμα Μέλους Διακομιστή (Domain Member Server (DMS)). Δείτε *Τμήμα 5, “As a Domain Controller” [313]* για περισσότερες πληροφορίες.
- *security = ADS*: επιτρέπει στο διακομιστή Samba να συνδεθεί στον τομέα Ενεργού Καταλόγου σαν ένα ιθαγενές μέλος. Δείτε *Τμήμα 6, “Active Directory Integration” [318]* για λεπτομέρειες.
- *security = server*: αυτή η κατάσταση έχει απομείνει από τότε που το samba δεν μπορούσε να γίνει μέλος ενός διακομιστή, και εξαιτίας ορισμένων θεμάτων ασφαλείας δεν πρέπει να χρησιμοποιείται. Δείτε το τμήμα του οδηγού Samba *Ασφάλεια Διακομιστή*¹³ για περισσότερες πληροφορίες.
- *security = share*: επιτρέπει στους πελάτες να συνδεθούν στα διαμοιραζόμενα χωρίς να παρέχουν ένα όνομα χρήστη και κωδικό πρόσβασης.

Η κατάσταση ασφαλείας που επιλέγεται θα βασίζεται στο περιβάλλον σας και στο τι χρειάζεστε να πετύχει ο διακομιστής Samba.

4.2. Security = User

Αυτό το τμήμα θα επαναδιαμορφώσει το αρχείο και το διακομιστή εκτυπωτή Samba, από *Τμήμα 2, “File Server” [303]* και *Τμήμα 3, “Διακομιστής Εκτύπωσης” [306]*, ώστε να απαιτεί πιστοποίηση.

Πρώτον, εγκαταστήστε το πακέτο `libram-smbrpass` το οποίο θα συγχρονίσει τους χρήστες του συστήματος στη βάση δεδομένων χρηστών του Samba:

¹³ <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html#id349531>

sudo apt-get install libpam-smbpass



Εάν επιλέξατε τη διεργασία *Διακομιστής Samba* κατά τη διάρκεια της εγκατάστασης τότε το `libpam-smbpass` είναι ήδη εγκατεστημένο.

Επεξεργαστείτε το `/etc/samba/smb.conf`, και στον τομέα *[διαμοιρασμένο]* αλλάξτε:

```
guest ok = no
```

Τέλος, επανεκκινήστε το Samba για να τεθούν σε ισχύ οι νέες ρυθμίσεις:

sudo restart smbd

sudo restart nmbd

Τώρα όταν συνδέεστε στους κοινόχρηστους καταλόγους ή εκτυπωτές θα σας ζητείται όνομα χρήστη και κωδικός.



Αν επιλέξετε να αντιστοιχίσετε μια μονάδα δίσκου στο διαμοιραζόμενο μπορείτε να τσεκάρετε το κουτί επιλογής `“Επανασύνδεση κατά την Είσοδο”`, το οποίο θα σας ζητήσει να εισάγετε το όνομα χρήστη και τον κωδικό πρόσβασης μία φορά, τουλάχιστον μέχρι να αλλάξει ο κωδικός.

4.3. Ασφάλεια Διαμοιραζόμενου

Υπάρχουν πολλές διαθέσιμες επιλογές για να αυξήσετε την ασφάλεια για κάθε μεμονωμένο κοινόχρηστο κατάλογο. Χρησιμοποιώντας το παράδειγμα *[share]*, αυτό το τμήμα θα καλυψει ορισμένες κοινές επιλογές.

4.3.1. Ομάδες

Οι ομάδες ορίζουν μια συλλογή από υπολογιστές ή χρήστες οι οποίοι έχουν ένα κοινό επίπεδο πρόσβασης σε συγκεκριμένους πόρους δικτύου και προσφέρουν ένα επίπεδο διακριτότητας για τον έλεγχο της πρόσβασης σε αυτούς τους πόρους. Για παράδειγμα, αν μια ομάδα *qa* ορίζεται και περιέχει τους χρήστες *freda*, *danika*, και *rob* και μια δεύτερη ομάδα *support* έχει οριστεί και περιέχει τους χρήστες *danika*, *jeremy*, και *vincent* τότε συγκεκριμένοι πόροι του δικτύου διαμορφωμένοι για να επιτρέπουν την είσοδο στην ομάδα *qa* ακολούθως θα επιτρέψει την είσοδο στους *freda*, *danika*, και *rob*, αλλά όχι στους *jeremy* ή *vincent*. Δεδομένου ότι ο χρήστης *danika* ανήκει και στην ομάδα *qa* και στην *support*, θα μπορεί να χρησιμοποιεί πόρους διαμορφωμένους για πρόσβαση και από τις δύο ομάδες, ενώ όλοι οι άλλοι χρήστες έχουν πρόσβαση μόνο σε πόρους που επιτρέπουν πρόσβαση στην ομάδα στην οποία ανήκουν.

Από προεπιλογή το Samba αναζητά τις τοπικές ομάδες συστήματος που ορίζονται στο `/etc/group` για να καθορίσει ποιοι χρήστες ανήκουν σε ποιες ομάδες. Για περισσότερες

πληροφορίες για εισαγωγή και διαγραφή χρηστών από ομάδες βλ. *Τμήμα 1.2, “Προσθήκη και Διαγραφή Χρηστών” [161]*.

Όταν ορίζετε ομάδες στο αρχείο διαμόρφωσης του Samba, `/etc/samba/smb.conf`, η αναγνωρισμένη σύνταξη είναι να προλογίσετε το όνομα της ομάδας με ένα σύμβολο `"@"`. Για παράδειγμα, εάν επιθυμούσατε να ορίσετε μια ομάδα με όνομα *sysadmin* σε ένα συγκεκριμένο τμήμα του `/etc/samba/smb.conf`, θα το κάνατε εισάγοντας το όνομα της ομάδας ως **@sysadmin**.

4.3.2. Άδειες Αρχείων

Οι Άδειες Αρχείων ορίζουν τα σαφή δικαιώματα που έχει ένας υπολογιστής ή χρήστης σε έναν συγκεκριμένο κατάλογο, αρχείο, ή σύνολο αρχείων. Τέτοιες άδειες μπορούν να οριστούν κάνοντας επεξεργασία του αρχείου `/etc/samba/smb.conf` και ορίζοντας τις σαφείς άδειες ενός ορισμένου διαμοιρασμένου αρχείου.

Για παράδειγμα, εάν έχετε ορίσει ένα διαμοιρασμένο του Samba με όνομα *share* και επιθυμείτε να δώσετε άδειες *read-only* στην ομάδα χρηστών γνωστών ως *qa*, αλλά θέλετε να επιτρέπετε την επεξεργασία του διαμοιραζόμενου από την ομάδα που ονομάζεται *sysadmin* και τον χρήστη με όνομα *vincent*, τότε θα μπορούσατε να επεξεργαστείτε το αρχείο `/etc/samba/smb.conf`, και να εισάγετε τις ακόλουθες τιμές κάτω από την εγγραφή *[share]*:

```
read list = @qa
write list = @sysadmin, vincent
```

Μια άλλη πιθανή άδεια του Samba είναι να δηλώσετε δικαιώματα *διαχειριστή* σε ένα συγκεκριμένο διαμοιρασμένο πόρο. Οι χρήστες που έχουν δικαιώματα διαχειριστή μπορούν να διαβάσουν, να επεξεργαστούν και τροποποιήσουν κάθε πληροφορία που περιέχεται στον πόρο για τον οποίο έχουν δοθεί στο χρήστη σαφή δικαιώματα διαχειριστή.

Για παράδειγμα, εάν θέλετε να δώσετε στο χρήστη *melissa* δικαιώματα διαχειριστή για το παράδειγμα *share*, θα επεξεργαζόσασταν το αρχείο `/etc/samba/smb.conf`, και θα εισάγατε την ακόλουθη γραμμή κάτω από την εγγραφή *[διαμοιραζόμενο]*:

```
admin users = melissa
```

Αφού επεξεργαστείτε το `/etc/samba/smb.conf`, επανεκκινήστε το Samba για να εφαρμοστούν οι αλλαγές:

```
sudo restart smbd
sudo restart nmbd
```



Για να δουλέψουν οι λίστες ανάγνωσης και λίστες επεξεργασίας η κατάσταση ασφαλείας του Samba δεν πρέπει να καθοριστεί σε *ασφάλεια* = *διαμοιραζόμενο*

Τώρα που το Samba έχει ρυθμιστεί έτσι ώστε να περιορίσει ποιες ομάδες έχουν πρόσβαση στο κοινόχρηστο κατάλογο, θα πρέπει τα δικαιώματα του συστήματος αρχείου να ενημερωθούν.

Τα παραδοσιακά δικαιώματα αρχείων του Linux δεν λειτουργούν καλά με τον Λίστα Ελέγχου Πρόσβασης (Access Control Lists (ACLs)) των Windows NT. Ευτυχώς οι POSIX ACLs είναι διαθέσιμες για διακομιστές Ubuntu παρέχοντας καλύτερο έλεγχο. Για παράδειγμα, για να ενεργοποιήσετε τις ACLs στο /srv ένα αρχείο συστήματος EXT3, επεξεργαστείτε το /etc/fstab εισάγοντας την επιλογή *acl*:

```
UUID=66bcdd2e-8861-4fb0-b7e4-e61c569fe17d /srv ext3 noatime,relatime,acl 0 1
```

Μετά κάντε ξανά mount το διαμέρισμα:

```
sudo mount -v -o remount /srv
```



Το παραπάνω παράδειγμα υποθέτει το /srv σε διαφορετικό διαμέρισμα. Εάν το /srv, ή όπου αλλού έχετε ρυθμίσει το κοινόχρηστο μονοπάτι, είναι μέρος του διαμερίσματος / μια επανεκκίνηση μπορεί να απαιτείται.

Για να ταιριάζετε τη παραπάνω ρύθμιση του Samba στην ομάδα *sysadmin* θα δοθούν δικαιώματα ανάγνωσης, επεξεργασίας και εκτέλεσης στο /srv/samba/share, στην ομάδα *qa* θα δοθούν δικαιώματα ανάγνωσης και εκτέλεσης, και τα αρχεία θα ανήκουν στο όνομα χρήστη *melissa*. Πληκτρολογήστε τα ακόλουθα στο τερματικό:

```
sudo chown -R melissa /srv/samba/share/
sudo chgrp -R sysadmin /srv/samba/share/
sudo setfacl -R -m g:qa:rx /srv/samba/share/
```



Η παραπάνω εντολή setfacl δίνει δικαιώματα *εκτέλεσης* σε όλα τα αρχεία του καταλόγου /srv/samba/share, κάτι το οποίο μπορεί να θέλετε ή να μην θέλετε.

Τώρα από έναν πελάτη των Windows θα πρέπει παρατηρήσετε ότι τα νέα δικαιώματα αρχείων είναι σε εφαρμογή. Δείτε τις σελίδες *acl* και *setfacl* για περισσότερες πληροφορίες πάνω στις POSIX ACLs.

4.4. Προφίλ Samba AppArmor

Το Ubuntu έρχεται με την υπομονάδα ασφαλείας AppArmor, η οποία παρέχει υποχρεωτικούς ελέγχους πρόσβασης. Το προεπιλεγμένο προφίλ AppArmor για το Samba θα χρειαστεί να προσαρμοστεί στη ρύθμισή σας. Για περισσότερες πληροφορίες στο πως να χρησιμοποιήσετε το AppArmor βλ. *Τμήμα 4, “AppArmor” [176]*.

Υπάρχουν προεπιλεγμένα προφίλ του AppArmor για τα /usr/sbin/smbd και /usr/sbin/nmbd, για τα daemon binaries του Samba, σαν μέρος των πακέτων apparmor-profiles. Για να εγκαταστήσετε το πακέτο, από ένα τερματικό εντολών πληκτρολογήστε:

sudo apt-get install apparmor-profiles apparmor-utils



Αυτό το πακέτο περιέχει προφίλ για πολλά άλλα binaries.

Από προεπιλογή τα προφίλ για τα `smbd` και `nmdbd` βρίσκονται σε κατάσταση *complain* επιτρέποντας στο Samba να δουλεύει χωρίς να τροποποιεί το προφίλ, και μόνο να καταγράφει σφάλματα. Για να τοποθετήσετε το προφίλ `smbd` σε κατάσταση *enforce*, και να δουλεύει το Samba όπως αναμένεται, το προφίλ θα χρειαστεί να επεξεργαστεί ώστε να αντικατοπτρίζει όλους τους καταλόγους που χρησιμοποιούνται.

Επεξεργαστείτε το `/etc/apparmor.d/usr.sbin.smbd` εισάγοντας πληροφορίες για *[share]* από το αρχείο παραδείγματος του διακομιστή:

```
/srv/samba/share/ r,  
/srv/samba/share/** rwkix,
```

Τώρα τοποθετήστε το προφίλ σε κατάσταση *enforce* και επαναφορτώστε το:

```
sudo aa-enforce /usr/sbin/smbd  
cat /etc/apparmor.d/usr.sbin.smbd | sudo apparmor_parser -r
```

Θα πρέπει τώρα να μπορείτε να διαβάσετε, να επεξεργαστείτε και να εκτελέσετε αρχεία στον κοινόχρηστο κατάλογο όπως πάντα, και το binary `smbd` θα έχει πρόσβαση μόνο σε ρυθμισμένα αρχεία και καταλόγους. Σιγουρευτείτε να εισάγετε εγγραφές για κάθε κατάλογο που ρυθμίζετε για να διαμοιράσει το Samba. Επίσης, όποια λάθη θα καταγραφούν στο `/var/log/syslog`.

4.5. Πόροι

- Για διαμορφώσεις του Samba σε βάθος δείτε το *Samba HOWTO Collection*¹⁴
- Ο οδηγός είναι επίσης διαθέσιμος σε *έντυπη μορφή*¹⁵.
- Το *Χρησιμοποιώντας το Samba*¹⁶ του O'Reilly είναι μια καλή παραπομπή.
- Το *Κεφάλαιο 18*¹⁷ του Samba HOWTO Collection είναι αφιερωμένο στην ασφάλεια.
- Για περισσότερες πληροφορίες για το Samba και το ACLs δείτε το *Samba ACLs page*¹⁸.
- Η σελίδα wiki του *Ubuntu για το Samba*¹⁹.

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>

¹⁹ <https://help.ubuntu.com/community/Samba>

5. As a Domain Controller

Παρόλο που δεν μπορεί να λειτουργήσει σαν ένας Ελεγκτής Τομέα Ενεργού Καταλόγου (Active Directory Primary Domain Controller (PDC)), ένας διακομιστής Samba μπορεί να ρυθμιστεί να εμφανίζεται σαν ένας ελεγκτής τομέα σε συλ Windows NT4. Ένα μείζων πλεονέκτημα αυτής της ρύθμισης είναι η ικανότητα να συγκεντρώνει τις πιστοποιήσεις του χρήστη και της μηχανής. Το Samba μπορεί επίσης να χρησιμοποιεί πολλαπλά προγράμματα υποστήριξης για να αποθηκεύει τις πληροφορίες του χρήστη.

5.1. Κύριος Ελεγκτής Τομέα

Αυτή η ενότητα καλύπτει τη ρύθμιση του Samba σαν ένα Κύριο Ελεγκτή Τομέα (Primary Domain Controller (PDC)) χρησιμοποιώντας το προεπιλεγμένο πρόγραμμα υποστήριξης `smbpasswd`.

1. Πρώτον, εγκαταστήστε τα Samba, και `libram-smbpass` για να συγχρονίσετε τους λογαριασμούς χρηστών, πληκτρολογώντας τα ακόλουθα σε ένα τερματικό εντολών:

```
sudo apt-get install samba libram-smbpass
```

2. Μετά, ρυθμίστε το Samba τροποποιώντας το `/etc/samba/smb.conf`. Η κατάσταση *ασφάλεια* θα πρέπει να τεθεί σε *χρήστης*, και η *ομάδα εργασίας* θα πρέπει να ταιριάζει στον οργανισμό σας:

```
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
```



Εάν επιθυμείτε να μη χρησιμοποιήσετε το *Roaming Profiles* αφήστε τις επιλογές *logon home* και *logon path* με σχόλια.

- *domain logons*: παρέχει την υπηρεσία `netlogon` που επιτρέπει το Samba να συμπεριφέρεται σαν ελεγκτής τομέα

- *logon path*: τοποθετεί το προφίλ χρήστη των Windows στον αρχικό τους κατάλογο. Επίσης είναι δυνατό να ρυθμιστεί ένα διαμοιρασμένο *[profiles]* για να τοποθετηθούν όλα τα προφίλ σε ένα κατάλογο.
- *logon drive*: προσδιορίζει το τοπικό μονοπάτι του αρχικού καταλόγου.
- *logon home*: προσδιορίζει την τοποθεσία του αρχικού καταλόγου
- *logon script*: καθορίζει το σενάριο που θα εκτελεστεί τοπικά όταν ένας χρήστη εισέρχεται. Το σενάριο χρειάζεται να τοποθετηθεί στο διαμοιρασμένο *[netlogon]*.
- *add machine script*: ένα σενάριο το οποίο αυτόματα θα δημιουργήσει το *Machine Trust Account* που χρειάζεται ώστε ένας σταθμός εργασίας να εισέλθει στον τομέα.

Σε αυτό το παράδειγμα η ομάδα *machines* θα χρειαστεί να δημιουργηθεί χρησιμοποιώντας την λειτουργία *addgroup* δείτε το *Τμήμα 1.2, Προσθήκη και Διαγραφή Χρηστών*; [161] για λεπτομέρειες.

4. Διαγράψτε τα σχόλια του διαμοιρασμένου *[homes]* για να επιτραπεί η αντιστοίχιση στο *logon home*:

```
[homes]
comment = Home Directories
browseable = no
read only = no
create mask = 0700
directory mask = 0700
valid users = %S
```

5. Όταν ρυθμιστεί σαν ελεγκτής τομέα ένα διαμοιρασμένο *[netlogon]* χρειάζεται να ρυθμιστεί. Για να ενεργοποιήσετε το διαμοιρασμένο, διαγράψτε τα σχόλια:

```
[netlogon]
comment = Network Logon Service
path = /srv/samba/netlogon
guest ok = yes
read only = yes
share modes = no
```



Το αρχικό μονοπάτι του διαμοιρασμένου *netlogon* είναι */home/samba/netlogon*, αλλά σύμφωνα με την Πρότυπη Ιεραρχία Αρχείων Συστήματος (Filesystem Hierarchy Standard (FHS)), */srv*²⁰ είναι η σωστή τοποθεσία για δεδομένα σχετικά με site που παρέχεται από το σύστημα.

6. Τώρα δημιουργήστε τον κατάλογο *netlogon* , και ένα άδειο (για τώρα) αρχείο σεναρίου *logon.cmd* :

```
sudo mkdir -p /srv/samba/netlogon
```

²⁰ <http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM>


```
sudo touch /srv/samba/netlogon/logon.cmd
```

Μπορείτε να εισάγετε οποιεσδήποτε εντολές σεναρίου των Windows στο logon.cmd για να προσαρμόσετε το περιβάλλον του πελάτη.

7. Επανεκκίνηση του Samba για να μπορέσει ο νέος τομέας να ελέγξει:

```
sudo restart smbd
sudo restart nmbd
```

8. Τελευταία, υπάρχουν μερικές πρόσθετες εντολές που απαιτούνται για την εγκατάσταση των σωστών δικαιωμάτων.

Με το *root* να είναι απενεργοποιημένο από προεπιλογή, για να εισέλθει ένας σταθμός εργασίας στον τομέα, μια ομάδα συστήματος πρέπει να αντιστοιχηθεί στην ομάδα των Windows *Domain Admins*. Χρησιμοποιώντας τη λειτουργία *net*, πληκτρολογήστε από ένα τερματικό:

```
sudo net groupmap add ntgroup="Domain Admins" unixgroup=sysadmin rid=512 type=d
```



Αλλάξτε το *sysadmin* σε όποια ομάδα προτιμάτε. Επίσης, ο χρήστης που χρησιμοποιείται για να εισέλθει στον τομέα πρέπει να είναι μέλος της ομάδας *sysadmin*, καθώς και μέλος της ομάδας συστήματος *admin*. Η ομάδα *admin* επιτρέπει τη χρήση του *sudo*.

Εάν ο χρήστης δεν έχει τα πιστοποιητικά του Samba ακόμη, μπορείτε να τα προσθέσετε με το βοηθητικό πρόγραμμα *smbpasswd*, αλλάζοντας το όνομα χρήστη *sysadmin* κατάλληλα:

```
sudo smbpasswd -a sysadmin
```

Επίσης, πρέπει να δοθούν ρητά δικαιώματα στην ομάδα *Domain Admins* (

```
net rpc rights grant -U sysadmin "EXAMPLE\Domain Admins" SeMachineAccountPrivilege \
SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege \
SeRemoteShutdownPrivilege
```

9. Θα μπορείτε τώρα να προσχωρήσετε πελάτες των Windows στον Τομέα με τον ίδιο τρόπο που τους προσχωρείτε σε έναν τομέα NT4 που τρέχει σε διακομιστή Windows.

5.2. Ελεγκτής Τομέα Αντιγράφου Ασφαλείας

Με έναν Κύριο Ελεγκτή Τομέα (Primary Domain Controller (PDC)) στο δίκτυο είναι καλύτερο να έχετε έναν Ελεγκτή Τομέα Αντιγράφου Ασφαλείας (Backup Domain Controller (BDC)) επίσης. Αυτό θα επιτρέπει στους πελάτες πιστοποιούνται σε περίπτωση που ο Κύριος Ελεγκτής Τομέα δεν είναι διαθέσιμος.

Όταν ρυθμίζετε το Samba σαν Ελεγκτή Τομέα Αντιγράφου Ασφαλείας χρειάζεται έναν τρόπο να συγχρονίζετε τις πληροφορίες λογαριασμών με τον Κύριο Ελεγκτή Τομέα. Υπάρχουν πολλοί τρόποι για να το πετύχετε αυτό `scp`, `rsync`, ή χρησιμοποιώντας το LDAP ως *passdb backend*.

Η χρησιμοποίηση του LDAP είναι ο πιο αυτοδύναμος τρόπος να συγχρονίσετε τις πληροφορίες λογαριασμού, επειδή και οι δύο ελεγκτές τομέα μπορούν να χρησιμοποιήσουν τις ίδιες πληροφορίες σε πραγματικό χρόνο. Παρόλα αυτά, το να στήσετε έναν διακομιστή LDAP μπορεί να είναι πού περίπλοκο για ένα μικρό νούμερο χρηστών και λογαριασμών υπολογιστών. Δείτε *Τμήμα 2, Samba και LDAP*; [123] για λεπτομέρειες.

1. Πρώτα, εγκαταστήστε τα `samba` και `libpam-smbpass`. Από ένα τερματικό πληκτρολογήστε:

```
sudo apt-get install samba libpam-smbpass
```

2. Τώρα, επεξεργαστείτε το `/etc/samba/smb.conf` και διαγράψτε τα σχόλια στο ακόλουθο *[global]*:

```
workgroup = EXAMPLE
...
security = user
```

3. Στο σχολιασμένο *Domains* διαγράψτε τα σχόλια ή προσθέστε:

```
domain logons = yes
domain master = no
```

4. Σιγουρευτείτε ότι ένας χρήστης έχει δικαιώματα ανάγνωσης των αρχείων στο `/var/lib/samba`. Για παράδειγμα, για να επιτρέπεται στους χρήστες στην ομάδα *admin* να `scp` τα αρχεία, πληκτρολογήστε:

```
sudo chgrp -R admin /var/lib/samba
```

5. Μετά, συγχρονίστε τους λογαριασμούς χρηστών, χρησιμοποιώντας το `scp` για να αντιγράψετε τον κατάλογο `/var/lib/samba` από τον Κύριο Ελεγκτή Τομέα:

```
sudo scp -r username@pdc:/var/lib/samba /var/lib
```



Αντικαταστήστε το *username* με ένα έγκυρο όνομα χρήστη και *pdc* με το όνομα του κεντρικού υπολογιστή ή την IP διεύθυνση του κανονικού Κύριου Ελεγκτή Τομέα.

6. Τέλος, επανεκκινήστε το `samba`:

```
sudo restart smbd
```

sudo restart nmbd

Μπορείτε να ελέγξετε ότι ο Ελεγκτής Τομέα Αντιγράφου Ασφαλείας δουλεύει σταματώντας το Samba daemon στον Κύριο Ελεγκτή Τομέα, μετά προσπαθώντας να εισέλθετε σε έναν πελάτη των Windows που έχει προσχωρηθεί στον τομέα.

Κάτι άλλο που πρέπει να θυμάστε είναι αν ρυθμίσατε την επιλογή *logon home* σαν κατάλογο στον Κύριο Ελεγκτή Τομέα, και αυτός γίνει μη διαθέσιμος, η πρόσβαση στην μονάδα του χρήστη *Home* θα είναι επίσης μη διαθέσιμη. Για αυτό το λόγο είναι καλύτερο να ρυθμίσετε το *logon home* να βρίσκεται σε έναν ξεχωριστό διακομιστή από τον Κύριο Ελεγκτή Τομέα και τον Ελεγκτή Τομέα Αντιγράφου Ασφαλείας.

5.3. Πόροι

- Για διαμορφώσεις του Samba σε βάθος δείτε το *Samba HOWTO Collection*²¹
- Ο οδηγός είναι επίσης διαθέσιμος σε *έντυπη μορφή*²².
- Το *Χρησιμοποιώντας το Samba*²³ του O'Reilly είναι μια καλή παραπομπή.
- Το *Κεφάλαιο 4*²⁴ του Samba HOWTO Collection εξηγεί πως να στήσετε ένα Κύριο Ελεγκτή Τομέα.
- Το *Κεφάλαιο 5*²⁵ του Samba HOWTO Collection εξηγεί πως να στήσετε έναν Ελεγκτή Τομέα Αντιγράφου Ασφαλείας.
- Η σελίδα wiki του *Ubuntu για το Samba*²⁶.

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. Πρόσβαση ενός Διαμοιρασμένου Samba

Μια άλλη χρήση του Samba είναι να ενοποιείται με ένα ήδη υπάρχων δίκτυο των Windows. Όταν είναι μέλος ενός τομέα Ενεργού Καταλόγου, το Samba μπορεί να παρέχει υπηρεσίες αρχείων και εκτύπωσης σε χρήστες Ενεργού Καταλόγου.

The simplest way to join an AD domain is to use Likewise-open. For detailed instructions see the *Likewise Open documentation*²⁷.

Όταν εμφανιστεί ένα τμήμα του τομέα Active Directory πληκτρολογήστε την ακόλουθη εντολή στην προτροπή τερματικού:

```
sudo apt-get install samba smbfs smbclient
```

Μετά, επεξεργαστείτε το `/etc/samba/smb.conf` αλλάζοντας τα:

```
workgroup = EXAMPLE
...
security = ads
realm = EXAMPLE.COM
...
idmap backend = ldapsd
idmap uid = 50-999999999
idmap gid = 50-999999999
```

Επανεκκινήστε το `samba` για να ενεργοποιηθούν οι καινούριες ρυθμίσεις:

```
sudo restart smbd
sudo restart nmbd
```

Θα πρέπει τώρα να είστε ικανοί να έχετε πρόσβαση σε κάθε διαμοιρασμένο του Samba από έναν πελάτη των Windows. Παρόλα αυτά, σιγουρευτείτε ότι δώσατε δώσατε πρόσβαση στους κατάλληλους χρήστες ή ομάδες του Ενεργού Καταλόγου στον διαμοιρασμένο κατάλογο. Δείτε το *Τμήμα 4, “Securing File and Print Server” [308]* για περισσότερες λεπτομέρειες.

6.2. Πρόσβαση σε ένα Διαμοιρασμένο των Windows

Τώρα που ο διακομιστής Samba είναι μέρος του τομέα Ενεργού Καταλόγου μπορείτε να έχετε πρόσβαση σε διαμοιρασμένα διακομιστή των Windows:

- Για να κάνετε mount ενός διαμοιρασμένου των Windows πληκτρολογήστε τα ακόλουθα σε ένα τερματικό εντολών:

²⁷ <http://www.beyondtrust.com/Technical-Support/Downloads/files/pbiso/Manuals/ubuntu-active-directory.html>

```
mount.cifs //fs01.example.com/share mount_point
```

Είναι επίσης δυνατό να έχετε πρόσβαση σε διαμοιρασμένα σε υπολογιστές που δεν είναι μέρος ενός τομέα Ενεργού Καταλόγου, αλλά πρέπει να δοθεί ένα όνομα χρήστη και κωδικός πρόσβασης.

- Για να κάνετε mount του διαμοιραζόμενου κατά την εκκίνηση του συστήματος τοποθετήστε μια εγγραφή στο `/etc/fstab`, για παράδειγμα:

```
//192.168.0.5/share /mnt/windows cifs auto,username=steve,password=secret,rw 0 0
```

- Ένας άλλος τρόπος για να αντιγράψετε τα αρχεία από έναν διακομιστή των Windows είναι να χρησιμοποιήσετε τη λειτουργία `smbclient`. Για να απαριθμήσετε τα αρχεία σε ένα διαμοιραζόμενο των Windows:

```
smbclient //fs01.example.com/share -k -c "ls"
```

- Για να αντιγράψετε από ένα διαμοιραζόμενο, πληκτρολογήστε:

```
smbclient //fs01.example.com/share -k -c "get file.txt"
```

Αυτό θα αντιγράψει το `file.txt` στον τρέχων κατάλογο.

- Και για να αντιγράψετε ένα αρχείο στο διαμοιραζόμενο:

```
smbclient //fs01.example.com/share -k -c "put /etc/hosts hosts"
```

Αυτό θα αντιγράψει το `/etc/hosts` στο `//fs01.example.com/share/hosts`.

- Η επιλογή `-c` που χρησιμοποιήθηκε παραπάνω σας επιτρέπει να εκτελέσετε την εντολή `smbclient` με τη μία. Αυτό είναι χρήσιμο για τη δημιουργία σεναρίου και για μικρές λειτουργίες αρχείων. Για να εισάγετε την εντολή `smb: |>`, μια εντολή σαν FTP που επιτρέπει την εκτέλεση κανονικών αρχείων και εντολών καταλόγων, απλά εκτελέστε:

```
smbclient //fs01.example.com/share -k
```



Αντικαταστήστε όλες τις περιπτώσεις των `fs01.example.com/share`, `//192.168.0.5/share`, `username=steve,password=secret`, και `file.txt` με την IP του διακομιστή σας, το όνομα υπολογιστή, το κοινόχρηστο όνομα, το όνομα αρχείου, και ένα πραγματικό όνομα χρήστη και κωδικό με δικαιώματα στο διαμοιραζόμενο.

6.3. Πόροι

For more `smbclient` options see the man page: **man `smbclient`**, also available *online*²⁸.

²⁸ <http://manpages.ubuntu.com/manpages/raring/en/man1/smbclient.1.html>

The `mount.cifs` *man page*²⁹ is also useful for more detailed information.

Η σελίδα wiki του *Ubuntu* για το *Samba*³⁰.

²⁹ <http://manpages.ubuntu.com/manpages/raring/en/man8/mount.cifs.8.html>

³⁰ <https://help.ubuntu.com/community/Samba>

Κεφάλαιο 19. Αντίγραφα ασφαλείας

Υπάρχουν πολλοί τρόποι για την διατήρηση αντιγράφων ασφαλείας μιας εγκατάστασης Ubuntu. Το πιο σημαντικό πράγμα για τα αντίγραφα ασφαλείας είναι η ανάπτυξη ενός *σχεδίου δημιουργίας αντιγράφων ασφαλείας* που να περιέχει τι θα αντιγραφεί, πού θα αντιγραφεί, και πώς θα γίνεται η επαναφορά του.

Οι παρακάτω ενότητες περιέχουν διάφορους τρόπους πραγματοποίησης αυτών των εργασιών.

1. Σενάρια εντολών κελύφους

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. Απλό σενάριο εντολών κελύφους

Το παρακάτω σενάριο εντολών κελύφους χρησιμοποιεί το tar για να δημιουργήσει ένα συμπιεσμένο αρχείο σε ένα απομακρυσμένο σύστημα αρχείων NFS που έχει προσαρτηθεί. Το όνομα του αρχείου προσδιορίζεται με τη χρήση επιπλέον εργαλείων γραμμής εντολών.

```
#!/bin/sh
#####
#
# Σενάριο εντολών δημιουργίας αντιγράφων ασφαλείας σε NFS.
#
#####

# Τι θα αντιγραφεί.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Πού θα δημιουργηθεί το αντίγραφο ασφαλείας.
dest="/mnt/backup"

# Δημιουργία του ονόματος του αρχείου.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Εμφάνιση μηνύματος έναρξης.
echo "Δημιουργείται αντίγραφο των αρχείων $backup_files στο $dest/$archive_file"
date
echo

# Δημιουργία αντιγράφου των αρχείων με τη χρήση του tar.
tar czf $dest/$archive_file $backup_files

# Εμφάνιση μηνύματος ολοκλήρωσης.
echo
echo "Η διαδικασία δημιουργίας αντιγράφου ασφαλείας ολοκληρώθηκε"
date

# Εμφάνιση λεπτομερούς λίστας των αρχείων στο $dest για τον έλεγχο του μεγέθους των αρχείων.
```


ls -lh \$dest

- *\$backup_files*: μια μεταβλητή που περιέχει τους καταλόγους από τους οποίους θέλετε να κρατήσετε αντίγραφο ασφαλείας. Η λίστα θα πρέπει να προσαρμοστεί ώστε να ταιριάζει στις ανάγκες σας.
- *\$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*: μεταβλητή που περιέχει το σύντομο όνομα του συστήματος. Προσθέτοντας το όνομα του συστήματος στο όνομα του αρχείου, σας δίνεται η επιλογή να τοποθετείτε καθημερινά αρχεία, από πολλά συστήματα, στον ίδιο κατάλογο.
- *\$archive_file*: το πλήρες όνομα του αρχείου.
- *\$dest*: destination of the archive file. The directory needs to be created and in this case *mounted* before executing the backup script. See *Τμήμα 2, Σύστημα Αρχείων Δικτύου (NFS)* [247] for details of using NFS.
- *μηνύματα κατάστασης*: προαιρετικά μηνύματα που εμφανίζονται στην κονσόλα χρησιμοποιώντας το εργαλείο echo.
- *tar czf \$dest/\$archive_file \$backup_files*: η εντολή tar που χρησιμοποιείται για τη δημιουργία του αρχείου.
 - *c*: δημιουργεί ένα αρχείο.
 - *z*: περνάει το αρχείο μέσα από το εργαλείο gzip, συμπιέζοντας έτσι το αρχείο.
 - *f*: output to an archive file. Otherwise the tar output will be sent to STDOUT.
- *ls -lh \$dest*: προαιρετική εντολή που εμφανίζει μια πλήρη λίστα (-l) σε φιλική προς τον άνθρωπο μορφή (-h) των αρχείων του καταλόγου προορισμού. Αυτό είναι χρήσιμο για έναν γρήγορο έλεγχο του μεγέθους του αρχείου. Αυτός ο έλεγχος δεν θα πρέπει να αντικαθιστά τον έλεγχο του αρχείου.

This is a simple example of a backup shell script; however there are many options that can be included in such a script. See *Τμήμα 1.4, Αναφορές* [325] for links to resources providing more in-depth shell scripting information.

1.2. Εκτέλεση του σεναρίου εντολών

1.2.1. Εκτέλεση από τερματικό

Ο απλούστερος τρόπος για να εκτελέσετε το παραπάνω σενάριο εντολών δημιουργίας αντιγράφων ασφαλείας είναι να αντιγράψετε τα περιεχόμενα σε ένα αρχείο, `backup.sh` για παράδειγμα. Μετά από ένα τερματικό, εκτελέστε:

```
sudo bash backup.sh
```

Αυτός είναι ένας πολύ καλός τρόπος για να ελέγξετε το σενάριο εντολών ώστε να σιγουρευτείτε πως τα πάντα δουλεύουν όπως περιμένετε.

1.2.2. Εκτέλεση με το cron

Το εργαλείο cron μπορεί να χρησιμοποιηθεί για την αυτοματοποίηση της εκτέλεσης του σεναρίου εντολών. Η υπηρεσία cron, επιτρέπει την εκτέλεση σεναρίων εντολών, ή εντολών, κάποια συγκεκριμένη ώρα και ημερομηνία.

Το cron ρυθμίζεται μέσα από καταχωρήσεις σε ένα αρχείο crontab. Τα αρχεία crontab χωρίζονται σε πεδία:

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*: η ημέρα του μήνα την οποία εκτελείται η εντολή.
- *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*: η εντολή που θα εκτελεστεί.

Για να προσθέσετε ή να τροποποιήσετε καταχωρήσεις σε ένα αρχείο crontab, θα πρέπει να χρησιμοποιηθεί η εντολή crontab -e. Επίσης, το περιεχόμενο ενός αρχείου crontab μπορεί να προβληθεί χρησιμοποιώντας την εντολή crontab -l.

Για να εκτελέσετε το σενάριο εντολών backup.sh που υπάρχει παραπάνω χρησιμοποιώντας το cron, πληκτρολογήστε το ακόλουθο σε ένα τερματικό:

sudo crontab -e



Χρησιμοποιώντας το sudo με την εντολή crontab -e, επεξεργάζεστε το crontab του χρήστη root. Αυτό είναι απαραίτητο αν δημιουργείτε αντίγραφα ασφαλείας καταλόγων που έχει πρόσβαση μόνο ο χρήστης root.

Προσθέστε την ακόλουθη καταχώρηση στο αρχείο crontab:

```
# m h dom mon dow command
0 0 * * * bash /usr/local/bin/backup.sh
```

Το σενάριο εντολών backup.sh θα εκτελείται τώρα κάθε μέρα στις 12:00 π.μ.



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 *Τμήμα 1.4, “Αναφορές” [325]*.

1.3. Επαναφορά από το αρχείο

Μόλις ένα αρχείο δημιουργηθεί, είναι σημαντικό να το ελέγξετε. Μπορείτε να ελέγξετε το αρχείο βλέποντας τα αρχεία που περιέχει, αλλά ο καλύτερος έλεγχος είναι να **επαναφέρετε** ένα αρχείο από το συμπιεσμένο αρχείο.

- To see a listing of the archive contents. From a terminal prompt type:

```
tar -tzvf /mnt/backup/υπολογιστής-Δευτέρα.tgz
```

- Για να επαναφέρετε ένα αρχείο από το συμπιεσμένο αρχείο σε έναν διαφορετικό κατάλογο, πληκτρολογήστε:

```
tar -xzf /mnt/backup/υπολογιστής-Δευτέρα.tgz -C /tmp etc/hosts
```

Η επιλογή `-C` στο `tar`, κατευθύνει τα αποσυμπιεσμένα αρχεία στον προσδιορισμένο κατάλογο. Το παραπάνω παράδειγμα θα αποσυμπιέσει το αρχείο `/etc/hosts` στο `/tmp/etc/hosts`. Το `tar` επαναδημιουργεί τη δομή καταλόγων που περιέχει.

Επίσης, παρατηρήστε πως η αρχική `"/` δεν συμπεριλαμβάνεται στη διαδρομή του αρχείου που θα επαναφερθεί.

- Για να επαναφέρετε όλα τα αρχεία που υπάρχουν στο συμπιεσμένο αρχείο, πληκτρολογήστε τα ακόλουθα:

```
cd /  
sudo tar -xzf /mnt/backup/υπολογιστής-Δευτέρα.tgz
```



Αυτό θα αντικαταστήσει τα τρέχοντα αρχεία στο σύστημα αρχείων.

1.4. Αναφορές

- Για περισσότερες πληροφορίες σχετικά με τα σενάρια εντολών κελύφους, δείτε τον *οδηγό προχωρημένων σεναρίων εντολών Bash*¹
- Το βιβλίο *Teach Yourself Shell Programming in 24 Hours*² είναι διαθέσιμο στο διαδίκτυο και είναι μια σπουδαία πηγή για σενάρια εντολών κελύφους.
- Η *σελίδα Wiki του CronHowto*³ περιέχει λεπτομέρειες για προχωρημένες επιλογές του `cron`.
- Δείτε το *εγχειρίδιο του GNU tar*⁴ για περισσότερες επιλογές του `tar`.
- The Wikipedia *Backup Rotation Scheme*⁵ article contains information on other backup rotation schemes.

¹ <http://tldp.org/LDP/abs/html/>

² <http://safari.sampublishing.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

- Το σενάριο εντολών κελύφους χρησιμοποιεί το `tar` για να δημιουργήσει το αρχείο, αλλά υπάρχουν πολλά άλλα εργαλεία γραμμής εντολών που μπορούν να χρησιμοποιηθούν. Για παράδειγμα:
 - *cpio*⁶: χρησιμοποιείται για την αντιγραφή αρχείων προς και από συμπιεσμένα αρχεία.
 - *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.

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 *Τμήμα 1, Σενάρια εντολών κελύφους* [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.

Αυτό είναι το νέο σενάριο εντολών:

```
#!/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/
```

Το σενάριο μπορεί να εκτελεστεί χρησιμοποιώντας τις ίδιες μεθόδους όπως στο *Τμήμα 1.2, “Εκτέλεση του σεναρίου εντολών”* [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. Συσκευές κασέτας

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.

Αυτό είναι το σενάριο κελύφους τροποποιημένο ώστε να χρησιμοποιεί μια συσκευή κασέτας:

```
#!/bin/bash
#####
#
# Σενάριο δημιουργίας αντιγράφων ασφαλείας σε συσκευή κασέτας.
#
#####

# Τι θα αντιγραφεί.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Πού θα δημιουργηθεί το αντίγραφο ασφαλείας.
dest="/dev/st0"

# Εμφάνιση μηνύματος έναρξης.
echo "Δημιουργείται αντίγραφο των αρχείων $backup_files στο $dest"
date
echo

# Επιβεβαίωση πως η κασέτα έχει γυριστεί στην αρχή.
mt -f $dest rewind

# Δημιουργία αντιγράφου των αρχείων με τη χρήση του tar.
tar czf $dest $backup_files

# Γύρισμα της κασέτας στην αρχή και εξαγωγή της.
mt -f $dest rewoffl

# Εμφάνιση μηνύματος ολοκλήρωσης.
echo
echo "Η δημιουργία αντιγράφου ασφαλείας ολοκληρώθηκε"
date
```



Το προεπιλεγμένο όνομα για μία συσκευή κασέτας SCSI είναι `/dev/st0`.

Χρησιμοποιήστε την κατάλληλη διαδρομή συσκευής για το σύστημά σας.

Η επαναφορά από μία συσκευή δισκέτας είναι βασικά το ίδιο με την επαναφορά από ένα αρχείο. Απλά γυρίστε την κασέτα στην αρχή και χρησιμοποιήστε τη διαδρομή της

συσκευής αντί για μία διαδρομή αρχείου. Για παράδειγμα για να επαναφέρετε το αρχείο /etc/hosts στο /tmp/etc/hosts εκτελέστε τα ακόλουθα:

```
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. Επισκόπηση

Bacula is made up of several components and services used to manage which files to backup and backup locations:

- Bacula Director: μια υπηρεσία που ελέγχει όλες τις εργασίες αντιγράφων ασφαλείας, επαναφοράς, επαλήθευσης και αρχείων.
- Bacula Console: μια εφαρμογή που επιτρέπει την επικοινωνία με το Director. Υπάρχουν τρεις εκδόσεις του Console:
 - Έκδοση γραμμής εντολών που βασίζεται σε κείμενο.
 - Γραφικό περιβάλλον χρήστη (GUI) GTK+ που βασίζεται στο Gnome.
 - Γραφικό περιβάλλον (GUI) wxWidgets.
- Bacula File: επίσης γνωστό ως το πρόγραμμα Bacula Client. Αυτή η εφαρμογή εγκαθίσταται σε μηχανήματα από τα οποία θα δημιουργηθούν αντίγραφα ασφαλείας και είναι υπεύθυνο για τα δεδομένα που ζητούνται από το Director.
- Bacula Storage: τα προγράμματα που πραγματοποιούν την αποθήκευση και την επαναφορά αρχείων στα φυσικά μέσα.
- Bacula Catalog: είναι υπεύθυνο για την διατήρηση των ευρετηρίων των αρχείων και των βάσεων δεδομένων των τόμων για όλα τα αρχεία για τα οποία διατηρούνται αντίγραφα ασφαλείας, επιτρέποντας γρήγορο εντοπισμό και επαναφορά των αρχειοθετημένων αρχείων. Το Catalog υποστηρίζει τρεις διαφορετικές βάσεις δεδομένων: MySQL, PostgreSQL και SQLite.
- Bacula Monitor: επιτρέπει την παρακολούθηση του Director, των υπηρεσιών του File και του Storage. Προς το παρόν, το Monitor είναι διαθέσιμο μόνο ως εφαρμογή με γραφικό περιβάλλον GTK+.

Αυτές οι υπηρεσίες και εφαρμογές μπορούν να εκτελεστούν σε πολλούς εξυπηρετητές και πελάτες, ή μπορούν να εγκατασταθούν σε ένα μηχάνημα, αν κρατάτε αντίγραφα ασφαλείας ενός μόνο δίσκου ή τόμου.

3.2. Εγκατάσταση



If using MySQL or PostgreSQL as your database, you should already have the services available. Bacula will not install them for you.

Υπάρχουν πολλά πακέτα που περιέχουν τα διαφορετικά μέρη του Bacula. Για να εγκαταστήσετε το Bacula, σε ένα τερματικό πληκτρολογήστε:

sudo apt-get install bacula

Από προεπιλογή, εγκαθιστώντας το πακέτο bacula, θα χρησιμοποιηθεί μια βάση δεδομένων MySQL για τον κατάλογο. Αν θέλετε να χρησιμοποιήσετε SQLite ή PostgreSQL, για τον κατάλογο, εγκαταστήστε το bacula-director-sqlite3 ή το bacula-director-pgsql αντίστοιχα.

Κατά τη διαδικασία εγκατάστασης, θα σας ζητηθεί να δώσετε πιστοποιητικά για τον *διαχειριστή* της βάσης δεδομένων και για τον *ιδιοκτήτη* της βάσης δεδομένων του bacula. Ο διαχειριστής της βάσης δεδομένων θα πρέπει να έχει τα κατάλληλα δικαιώματα για να δημιουργήσει μια βάση δεδομένων. Δείτε το *Τμήμα 1, MySQL [222]* για περισσότερες πληροφορίες.

3.3. Ρυθμίσεις

Τα αρχεία ρυθμίσεων του Bacula είναι μορφοποιημένα βάσει των καταχωρήσεων που περιλαμβάνουν *οδηγίες* μέσα σε αγκύλες `{}`. Κάθε μέρος του Bacula έχει ένα ξεχωριστό αρχείο στον κατάλογο `/etc/bacula`.

Τα διάφορα μέρη του Bacula πρέπει να εξουσιοδοτηθούν μεταξύ τους. Αυτό επιτυγχάνεται με τη χρήση της οδηγίας κωδικού πρόσβασης *password*. Για παράδειγμα, ο κωδικός πρόσβασης της καταχώρησης *Storage* στο αρχείο `/etc/bacula/bacula-dir.conf` πρέπει να είναι ο ίδιος με αυτόν της καταχώρησης *Director* στο `/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"
}
```



Το παραπάνω παράδειγμα αλλάζει το όνομα της εργασίας σε *BackupServer* που είναι το όνομα του μηχανήματος. Αντικαταστήστε το `BackupServer` με το κατάλληλο όνομα υπολογιστή, ή με κάποιο άλλο περιγραφικό όνομα.

Το *Console* μπορεί να χρησιμοποιηθεί για να λάβετε πληροφορίες από το *Director* για εργασίες, αλλά για να χρησιμοποιήσετε το Console με έναν χρήστη *μη-root*, ο χρήστης θα πρέπει να είναι στην ομάδα *bacula*. Για να προσθέσετε έναν χρήστη στην ομάδα bacula πληκτρολογήστε τα ακόλουθα σε ένα τερματικό:

sudo adduser \$username bacula



Αντικαταστήστε το *\$username* με το πραγματικό όνομα χρήστη. Επίσης, αν προσθέσετε τον τρέχοντα χρήστη στην ομάδα, θα πρέπει να αποσυνδεθείτε και να επανασυνδεθείτε για να ισχύσουν τα νέα δικαιώματα.

3.4. Αντίγραφα ασφαλείας του τοπικού υπολογιστή

Αυτή η ενότητα περιγράφει πώς να δημιουργήσετε αντίγραφα ασφαλείας συγκεκριμένων καταλόγων ενός υπολογιστή σε μια τοπική συσκευή κασέτας.

- Πρώτα, η συσκευή *αποθήκευσης* πρέπει να ρυθμιστεί. Επεξεργαστείτε το `/etc/bacula/bacula-sd.conf` και προσθέστε:

```
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.

Μπορείτε επίσης να αποσχολιάσετε κάποιο από τα άλλα παραδείγματα στο αρχείο.

- Αφού επεξεργαστείτε το `/etc/bacula/bacula-sd.conf`, η υπηρεσία *Storage* θα πρέπει να επανεκκινηθεί:

sudo service bacula-sd restart

- Τώρα προσθέστε μία καταχώρηση *Storage* στο `/etc/bacula/bacula-dir.conf` για να χρησιμοποιήσετε τη νέα συσκευή:

```
# 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
```

```
}
```

Η οδηγία *Address* πρέπει να είναι το Πλήρως πιστοποιημένο όνομα τομέα (FQDN) του εξυπηρετητή. Αλλάξτε το *backupserver* με το πραγματικό όνομα του υπολογιστή.

Επίσης, σιγουρευτείτε πως η οδηγία *Password* είναι ίδια με τον κωδικό πρόσβασης στο `/etc/bacula/bacula-sd.conf`.

- Δημιουργήστε ένα νέο *FileSet*, που θα καθορίσει για ποιους καταλόγους θα δημιουργηθούν αντίγραφα ασφαλείας, προσθέτοντας:

```
# LocalhostBackup 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.

- Μετά, δημιουργήστε ένα νέο *Schedule* για την εργασία δημιουργίας αντιγράφων ασφαλείας:

```
# LocalhostBackup Schedule -- Daily.  
Schedule {  
  Name = "LocalhostDaily"  
  Run = Full daily at 00:01  
}
```

Η εργασία θα εκτελείται κάθε μέρα στις 00:01 ή 12:01 π.μ. Υπάρχουν πολλές άλλες επιλογές προγραμματισμού διαθέσιμες.

- Τέλος, δημιουργήστε την εργασία (*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"
}
```

Η εργασία θα δημιουργεί ένα *πλήρες* αντίγραφο ασφαλείας κάθε μέρα στη συσκευή κασέτας.

- Κάθε κασέτα θα πρέπει να έχει μια *ετικέτα*. Αν η τρέχουσα κασέτα δεν έχει ετικέτα, το Bacula θα σας στείλει ένα email για να σας ενημερώσει. Για να βάλετε ετικέτα σε μία κασέτα χρησιμοποιώντας το Console πληκτρολογήστε τα ακόλουθα σε ένα τερματικό:

bconsole

- Στην γραμμή εντολών του Bacula Console, πληκτρολογήστε:

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
```

- Πληκτρολογήστε το νέο όνομα του *τόμου*:

```
Enter new Volume name: Κυριακή
Defined Pools:
  1: Default
  2: Scratch
```

Αντικαταστήστε το *Κυριακή* με την επιθυμητή ετικέτα.

- Τώρα, επιλέξτε το *Pool*:

```
Select the Pool (1-2): 1
Connecting to Storage daemon TapeDrive at backupserver:9103 ...
Sending label command for Volume "Sunday" Slot 0 ...
```

Συγχαρητήρια, έχετε τώρα ρυθμίσει το *Bacula* ώστε να δημιουργεί αντίγραφο ασφαλείας του τοπικού υπολογιστή σε μία προσαρτημένη συσκευή κασέτας.

¹⁰ <http://www.bacula.org/en/rel-manual/index.html>

3.5. Πόροι

- Για περισσότερες επιλογές ρυθμίσεων του *Bacula* αναφερθείτε στο *εγχειρίδιο χρήστη του Bacula*¹⁰
- Η *αρχική σελίδα του Bacula*¹¹ περιέχει τις τελευταίες ειδήσεις και εκδόσεις του Bacula.
- Also, see the *Bacula Ubuntu Wiki*¹² page.

¹¹ <http://www.bacula.org/>

¹² <https://help.ubuntu.com/community/Bacula>

Κεφάλαιο 20. Εικονικοποίηση

Η εικονικοποίηση υιοθετείται από πολλά διαφορετικά περιβάλλοντα και καταστάσεις. Εάν είστε προγραμματιστής, η εικονικοποίηση μπορεί να σας παρέχει ένα περιορισμένο περιβάλλον στο οποίο μπορείτε με ασφάλεια να κάνετε σχεδόν κάθε είδους ανάπτυξη χωρίς να πειράζετε το κύριο περιβάλλον εργασίας σας. Εάν είστε διαχειριστής συστημάτων, μπορείτε να χρησιμοποιήσετε την εικονικοποίηση για να διαχωρίζετε πιο εύκολα τις υπηρεσίες σας και να τις μετακινείτε με βάση τη ζήτηση.

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

Η βιβλιοθήκη libvirt χρησιμοποιείται για να κάνει διεπαφή με διάφορες τεχνολογίες εικονικοποίησης. Πριν ξεκινήσετε με το libvirt είναι καλό να σιγουρευτείτε ότι το υλικό σας υποστηρίζει τις κατάλληλες επεκτάσεις εικονικοποίησης για το KVM. Πληκτρολογείτε τα ακόλουθα από ένα τερματικό εντολών:

```
kvm-ok
```

Θα εμφανιστεί ένα μήνυμα που θα σας πληροφορεί αν ο επεξεργαστής σας *υποστηρίζει* ή *δεν υποστηρίζει* εικονικές μηχανές (hardware virtualization).



Στους περισσότερους υπολογιστές των οποίων ο επεξεργαστής υποστηρίζει εικονικοποίηση, είναι απαραίτητο να ενεργοποιήσετε μια επιλογή στο BIOS.

1.1. Εικονική Διαδικτύωση

Αυτοί είναι διαφορετικοί τρόποι να επιτρέψετε σε μια εικονική μηχανή να έχει πρόσβαση στο εξωτερικό διαδίκτυο. Η προεπιλεγμένη διαμόρφωση του εικονικού διαδικτύου είναι διαδικτύωση *usermode*, η οποία χρησιμοποιεί το πρωτόκολλο SLIRP και κίνηση NATed μέσω της διεπαφής του κεντρικού υπολογιστή στο εξωτερικό δίκτυο.

Για να επιτρέψετε εξωτερικούς κεντρικούς υπολογιστές να έχουν πρόσβαση άμεσα σε εικονικές μηχανές μια *γέφυρα* πρέπει να ρυθμιστεί. Αυτό επιτρέπει στις εικονικές διεπαφές να συνδεθούν σε εξωτερικά δίκτυα μέσω της φυσικής διεπαφής, κάνοντάς τες να εμφανίζονται σαν κανονικοί κεντρικοί υπολογιστές στο υπόλοιπο δίκτυο. Για πληροφορίες σχετικές με το πως να στήσετε μια γέφυρα βλ. *Τμήμα 1.4, <Γεφύρωση> [43]*.

1.2. Εγκατάσταση

Για να εγκαταστήσετε τα απαραίτητα πακέτα, από ένα τερματικό εντολών πληκτρολογείτε:

```
sudo apt-get install kvm libvirt-bin
```

Αφού εγκαταστήσετε το libvirt-bin, ο χρήστης που χρησιμοποιείτε για να διαχειρίζεται εικονικές μηχανές θα πρέπει να ενταχθεί στην ομάδα *libvirtd*. Έτσι θα επιτραπεί στο χρήστη πρόσβαση σε ειδικές επιλογές δικτύωσης.

Σε ένα τερματικό πληκτρολογήστε:

```
sudo adduser $USER libvirtd
```




Εάν ο χρήστης που έχει επιλεγεί είναι ο τρέχων χρήστης, θε πρέπει να αποσυνδεθείτε και να συνδεθείτε ξανά για να ισχύσει η καινούρια ιδιότητα μέλους στην ομάδα.

Είστε τώρα έτοιμος να εγκαταστήσετε το λειτουργικό σύστημα *Guest*. Η εγκατάσταση μιας εικονικής μηχανής οδηγεί την ίδια διαδικασία με την εγκατάσταση του λειτουργικού συστήματος απευθείας στο υλικό. Χρειάζεστε είτε έναν τρόπο να αυτοματοποιήσετε την εγκατάσταση, ή ένα πληκτρολόγιο και μια οθόνη θα πρέπει να συνδεθούν στη φυσική μηχανή.

Σε περίπτωση εικονικών μηχανών ένα Γραφικό Περιβάλλον Εργασίας (Graphical User Interface (GUI)) είναι ανάλογο του φυσικού πληκτρολογίου και ποντικιού. Αντί να εγκαταστήσετε ένα Γραφικό Περιβάλλον Εργασίας η εφαρμογή *virt-viewer* μπορεί να χρησιμοποιηθεί για τη σύνδεση σε μια κονσόλα εικονικής μηχανής χρησιμοποιώντας το VNC. Δείτε το *Τμήμα 1.6, Πρόγραμμα Παρουσίασης Εικονικής Μηχανής*; [342] για περισσότερες πληροφορίες.

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.

Ακόμη ένας τρόπος για να εγκαταστήσετε μια εικονική μηχανή Ubuntu είναι να χρησιμοποιήσετε *ubuntu-vm-builder*. Το *ubuntu-vm-builder* σας επιτρέπει να εγκαταστήσετε ειδικά διαμερίσματα, να εκτελείτε σενάρια μετά την εγκατάσταση, κλπ. Για λεπτομέρειες βλ. *Τμήμα 2, JeOS και vmbuilder*; [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 είναι μέρος του πακέτου *virtinst*. Για να το εγκαταστήσετε από ένα τερματικό εντολών πληκτρολογήστε:

```
sudo apt-get install virtinst
```

Υπάρχουν πολλές επιλογές διαθέσιμες όταν χρησιμοποιείται το *virt-install*. Για παράδειγμα:

```
sudo virt-install -n web_devel -r 256 \
--disk path=/var/lib/libvirt/images/web_devel.img,bus=virtio,size=4 -c \
jeos.iso --accelerate --network network=default,model=virtio \
--connect=qemu:///system --vnc --noautoconsole -v
```

- *-n web_devel*: το όνομα της καινούριας εικονικής μηχανής θα είναι *web_devel* σε αυτό το παράδειγμα.

¹ <https://help.ubuntu.com/13.04/installation-guide/>

- `-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 jeos.iso`: αρχείο που θα χρησιμοποιηθεί σαν εικονικό CDROM. Το αρχείο μπορεί να είναι είτε ένα αρχείο ISO είτε το μονοπάτι για τη συσκευή CDROM του κεντρικού υπολογιστή.
- `--accelerate`: ενεργοποιεί της τεχνολογίες επιτάχυνσης kernel.
- `--network` provides details related to the VM's network interface. Here the *default* network is used, and the interface model is configured for *virtio*.
- `--vnc`: εξάγει την εικονική κονσόλα του επισκέπτη χρησιμοποιώντας VNC.
- `--noautoconsole`: δε θα συνδεθεί αυτόματα στην κονσόλα της εικονικής μηχανής.
- `-v`: δημιουργεί έναν πλήρως εικονικό επισκέπτη.

Αφού εκκινήσετε το `virt-install` μπορείτε να συνδεθείτε στην κονσόλα της εικονικής μηχανής είτε τοπικά χρησιμοποιώντας ένα Γραφικό Περιβάλλον Εργασίας ή με τη λειτουργία `virt-viewer`.

1.4. `virt-clone`

Η εφαρμογή `virt-clone` μπορεί να χρησιμοποιηθεί για να αντιγράψει μια εικονική μηχανή σε μια άλλη. Για παράδειγμα:

```
sudo virt-clone -o web_devel -n database_devel -f /path/to/database_devel.img \
--connect=qemu:///system
```

- `-o`: αρχική εικονική μηχανή.
- `-n`: όνομα της καινούριας εικονικής μηχανής.
- `-f`: μονοπάτι του αρχείου, λογικού τόμου, ή διαμερίσματος που θα χρησιμοποιηθεί από την καινούρια εικονική μηχανή.
- `--connect`: προσδιορίζει σε ποιο hypervisor να συνδεθεί.

Επίσης, χρησιμοποιείτε τις επιλογές `-d` ή `--debug` για να λύσετε προβλήματα με το `virt-clone`.



Αντικαταστήστε τα `web_devel` και `database_devel` με κατάλληλα ονόματα εικονικών μηχανών.

1.5. Διαχείριση Εικονικής Μηχανής

1.5.1. virsh

Υπάρχουν πολλές λειτουργίες διαθέσιμες για να διαχειριστείτε εικονικές μηχανές και το libvirt. Η λειτουργία virsh μπορεί να χρησιμοποιηθεί από τη γραμμή εντολών. Μερικά παραδείγματα:

- Για να καταγραφούν οι εικονικές μηχανές:

```
virsh -c qemu:///system list
```

- Για να εκκινήσετε μια εικονική μηχανή:

```
virsh -c qemu:///system start web_devel
```

- Ομοίως, για να εκκινήσετε μια εικονική μηχανή κατά την εκκίνηση:

```
virsh -c qemu:///system autostart web_devel
```

- Επανεκκινήστε μια εικονική μηχανή με:

```
virsh -c qemu:///system reboot web_devel
```

- Η κατάσταση των εικονικών μηχανών μπορεί να αποθηκευτεί σε ένα αρχείο ώστε να αποκατασταθεί αργότερα. Το ακόλουθο θα αποθηκεύσει την κατάσταση της εικονικής μηχανής σε ένα αρχείο που θα ονομαστεί σύμφωνα με την ημερομηνία:

```
virsh -c qemu:///system save web_devel web_devel-022708.state
```

Όταν αποθηκευτεί η εικονική μηχανή δε θα εκτελείτε πλέον.

- Μια αποθηκευμένη εικονική μηχανή μπορεί να αποκατασταθεί χρησιμοποιώντας:

```
virsh -c qemu:///system restore web_devel-022708.state
```

- Για να τερματίσετε μια εικονική μηχανή κάντε:

```
virsh -c qemu:///system shutdown web_devel
```

- Μια συσκευή CDROM μπορεί να φορτωθεί σε μια εικονική μηχανή πληκτρολογώντας:

```
virsh -c qemu:///system attach-disk web_devel /dev/cdrom /media/cdrom
```



Στο παραπάνω παραδείγματα αντικαταστήστε το *web_devel* με το κατάλληλο όνομα της εικονικής μηχανής, και το *web_devel-022708.state* με ένα περιγραφικό όνομα αρχείου.

1.5.2. Διαχειριστής Εικονικής Μηχανής

Το πακέτο `virt-manager` περιέχει μια γραφική λειτουργία για να διαχειρίζεστε τοπικές και απομακρυσμένες εικονικές μηχανές. Για να εγκαταστήσετε το `virt-manager` πληκτρολογείτε:

```
sudo apt-get install virt-manager
```

Αφού το `virt-manager` απαιτεί ένα περιβάλλον Γραφικής Διεπαφής Χρήστη (Graphical User Interface (GUI)) συνίσταται να το εγκαταστήσετε σε ένα σταθμό εργασίας ή μηχανή ελέγχου αντί σε ένα διακομιστή παραγωγής. Για να συνδεθείτε στην τοπική υπηρεσία `libvirt` πληκτρολογείτε:

```
virt-manager -c qemu:///system
```

Μπορείτε να συνδεθείτε στην υπηρεσία `libvirt` που εκτελείτε σε έναν άλλο κεντρικό υπολογιστή πληκτρολογώντας τα ακόλουθα σε ένα τερματικό εντολών:

```
virt-manager -c qemu+ssh://virtnode1.mydomain.com/system
```



Το παραπάνω παράδειγμα υποθέτει ότι η συνδεσιμότητα SSH μεταξύ του συστήματος διαχείρισης και του `virtnode1.mydomain.com` έχει ήδη διαμορφωθεί, και χρησιμοποιεί κλειδιά SSH για ταυτοποίηση. *Κλειδιά SSH* χρησιμοποιούνται γιατί το `libvirt` στέλνει την προτροπή κωδικικού σε άλλη διαδικασία. Για πληροφορίες στο πως να διαμορφώσετε SSH δείτε *Τμήμα 1, “OpenSSH Server” [85]*

1.6. Πρόγραμμα Παρουσίασης Εικονικής Μηχανής

Η εφαρμογή `virt-viewer` σας επιτρέπει να συνδέεστε στην κονσόλα εικονικής μηχανής. Το `virt-viewer` απαιτεί μια Γραφική Διεπαφή Χρήστη (Graphical User Interface (GUI)) για να συνδέεστε με την εικονική μηχανή.

Για να εγκαταστήσετε το `virt-viewer` από ένα τερματικό πληκτρολογείτε:

```
sudo apt-get install virt-viewer
```

Όταν μια εικονική μηχανή έχει εγκατασταθεί και εκτελείτε μπορείτε να συνδεθείτε στην κονσόλα της εικονικής μηχανής χρησιμοποιώντας:

```
virt-viewer -c qemu:///system web_devel
```

Όμοια με το `virt-manager`, το `virt-viewer` μπορεί να συνδεθεί σε έναν απομακρυσμένο κεντρικό υπολογιστή χρησιμοποιώντας *SSH* με κλειδιά ταυτοποίησης, επίσης:

```
virt-viewer -c qemu+ssh://virtnode1.mydomain.com/system web_devel
```

Βεβαιωθείτε να αντικαταστήσετε το *web_devel* με το κατάλληλο όνομα εικονικής μηχανής.

Εάν έχει διαμορφωθεί να χρησιμοποιεί *γεφυρωμένη* διεπαφή δικτύου μπορείτε επίσης να εγκαταστήσετε πρόσβαση SSH στην εικονική μηχανή. Δείτε *Τμήμα 1, “OpenSSH Server” [85]* και *Τμήμα 1.4, “Γεφύρωση” [43]* για περισσότερες λεπτομέρειες.

1.7. Πόροι

- See the *KVM*² home page for more details.
- Για περισσότερες λεπτομέρειες σχετικές με το libvirt δείτε το *libvirt home page*³
- Η ιστοσελίδα *Virtual Machine Manager*⁴ έχει περισσότερες πληροφορίες για την ανάπτυξη virt-manager.
- Επίσης, περάστε από το *#ubuntu-virt* κανάλι IRC στο *freenode*⁵ για να συζητήσετε για την τεχνολογία εικονικοποίησης στο Ubuntu.
- Άλλη μια καλή πηγή είναι η σελίδα *Ubuntu Wiki KVM*⁶.
- For information on Xen, including using Xen with libvirt, please see the *Ubuntu Wiki Xen*⁷ page.

² <http://www.linux-kvm.org/>

³ <http://libvirt.org/>

⁴ <http://virt-manager.et.redhat.com/>

⁵ <http://freenode.net/>

⁶ <https://help.ubuntu.com/community/KVM>

⁷ <https://help.ubuntu.com/community/Xen>

2. JeOS και vmbuilder

2.1. Εισαγωγή

2.1.1. Τι είναι το JeOS

Το Ubuntu *JeOS* (προφέρεται "Τζους") είναι μια αποδοτική παραλλαγή του λειτουργικού συστήματος Διακομιστή Ubuntu, διαμορφωμένο συγκεκριμένα για εικονικές συσκευές. Δεν είναι πλέον διαθέσιμο σαν CD-ROM ISO για μεταφόρτωση, αλλά μόνο σαν επιλογή είτε:

- Καθώς εγκαθιστάτε από το Server Edition ISO (πατώντας *F4* στην πρώτη οθόνη θα σας επιτρέψει να επιλέξετε "Ελάχιστη Εγκατάσταση", που είναι η επιλογή πακέτου ισοδύναμη με το JeOS).
- Ή να στηθεί χρησιμοποιώντας το vmbuilder του Ubuntu, το οποίο περιγράφεται εδώ.

Το JeOS είναι εξειδικευμένη εγκατάσταση της Έκδοσης Διακομιστή Ubuntu με ένα συντονισμένο πυρήνα ο οποίος περιέχει μόνο τα βασικά στοιχεία που χρειάζονται για να εκτελεστεί σε ένα εικονικό περιβάλλον.

Το Ubuntu JeOS έχει ρυθμιστεί ώστε να εκμεταλλεύεται βασικές τεχνολογίες απόδοσης στα τελευταία προϊόντα εικονικοποίησης από το VMware. Αυτός ο συνδυασμός του μειωμένου μεγέθους και τις βελτιστοποιημένης επίδοσης διασφαλίζει ότι η έκδοση Ubuntu JeOS παρέχει μια άκρως αποτελεσματική χρήση των πόρων του διακομιστή σε μεγάλες εικονικές αναπτύξεις.

Χωρίς περιττούς οδηγούς, και μόνο τα ελάχιστα απαιτούμενα πακέτα, το ISVs μπορεί να διαμορφώσει το υποστηριζόμενο OS ακριβώς όπως επιθυμούν. Έχουν τη σιγουριά ότι η ενημερώσεις, είτε για ασφάλεια είτε για λόγους ενίσχυσης, θα είναι περιορισμένες στο ελάχιστο που απαιτείται στο συγκεκριμένο περιβάλλον τους. Σε αντάλλαγμα, οι χρήστες που αναπτύσσουν εικονικές συσκευές χτισμένες σε JeOS θα πρέπει να περάσουν από λίγες ενημερώσεις και γι' αυτό λιγότερη συντήρηση από αυτή που θα είχαν με μία κανονική πλήρη εγκατάσταση ενός διακομιστή.

2.1.2. Τι είναι το vmbuilder

Με το vmbuilder, δεν είναι πλέον απαραίτητο να κάνετε λήψη ενός JeOS ISO. Το vmbuilder θα βρει τα διάφορα πακέτα και θα φτιάξει μια εικονική μηχανή προσαρμοσμένη στις ανάγκες σας σε περίπου ένα λεπτό. Το vmbuilder είναι ένα script που αυτοματοποιεί τη διαδικασία δημιουργίας μιας έτοιμης προς χρήση εικονικής μηχανής βασισμένης στο Linux. Οι hypervisor που υποστηρίζονται αυτή τη στιγμή είναι το KVM και το Xen.

Μπορείτε να περάσετε επιλογές γραμμής εντολών για να προσθέσετε επιπλέον πακέτα, να αφαιρέσετε πακέτα, να επιλέξετε ποια έκδοση του Ubuntu, ποιόν καθρέφτη κλπ. Σε πρόσφατο υλικό με μεγάλη RAM, να κάνετε `tmpdir` στο `/dev/shm` ή να χρησιμοποιήσετε ένα

tmrfs, και έναν τοπικό καθρέφτη, μπορείτε να εκκινήσετε αυτόματα ένα VM σε λιγότερο από ένα λεπτό.

Πρωτοεμφανίστηκε ως shell script στο Ubuntu 8.04 LTS, το ubuntu-vm-builder ξεκίνησε με μικρή έμφαση ως hack για να βοηθήσει τους προγραμματιστές να δοκιμάσουν τον καινούριο τους κώδικα σε μια εικονική μηχανή χωρίς να πρέπει να ξεκινήσουν από το μηδέν κάθε φορά. Καθώς αρκετοί διαχειριστές του Ubuntu άρχισαν να προσέχουν αυτό το script, κάποιοι από αυτούς συνέχισαν να το βελτιώνουν και να το προσαρμόζουν για τόσες περιπτώσεις χρήσης που ο Soren Hansen (ο δημιουργός του script και ειδικός στην εικονικοποίηση του Ubuntu, όχι ο παίκτης του γκολφ) αποφάσισε να το ξαναγράψει από το μηδέν για το Intrepid ως script της python με μερικούς νέους στόχους στη σχεδίαση:

- Να το αναπτύξει ώστε να μπορεί να επαναχρησιμοποιηθεί από άλλες διανομές.
- Να χρησιμοποιεί μηχανισμούς plugin για όλες τις αλληλεπιδράσεις εικονικοποίησης ώστε άλλοι να μπορούν εύκολα να προσθέσουν λογική για άλλα περιβάλλοντα εικονικοποίησης.
- Να παρέχει μια εύκολη να διατηρηθεί διεπαφή ιστού σαν επιλογή στη διεπαφή γραμμής εντολών.

Αλλά οι βασικές αρχές και εντολές να παραμείνουν ίδιες.

2.2. Αρχική εγκατάσταση

Υποθέτουμε ότι έχει εγκαταστήσει και διαμορφώσει τα libvirt και KVM τοπικά στη μηχανή ου χρησιμοποιείτε. Για πληροφορίες στο πως να το κάνετε, παρακαλώ αναφερθείτε στο:

- *Τμήμα 1, “libvirt” [338]*
- Η σελίδα Wiki KVM⁸

Επίσης υποθέτουμε ότι ξέρετε πως να χρησιμοποιήσετε έναν επεξεργαστή κειμένου με βάση κείμενο όπως οι nano ή vi. Εάν δεν έχετε χρησιμοποιήσει κανέναν από τους δύο στο παρελθόν, μπορείτε να δείτε μια επισκόπηση των διαφόρων επεξεργαστών κειμένου που είναι διαθέσιμοι διαβάζοντας τη σελίδα *PowerUsersTextEditors*⁹. Αυτό το εγχειρίδιο οδηγιών έχει δημιουργηθεί σε KVM, αλλά η βασική αρχή πρέπει να παραμείνει σε άλλες τεχνολογίες εικονικοποίησης.

2.2.1. Εγκατάσταση του vmbuilder

Το όνομα του πακέτου που χρειάζεται να εγκαταστήσετε είναι python-vm-builder. Σε ένα τερματικό εντολών πληκτρολογείτε:

```
sudo apt-get install python-vm-builder
```

⁸ <https://help.ubuntu.com/community/KVM>

⁹ <https://help.ubuntu.com/community/PowerUsersTextEditors>



Εάν τρέχετε Hardy, μπορείτε ακόμα να εκτελείτε τα περισσότερα από αυτά χρησιμοποιώντας την παλιά έκδοση του πακέτου που ονομάζεται `ubuntu-vm-builder`, υπάρχουν μόνο λίγες αλλαγές στη σύνταξη του πακέτου.

2.3. Καθορισμός της Εικονικής Μηχανής σας

Το να καθορίσετε μια εικονική μηχανή με το `vmbuilder` του Ubuntu είναι αρκετά απλό, αλλά εδώ είναι κάποια πράγματα που πρέπει να λάβετε υπόψιν:

- Εάν σκοπεύετε να στείλετε μια εικονική συσκευή, μην υποθέσετε ότι ο τελικός χρήστης θα ξέρει πως να επεκτείνει το μέγεθος του δίσκου ώστε να καλύπτει τις ανάγκες του, έτσι είτε σχεδιάστε για έναν μεγάλο εικονικό δίσκο για να επιτρέπει στη συσκευή σας να μεγαλώνει, ή εξηγήστε αρκετά καλά στις βοηθητικές οδηγίες πως να δεσμεύουν περισσότερο χώρο. Ίσως είναι καλή ιδέα να αποθηκεύει δεδομένα σε κάποιο ξεχωριστό εξωτερικό μέσο αποθήκευσης.
- Δεδομένου ότι η RAM είναι πολύ πιο εύκολο να δεσμευτεί σε ένα VM, το μέγεθος της RAM θα πρέπει να τεθεί σε ότι πιστεύετε είναι ασφαλές για τη συσκευή σας.

Η εντολή `vmbuilder` έχει 2 κύριες παραμέτρους: την *τεχνολογία εικονικοποίησης (hypervisor)* και την στοχοθετημένη *κατανομή*. Προαιρετικές παράμετροι είναι πολλές και μπορούν να βρεθούν χρησιμοποιώντας την ακόλουθη εντολή:

```
vmbuilder kvm ubuntu --help
```

2.3.1. Βασικές Παράμετροι

As this example is based on KVM and Ubuntu 13.04 (Raring Ringtail), and we are likely to rebuild the same virtual machine multiple time, we'll invoke `vmbuilder` with the following first parameters:

```
sudo vmbuilder kvm ubuntu --suite raring --flavour virtual --arch i386 \  
-o --libvirt qemu:///system
```

Η `--suite` προσδιορίζει την έκδοση Ubuntu, η `--flavour` προσδιορίζει ότι θέλουμε να χρησιμοποιήσουμε τον εικονικό πυρήνα kernel (αυτός χρησιμοποιείται για το στήσιμο μιας εικόνας JeOS), η `--arch` δηλώνει ότι θέλουμε να χρησιμοποιήσουμε μια μηχανή 32 bit, η `-o` λέει στο `vmbuilder` να αντικαταστήσει την προηγούμενη έκδοση του VM και η `--libvirt` λέει να ενημερωθεί το τοπικό εικονικό περιβάλλον να προσθέσει το VM που προκύπτει στη λίστα διαθέσιμων μηχανών.

Σημειώσεις:

- Λόγω της φύσεως των λειτουργιών που εκτελούνται από το `vmbuilder`, χρειάζεται να έχουμε διακαιώματα βάσης, γι' αυτό το `sudo`.
- Εάν η εικονική σας μηχανή χρειάζεται να χρησιμοποιήσει πάνω από 3Gb ram, πρέπει να στήσετε μηχανή 64 bit (`--arch amd64`).

- Μέχρι το Ubuntu 8.10, ο εικονικός πυρήνας ήταν φτιαγμένος μόνο για αρχιτεκτονική 32 bit, έτσι αν θέλετε να ορίσετε μηχανή amd64 στο Hardy, πρέπει να χρησιμοποιήσετε διακομιστή *--flavour* αντί αυτού.

2.3.2. Παράμετροι Εγκατάστασης JeOS

2.3.2.1. Δικτύωση JeOS

2.3.2.1.1. Αντιστοίχιση σταθερής διεύθυνσης IP

Σαν εικονική συσκευή που μπορεί να ανατεθεί σε διάφορα πολύ διαφορετικά δίκτυα, είναι πολύ δύσκολο να γνωρίζουμε πως ακριβώς θα είναι το δίκτυο. Για να απλοποιήσουμε τη διαμόρφωση, είναι καλή ιδέα να ακολουθήσουμε μια προσέγγιση παρόμοια με αυτή που συνήθως κάνουν οι κατασκευαστές υλικού, να αναθέτουν μια σταθερή IP διεύθυνση στη συσκευή σε δίκτυα ιδιωτικής κλάσης τα οποία θα παρέχετε στις βοηθητικές οδηγίες. Μια διεύθυνση με εμβέλεια 192.168.0.0/255 είναι συνήθως μια καλή επιλογή.

Για να το κάνουμε θα χρησιμοποιήσουμε τις ακόλουθες παραμέτρους:

- *--ip ADDRESS*: διεύθυνση IP σε μορφή με τελείες (εξορισμού σε dhcp εάν δεν διευκρινίζεται)
- *--hostname NAME*: Set NAME as the hostname of the guest.
- *--mask VALUE*: μάσκα IP σε μορφή με τελείες (εξορισμού: 255.255.255.0)
- *--net VALUE*: IP διεύθυνση δικτύου (εξορισμού: X.X.X.0)
- *--bcast VALUE*: IP εκπομπής (εξορισμού: X.X.X.255)
- *--gw ADDRESS*: διεύθυνση πυλώνα (εξορισμού: X.X.X.1)
- *--dns ADDRESS*: Διεύθυνση ονόματος διακομιστή (εξορισμού: X.X.X.1)

Υποθέτουμε για τώρα ότι η τιμές εξορισμού είναι αρκετά καλές, έτσι η προκύπτουσα επίκληση γίνεται:

```
sudo vmbuilder kvm ubuntu --suite raring --flavour virtual --arch i386 \
-o --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm
```

2.3.2.1.2. Γεφύρωση

Because our appliance will be likely to need to be accessed by remote hosts, we need to configure libvirt so that the appliance uses bridge networking. To do this add the *--bridge* option to the command:

```
sudo vmbuilder kvm ubuntu --suite raring --flavour virtual --arch i386 \
-o --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm --bridge br0
```



You will need to have previously setup a bridge interface, see *Τμήμα 1.4, “Γεφύρωση” [43]* for more information. Also, if the interface name is different change *br0* to the actual bridge interface.

2.3.2.2. Διαμερισμός

Ο διαμερισμός σε μια εικονική συσκευή θα πρέπει να λάβει υπόψιν τι σχεδιάζετε να κάνετε με αυτό. Επειδή οι περισσότερες συσκευές θέλουν να έχουν ξεχωριστό μέσο αποθήκευσης για δεδομένα, το να έχουν ένα ξεχωριστό `/var` θα έβγαζε νόημα.

Για να το κάνουμε αυτό το `vmbuilder` μας παρέχει το `--part`:

```
--part PATH
Allows you to specify a partition table in a partition file, located at PATH. Each
line of the partition file should specify (root first):
  mountpoint size
where size is in megabytes. You can have up to 4 virtual disks, a new disk starts
on a line with '---'. ie :
  root 1000
  /opt 1000
  swap 256
  ---
  /var 2000
  /log 1500
```

Στην περίπτωση μας θα προσδιορίσουμε ένα όνομα αρχείου κειμένου `vmbuilder.partition` το οποίο θα περιέχει τα ακόλουθα:

```
root 8000
swap 4000
---
/var 20000
```



Σημειώστε ότι χρησιμοποιούμε εικόνες εικονικού δίσκου, τα πραγματικά μεγέθη που βάζουμε εδώ είναι τα μέγιστα μεγέθη αυτών των τόμων.

Η γραμμή εντολών μας τώρα είναι:

```
sudo vmbuilder kvm ubuntu --suite raring --flavour virtual --arch i386 \
-o --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm --part vmbuilder.partition
```



Η χρήση `"\"` σε μια εντολή θα επιτρέψει μεγάλες συμβολοσειρές εντολών να αναδιπλώνονται στην επόμενη γραμμή.

2.3.2.3. Χρήστης και Κωδικός

Ξανά στήνοντας μια εικονική συσκευή, θα πρέπει να παρέχετε έναν εξορισμού χρήστη και κωδικό που θα είναι γενικά ώστε να μπορείτε να τα συμπεριλάβετε στις βοηθητικές οδηγίες. Θα δούμε αργότερα σε αυτό το εγχειρίδιο πως θα παρέχουμε ασφάλεια ορίζοντας ένα σενάριο που θα εκτελείται την πρώτη φορά που ο χρήστης εισέρχεται στη συσκευή, που, μεταξύ άλλων, θα του ζητάει να αλλάξει κωδικό. Σε αυτό το παράδειγμα θα χρησιμοποιήσω το `'user'` σαν όνομα χρήστη, και το `'default'` σαν κωδικό.

Για να το κάνουμε αυτό χρησιμοποιούμε προαιρετικές παραμέτρους:

- `--user USERNAME`: Ορίζει το όνομα του χρήστη που θα προστεθεί. Εξορισμού: `ubuntu`.
- `--name FULLNAME`: Ορίζει το πλήρες όνομα το χρήστη που θα προστεθεί. Εξορισμού: `Ubuntu`.
- `--pass PASSWORD`: Ορίζει τον κωδικό χρήστη. Εξορισμού: `ubuntu`.

Η προκύπτουσα γραμμή εντολής γίνεται:

```
sudo vmbuilder kvm ubuntu --suite raring --flavour virtual --arch i386 \  
-o --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm --part \  
vmbuilder.partition --user user --name user --pass default
```

2.3.3. Εγκατάσταση Απαιτούμενων Πακέτων

Σε αυτό το παράδειγμα θα εγκαταστήσουμε το πακέτο (Limesurvey) που έχει πρόσβαση στη βάση δεδομένων MySQL και έχει διεπαφή ιστού. Επομένως θα χρειαστούμε το λειτουργικό μας Σύστημα να μας παρέχει:

- Apache
- PHP
- MySQL
- OpenSSH Server
- Limesurvey (σαν εφαρμογή παράδειγμα που έχουμε πακετάρει)

Αυτό γίνεται χρησιμοποιώντας το `vmbuilder` ορίζοντας την επιλογή `--addpkg` πολλές φορές:

```
--addpkg PKG
```

Εγκαταστήστε το PKG στον επισκέπτη (μπορεί να οριστεί πολλαπλές φορές)

Όμως, λόγω του τρόπου που λειτουργεί το `vmbuilder`, τα πακέτα που πρέπει να κάνουν ερωτήσεις στον χρήστη κατά τη διάρκεια της φάσης πριν την εγκατάσταση δεν υποστηρίζονται και πρέπει αντί αυτών να εγκατασταθούν όταν μπορεί να συμβεί διαδραστικότητα. Αυτή είναι η περίπτωση Limesurvey, την οποία θα πρέπει να εγκαταστήσουμε αργότερα, όταν συνδεθεί ο χρήστης.

Άλλα πακέτα που ρωτούν απλή ερώτηση `debconf`, όπως ο `mysql-server` που ζητάει να οριστεί κωδικός, το πακέτο μπορεί να εγκατασταθεί αμέσως, αλλά θα πρέπει να το αναδιαμορφώσουμε την πρώτη φορά που θα συνδεθεί ο χρήστης.

Εάν κάποια πακέτα που πρέπει να εγκαταστήσουμε δεν είναι στο `main`, πρέπει να ενεργοποιήσουμε τα επιπλέον αποθετήρια χρησιμοποιώντας `--comp` και `--ppa`:

```
--components COMP1,COMP2,...,COMPn
```

A comma separated list of distro components to include (e.g. main,universe).

This defaults to "main"

```
--ppa=PPA Add ppa belonging to PPA to the vm's sources.list.
```

Εφόσον το Limesurvey δεν είναι μέρος του αρχείου αυτή τη στιγμή, θα ορίσουμε τη διεύθυνση PPA (αρχείο προσωπικού πακέτου) ώστε να προστεθεί στο VM /etc/apt/source.list, άρα προσθέτουμε τις ακόλουθες επιλογές στην γραμμή εντολών:

```
--addpkg apache2 --addpkg apache2-mpm-prefork --addpkg apache2-utils \
--addpkg apache2.2-common --addpkg dbconfig-common --addpkg libapache2-mod-php5 \
--addpkg mysql-client --addpkg php5-cli --addpkg php5-gd --addpkg php5-ldap \
--addpkg php5-mysql --addpkg wwwconfig-common --addpkg mysql-server --ppa nijaba
```

2.3.4. Εκτιμήσεις Ταχύτητας

2.3.4.1. Κρυφά αρχεία Πακέτου

Όταν το vmbuilder δημιουργεί το σύστημά σας, πρέπει να μεταφέρει καθένα από τα πακέτα που το απαρτίζουν από το διαδίκτυο από ένα από τα επίσημα αποθετήρια, το οποίο, ανάλογα με το σύστημά σας και την ταχύτητα της σύνδεσής σας με το διαδίκτυο και το φόρτο του mirror, μπορεί να έχει μεγάλη επίδραση στον πραγματικό χρόνο δημιουργίας. Για να μειωθεί, συνίσταται να έχετε είτε ένα τοπικό αποθετήριο (το οποίο μπορεί να δημιουργηθεί με τη χρήση του apt-mirror) είτε να χρησιμοποιήσετε έναν proxy προσωρινής αποθήκευσης όπως το apt-proxy. Η δεύτερη επιλογή είναι πιο απλή στην υλοποίηση και απαιτεί λιγότερο χώρο, έτσι την επιλέξαμε για αυτό το μάθημα. Για να το εγκαταστήσετε, απλά πληκτρολογήστε:

```
sudo apt-get install apt-proxy
```

Όταν ολοκληρωθεί αυτό, ο (άδειος) διαμεσολαβητής σας είναι έτοιμος για χρήση στο `http://mirroraddress:9999` και θα βρείτε το αποθετήριο ubuntu στο /ubuntu. Για να το χρησιμοποιήσει το vmbuilder, θα πρέπει να χρησιμοποιήσουμε την επιλογή `--mirror`:

```
--mirror=URL Χρησιμοποιήστε το καθρέφτη Ubuntu στο URL αντί του προεπιλεγμένου που είναι
http://archive.ubuntu.com/ubuntu for official
arches and http://ports.ubuntu.com/ubuntu-ports
otherwise
```

Άρα προσθέτουμε στη γραμμή εντολής:

```
--mirror http://mirroraddress:9999/ubuntu
```



The mirror address specified here will also be used in the /etc/apt/sources.list of the newly created guest, so it is useful to specify here an address that can be resolved by the guest or to plan on resetting this address later on.

2.3.4.2. Εγκατάσταση ενός Τοπικού Καθρέφτη

Εάν είμαστε σε ένα μεγαλύτερο περιβάλλον, μπορεί να έχει νόημα να στήσουμε έναν τοπικό καθρέφτη των αποθετηρίων Ubuntu. Το πακέτο apt-mirror παρέχει ένα σενάριο το οποίο χειρίζεται τη δημιουργία καθρεφτών για εσάς. Πρέπει να υπολογίσετε να έχετε περίπου 20 gigabyte ελεύθερου χώρου ανά υποστηριζόμενη έκδοση και αρχιτεκτονική.

By default, apt-mirror uses the configuration file in /etc/apt/mirror.list. As it is set up, it will replicate only the architecture of the local machine. If you would like to support other architectures on your mirror, simply duplicate the lines starting with "deb", replacing the deb keyword by /deb-{arch} where arch can be i386, amd64, etc... For example, on an amd64 machine, to have the i386 archives as well, you will have (some lines have been split to fit the format of this document):

```
deb http://archive.ubuntu.com/ubuntu raring main restricted universe multiverse
/deb-i386 http://archive.ubuntu.com/ubuntu raring main restricted universe multiverse
```

```
deb http://archive.ubuntu.com/ubuntu raring-updates main restricted universe multiverse
/deb-i386 http://archive.ubuntu.com/ubuntu raring-updates main
restricted universe multiverse
```

```
deb http://archive.ubuntu.com/ubuntu/ raring-backports main restricted universe multiverse
/deb-i386 http://archive.ubuntu.com/ubuntu raring-backports main
restricted universe multiverse
```

```
deb http://security.ubuntu.com/ubuntu raring-security main restricted universe multiverse
/deb-i386 http://security.ubuntu.com/ubuntu raring-security main
restricted universe multiverse
```

```
deb http://archive.ubuntu.com/ubuntu raring main/debian-installer
restricted/debian-installer universe/debian-installer multiverse/debian-installer
/deb-i386 http://archive.ubuntu.com/ubuntu raring main/debian-installer
restricted/debian-installer universe/debian-installer multiverse/debian-installer
```

Παρατηρείστε ότι τα πακέτα πηγής δεν είναι στον καθρέφτη καθώς χρησιμοποιούνται σπάνια σε σχέση με τα binaries και δεν πιάνουν πολύ χώρο, αλλά μπορούν εύκολα να προστεθούν στη λίστα.

Όταν ο καθρέφτης τελειώσει την αντιγραφή (και αυτό μπορεί να διαρκέσει πολύ), πρέπει να ρυθμίσετε τον Apache ώστε τα αρχεία καθρέφτη σας (στο /var/spool/apt-mirror εάν δεν αλλάξατε την προεπιλογή), να εκδίδονται από τον διακομιστή Apache. Για περισσότερες πληροφορίες στον Apache δείτε *Τμήμα 1, “HTTPD - Apache2 Διακομιστής Ιστού” [200]*.

2.4. Η Εφαρμογή σε Πακέτο

Δύο επιλογές είναι διαθέσιμες σε εμάς:

- Η προτεινόμενη μέθοδος για να το κάνετε είναι να δημιουργήσετε ένα πακέτο *Debian*. Μιας και αυτό είναι εκτός πεδίου εφαρμογής αυτού του εγχειριδίου, δε θα το εκτελέσουμε εδώ και θα καλέσουμε το χρήστη να διαβάσει τις βοηθητικές οδηγίες για το πως να το κάνει στο *Ubuntu Packaging Guide*¹⁰. Σε αυτή την περίπτωση είναι επίσης καλή ιδέα να στήσετε ένα αποθετήριο για το πακέτο ώστε οι ενημερώσεις να τις τραβήξετε βολικά από εκεί. Δείτε το άρθρο *Debian Administration*¹¹ για ένα εγχειρίδιο οδηγιών πάνω σε αυτό.
- Εγκαταστήστε την εφαρμογή χειροκίνητα στο `/opt` όπως συνίσταται από τις *κατευθυντήριες γραμμές FHS*¹².

Στην περίπτωσή μας θα χρησιμοποιήσουμε το Limesurvey σαν παράδειγμα εφαρμογής ιστού για την οποία επιθυμούμε να παρέχουμε μια εικονική συσκευή. Όπως επισημάνθηκε πριν, έχουμε δημιουργήσει έκδοση του πακέτου διαθέσιμο στο PPA (Αρχείο Προσωπικού Πακέτου).

2.5. Χρήσιμες Προσθήκες

2.5.1. Διαμόρφωση Αυτόματων Ενημερώσεων

Για να διαμορφωθεί το σύστημά σας ώστε να ενημερώνεται αυτόματα σε τακτική βάση, θα εγκαταστήσουμε απλά το `unattended-upgrades`, άρα προσθέτουμε την ακόλουθη επιλογή στη γραμμή εντολής μας:

```
--addpkg unattended-upgrades
```

Καθώς έχουμε βάλει το πακέτο εφαρμογής μας στο PPA, η διαδικασία θα ενημερώσει όχι μόνο το σύστημα, αλλά και την εφαρμογή κάθε φορά που ενημερώνουμε την έκδοση στο PPA.

2.5.2. Διαχείριση Γεγονότων ACPI

Για να μπορεί να διαχειρίζεται η εικονική σας μηχανή γεγονότα εκκίνησης και τερματισμού, είναι καλή ιδέα να εγκαταστήσετε το πακέτο `acpid` επίσης. Για να το κάνουμε αυτό απλά προσθέτουμε την ακόλουθη επιλογή:

```
--addpkg acpid
```

2.6. Τελική Εντολή

Εδώ είναι η εντολή με όλες τις επιλογές που συζητήθηκαν παραπάνω:

¹⁰ <https://wiki.ubuntu.com/PackagingGuide>

¹¹ <http://www.debian-administration.org/articles/286>

¹² <http://www.pathname.com/fhs/>

```
sudo vmbuilder kvm ubuntu --suite raring --flavour virtual --arch i386 -o \  
  --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm \  
  --part vmbuilder.partition --user user --name user --pass default \  
  --addpkg apache2 --addpkg apache2-mpm-prefork --addpkg apache2-utils \  
  --addpkg apache2.2-common --addpkg dbconfig-common \  
  --addpkg libapache2-mod-php5 --addpkg mysql-client --addpkg php5-cli \  
  --addpkg php5-gd --addpkg php5-ldap --addpkg php5-mysql \  
  --addpkg wwwconfig-common --addpkg mysql-server \  
  --addpkg unattended-upgrades --addpkg acpid --ppa nijaba \  
  --mirror http://mirroraddress:9999/ubuntu
```

2.7. Πόροι

Εάν ενδιαφέρεστε να μάθετε περισσότερα, έχετε απορίες ή προτάσεις, παρακαλώ επικοινωνήστε με την Ομάδα Διακομιστή Ubuntu στο:

- IRC: #ubuntu-server on freenode
- Λίστα Ηλεκτρονικής Αλληλογραφίας: *ubuntu-server at lists.ubuntu.com*¹³
- Επίσης δείτε τη σελίδα *JeOSVMBuilder Ubuntu Wiki*¹⁴.

¹³ <https://lists.ubuntu.com/mailman/listinfo/ubuntu-server>

¹⁴ <https://help.ubuntu.com/community/JeOSVMBuilder>

3. 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.

3.1. Επισκόπηση

This tutorial covers the OpenStack installation from the Ubuntu 12.10 Server Edition CD, and assumes a basic network topology, with a single system serving as the "all-in-one cloud infrastructure". Due to the tutorial's simplicity, the instructions as-is are not intended to set up production servers although it allows you to have a POC (proof of concept) of the Ubuntu Cloud using OpenStack.

3.2. Προαπαιτούμενα

To deploy a minimal Ubuntu Cloud infrastructure, you'll need at least:

- One dedicated system.
- Two network address ranges (private network and public network).
- Make sure the host in question supports VT (Virtualization Technology) since we will be using KVM as the virtualization technology. Other hypervisors are also supported such as QEMU, UML, Vmware ESX/ESXi and XEN. LXC (Linux Containers) is also supported through libvirt.

Check if your system supports kvm issuing **sudo kvm-ok** in a linux terminal.

The "**Minimum Topology**" recommended for production use is using three nodes - One master server running nova services (except compute) and two servers running nova-compute. This setup is not redundant and the master server is a SPoF (Single Point of Failure).

3.3. Preconfiguring the network

Before we start installing OpenStack we need to make sure we have bridging support installed, a MySQL database, and a central time server (ntp). This will assure that we have instantiated machines and hosts in sync.

In this example the "private network" will be in the 10.0.0.0/24 range on eth1. All the internal communication between instances will happen there while the "public network" will be in the 10.153.107.0/29 range on eth0.

3.3.1. Install bridging support

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

3.3.2. Install and configure NTP

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

Add these two lines at the end of the `/etc/ntp.conf` file.

```
server 127.127.1.0  
fudge 127.127.1.0 stratum 10
```

Restart ntp service

```
sudo service ntp restart
```

3.3.3. Install and configure MySQL

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

Create a database and mysql user for OpenStack

```
sudo mysql -uroot -ppassword -e "CREATE DATABASE nova;"  
sudo mysql -uroot -ppassword -e "GRANT ALL ON nova.* TO novauser@localhost \  
IDENTIFIED BY 'novapassword' ";
```

The line continuation character `"\"` implies that you must include the subsequent line as part of the current command.

3.4. Install OpenStack Compute (Nova)

OpenStack Compute (Nova) is a cloud computing fabric controller (the main part of an IaaS system). It is written in Python, using the Eventlet and Twisted frameworks, and relies on the standard AMQP messaging protocol, and SQLAlchemy for data store access.

Install OpenStack Nova components

```
sudo apt-get install nova-api nova-network nova-volume nova-objectstore nova-scheduler \  
nova-compute euca2ools unzip
```

Restart libvirt-bin just to make sure libvirtd is aware of ebtables.

```
sudo service libvirt-bin restart
```

Install RabbitMQ – Advanced Message Queuing Protocol (AMQP)

```
sudo apt-get install rabbitmq-server
```

Edit /etc/nova/nova.conf and add the following:

```
# Nova config FlatDHCPManager
--sql_connection=mysql://novauser:novapassword@localhost/nova
--flat_injected=true
--network_manager=nova.network.manager.FlatDHCPManager
--fixed_range=10.0.0.0/24
--floating_range=10.153.107.72/29
--flat_network_dhcp_start=10.0.0.2
--flat_network_bridge=br100
--flat_interface=eth1
--public_interface=eth0
```

Restart OpenStack services

```
for i in nova-api nova-network nova-objectstore nova-scheduler nova-volume nova-compute; \  
do sudo stop $i; sleep 2; done
```

```
for i in nova-api nova-network nova-objectstore nova-scheduler nova-volume nova-compute; \  
do sudo start $i; sleep 2; done
```

Migrate Nova database from sqlite db to MySQL db. It may take a while.

```
sudo nova-manage db sync
```

Define a specific private network where all your Instances will run. This will be used in the network of fixed Ips set inside nova.conf .

```
sudo nova-manage network create --fixed_range_v4 10.0.0.0/24 --label private \  
--bridge_interface br100
```

Define a specific public network and allocate 6 (usable) Floating Public IP addresses for use with the instances starting from 10.153.107.72.

```
sudo nova-manage floating create --ip_range=10.153.107.72/29
```

Create a user (user1), a project (project1), download credentials and source its configuration file.

```
cd ; mkdir nova ; cd nova  
sudo nova-manage user admin user1  
sudo nova-manage project create project1 user1
```

```
sudo nova-manage project zipfile project1 user1
unzip nova.zip
source novarc
```

Verify the OpenStack Compute installation by typing:

```
sudo nova-manage service list
sudo nova-manage version list
```

If nova services don't show up correctly restart OpenStack services as described previously. For more information please refer to the troubleshooting section on this guide.

3.5. Install Imaging Service (Glance)

Nova uses Glance service to manage Operating System images that it needs for bringing up instances. Glance can use several types of storage backends such as filestore, s3 etc. Glance has two components - *glance-api* and *glance-registry*. These can be controlled using the concerned upstart service jobs. For this specific case we will be using mysql as a storage backend.

Install Glance

```
sudo apt-get install glance
```

Create a database and user for glance

```
sudo mysql -uroot -ppassword -e "CREATE DATABASE glance;"
sudo mysql -uroot -ppassword -e "GRANT ALL ON glance.* TO glanceuser@localhost \
IDENTIFIED BY 'glancepassword' ";
```

Edit the file `/etc/glance/glance-registry.conf` and edit the line which contains the option `"sql_connection ="` to this:

```
sql_connection = mysql://glanceuser:glancepassword@localhost/glance
```

Remove the sqlite database

```
rm -rf /var/lib/glance/glance.sqlite
```

Restart glance-registry after making changes to `/etc/glance/glance-registry.conf`. The MySQL database will be automatically populated.

```
sudo restart glance-registry
```

If you find issues take a look at the log file in `/var/log/glance/api.log` and `/var/log/glance/registry.log`.

3.6. Running Instances

Before you can instantiate images, you first need to setup user credentials. Once this first step is achieved you also need to upload images that you want to run in the cloud. Once you have these images uploaded to the cloud you will be able to run and connect to them. Here are the steps you should follow to get OpenStack Nova running instances:

Download, register and publish an Ubuntu cloud image

```
distro=lucid
wget http://cloud-images.ubuntu.com/$distro/current/$distro-server-cloudimg-amd64.tar.gz
cloud-publish-tarball "$distro"-server-cloudimg-amd64.tar.gz "$distro"_amd64
```

Create a key pair and start an instance

```
cd ~/nova
source novarc
euca-add-keypair user1 > user1.priv
chmod 0600 user1.priv
```

Allow icmp (ping) and ssh access to instances

```
euca-authorize default -P tcp -p 22 -s 0.0.0.0/0
euca-authorize -P icmp -t -1:-1 default
```

Run an instance

```
ami=`euca-describe-images | awk {'print $2'} | grep -m1 ami`
euca-run-instances $ami -k user1 -t m1.tiny
euca-describe-instances
```

Assign public address to the instance.

```
euca-allocate-address
euca-associate-address -i instance_id public_ip_address
euca-describe-instances
```

You must enter above the instance_id (ami) and public_ip_address shown above by euca-describe-instances and euca-allocate-address commands.

Now you should be able to SSH to the instance

```
ssh -i user1.priv ubuntu@ipaddress
```

To terminate instances

euca-terminate-instances instance_id

3.7. Install the Storage Infrastructure (Swift)

Swift is a highly available, distributed, eventually consistent object/blob store. It is used by the OpenStack Infrastructure to provide S3 like cloud storage services. It is also S3 api compatible with amazon.

Organizations use Swift to store lots of data efficiently, safely, and cheaply where applications use an special api to interface between the applications and objects stored in Swift.

Although you can install Swift on a single server, a multiple-server installation is required for production environments. If you want to install OpenStack Object Storage (Swift) on a single node for development or testing purposes, use the Swift All In One instructions on Ubuntu.

For more information see: http://swift.openstack.org/development_saio.html¹⁵.

3.8. Support and Troubleshooting

Community Support

- *OpenStack Mailing list*¹⁶
- *The OpenStack Wiki search*¹⁷
- *Launchpad bugs area*¹⁸
- Join the IRC channel #openstack on freenode.

3.9. Πόροι

- *Cloud Computing - Service models*¹⁹
- *OpenStack Compute*²⁰
- *OpenStack Image Service*²¹
- *OpenStack Object Storage Administration Guide*
- *Installing OpenStack Object Storage on Ubuntu*²²
- <http://cloudglossary.com/>

¹⁵ http://swift.openstack.org/development_saio.html

¹⁶ <https://launchpad.net/~openstack>

¹⁷ <http://wiki.openstack.org>

¹⁸ <https://bugs.launchpad.net/nova>

¹⁹ http://en.wikipedia.org/wiki/Cloud_computing#Service_Models

²⁰ docs.openstack.org/trunk/openstack-compute/

²¹ <http://docs.openstack.org/diablo/openstack-compute/starter/content/GlanceMS-d2s21.html>

²² <http://docs.openstack.org/trunk/openstack-object-storage/admin/content/installing-openstack-object-storage-on-ubuntu.html>

3.10. Γλωσσάριο

The Ubuntu Cloud documentation uses terminology that might be unfamiliar to some readers. This page is intended to provide a glossary of such terms and acronyms.

- *Cloud* - A federated set of physical machines that offer computing resources through virtual machines, provisioned and recollected dynamically.
- *IaaS* - Infrastructure as a Service — Cloud infrastructure services, whereby a virtualized environment is delivered as a service over the Internet by the provider. The infrastructure can include servers, network equipment, and software.
- *EBS* - Elastic Block Storage.
- *EC2* - Elastic Compute Cloud. Amazon's pay-by-the-hour, pay-by-the-gigabyte public cloud computing offering.
- *Node* - A node is a physical machine that's capable of running virtual machines, running a node controller. Within Ubuntu, this generally means that the CPU has VT extensions, and can run the KVM hypervisor.
- *S3* - Simple Storage Service. Amazon's pay-by-the-gigabyte persistent storage solution for EC2.
- *Ubuntu Cloud* - Ubuntu Cloud. Ubuntu's cloud computing solution, based on OpenStack.
- *VM* - Virtual Machine.
- *VT* - Virtualization Technology. An optional feature of some modern CPUs, allowing for accelerated virtual machine hosting.

4. 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. Therefore containers are better compared 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. Some vserver and OpenVZ functionality is still missing in containers, however containers can *boot* many Linux distributions and have the advantage that they can be used with an un-modified upstream kernel.

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. Toward the end, we will describe how to use the libvirt LXC driver.

In this document, a container name will be shown as CN, C1, or C2.

4.1. Εγκατάσταση

The lxc package can be installed using

```
sudo apt-get install lxc
```

This will pull in the required and recommended dependencies, including cgroup-lite, lvm2, and debootstrap. To use libvirt-lxc, install libvirt-bin. LXC and libvirt-lxc can be installed and used at the same time.

4.2. Host Setup

4.2.1. Basic layout of LXC files

Following is a description of the files and directories which are installed and used by LXC.

- There are two upstart jobs:
 - /etc/init/lxc-net.conf: is an optional job which only runs if /etc/default/lxc specifies USE_LXC_BRIDGE (true by default). It sets up a NATed bridge for containers to use.

- `/etc/init/lxc.conf`: runs if `LXC_AUTO` (true by default) is set to true in `/etc/default/lxc`. It looks for entries under `/etc/lxc/auto/` which are symbolic links to configuration files for the containers which should be started at boot.
- `/etc/lxc/lxc.conf`: There is a default container creation configuration file, `/etc/lxc/lxc.conf`, which directs containers to use the LXC bridge created by the `lxc-net` upstart job. If no configuration file is specified when creating a container, then this one will be used.
- Examples of other container creation configuration files are found under `/usr/share/doc/lxc/examples`. These show how to create containers without a private network, or using `macvlan`, `vlan`, or other network layouts.
- The various container administration tools are found under `/usr/bin`.
- `/usr/lib/lxc/lxc-init` is a very minimal and lightweight init binary which is used by `lxc-execute`. Rather than 'booting' a full container, it manually mounts a few filesystems, especially `/proc`, and executes its arguments. You are not likely to need to manually refer to this file.
- `/usr/lib/lxc/templates/` contains the 'templates' which can be used to create new containers of various distributions and flavors. Not all templates are currently supported.
- `/etc/apparmor.d/lxc/lxc-default` contains the default Apparmor MAC policy which works to protect the host from containers. Please see the *Τμήμα 4.2.6, “Apparmor” [364]* for more information.
- `/etc/apparmor.d/usr.bin.lxc-start` contains a profile to protect the host from **lxc-start** while it is setting up the container.
- `/etc/apparmor.d/lxc-containers` causes all the profiles defined under `/etc/apparmor.d/lxc` to be loaded at boot.
- There are various man pages for the LXC administration tools as well as the `lxc.conf` container configuration file.
- `/var/lib/lxc` is where containers and their configuration information are stored.
- `/var/cache/lxc` is where caches of distribution data are stored to speed up multiple container creations.

4.2.2. lxcbr0

When `USE_LXC_BRIDGE` is set to true in `/etc/default/lxc` (as it is by default), a bridge called `lxcbr0` is created at startup. This bridge is given the private address 10.0.3.1, and containers using this bridge will have a 10.0.3.0/24 address. A `dnsmasq` instance is run listening on that bridge, so if another `dnsmasq` has bound all interfaces before the `lxc-net` upstart job runs, `lxc-net` will fail to start and `lxcbr0` will not exist.

If you have another bridge - `libvirt`'s default `virbr0`, or a `br0` bridge for your default NIC - you can use that bridge in place of `lxcbr0` for your containers.

4.2.3. Using a separate filesystem for the container store

LXC stores container information and (with the default backing store) root filesystems under `/var/lib/lxc`. Container creation templates also tend to store cached distribution information under `/var/cache/lxc`.

If you wish to use another filesystem than `/var`, you can mount a filesystem which has more space into those locations. If you have a disk dedicated for this, you can simply mount it at `/var/lib/lxc`. If you'd like to use another location, like `/srv`, you can bind mount it or use a symbolic link. For instance, if `/srv` is a large mounted filesystem, create and symlink two directories:

```
sudo mkdir /srv/lxclib /srv/lxccache
sudo rm -rf /var/lib/lxc /var/cache/lxc
sudo ln -s /srv/lxclib /var/lib/lxc
sudo ln -s /srv/lxccache /var/cache/lxc
```

or, using bind mounts:

```
sudo mkdir /srv/lxclib /srv/lxccache
sudo sed -i '$a \
/srv/lxclib /var/lib/lxc  none defaults,bind 0 0 \
/srv/lxccache /var/cache/lxc none defaults,bind 0 0' /etc/fstab
sudo mount -a
```

4.2.4. Containers backed by lvm

It is possible to use LVM partitions as the backing stores for containers. Advantages of this include flexibility in storage management and fast container cloning. The tools default to using a VG (volume group) named `lxc`, but another VG can be used through command line options. When a LV is used as a container backing store, the container's configuration file is still `/var/lib/lxc/CN/config`, but the root fs entry in that file (`lxc.rootfs`) will point to the LV block device name, i.e. `/dev/lxc/CN`.

Containers with directory tree and LVM backing stores can co-exist.

4.2.5. Btrfs

If your host has a btrfs `/var`, the LXC administration tools will detect this and automatically exploit it by cloning containers using btrfs snapshots.

4.2.6. Apparmor

LXC ships with an 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.

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. If you wish 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 reusable 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
```

lxc-execute does not enter an Apparmor profile, but the container it spawns will be confined.

4.2.7. 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, LXC depends on the cgroup-lite package to be installed, which provides the proper cgroup initialization at boot. The cgroup-lite package mounts each cgroup subsystem separately under `/sys/fs/cgroup/SS`, where SS is the subsystem name. For instance the freezer subsystem is mounted under `/sys/fs/cgroup/freezer`. LXC cgroup are kept under `/sys/fs/cgroup/SS/INIT/lxc`, where INIT is the init task's cgroup. This is / by default, so in the end the freezer cgroup for container CN would be `/sys/fs/cgroup/freezer/lxc/CN`.

4.2.8. Privilege

The container administration tools must be run with root user privilege. A utility called `lxc-setup` was written with the intention of providing the tools with the needed file capabilities to allow non-root users to run the tools with sufficient privilege. However, as root in a container cannot yet be reliably contained, this is not worthwhile. It is therefore recommended to not use `lxc-setup`, and to provide the LXC administrators the needed sudo privilege.

The user namespace, which is expected to be available in the next Long Term Support (LTS) release, will allow containment of the container root user, as well as reduce the amount of privilege required for creating and administering containers.

4.2.9. LXC Upstart Jobs

As listed above, the `lxc` package includes two upstart jobs. The first, `lxc-net`, is always started when the other, `lxc`, is about to begin, and stops when it stops. If the `USE_LXC_BRIDGE` variable is set to false in `/etc/defaults/lxc`, then it will immediately exit. If it is true, and an error occurs bringing up the LXC bridge, then the `lxc` job will not start. `lxc-net` will bring down the LXC bridge when stopped, unless a container is running which is using that bridge.

The `lxc` job starts on runlevel 2-5. If the `LXC_AUTO` variable is set to true, then it will look under `/etc/lxc` for containers which should be started automatically. When the `lxc` job is stopped, either manually or by entering runlevel 0, 1, or 6, it will stop those containers.

To register a container to start automatically, create a symbolic link `/etc/default/lxc/name.conf` pointing to the container's config file. For instance, the configuration file for a container CN is `/var/lib/lxc/CN/config`. To make that container auto-start, use the command:

```
sudo ln -s /var/lib/lxc/CN/config /etc/lxc/auto/CN.conf
```

4.3. Container Administration

4.3.1. Creating Containers

The easiest way to create containers is using **lxc-create**. This script uses distribution-specific templates under `/usr/lib/lxc/templates/` to set up container-friendly chroots under `/var/lib/lxc/CN/rootfs`, and initialize the configuration in `/var/lib/lxc/CN/fstab` and `/var/lib/lxc/CN/config`, where CN is the container name

The simplest container creation command would look like:

```
sudo lxc-create -t ubuntu -n CN
```

This tells `lxc-create` to use the `ubuntu` template (`-t ubuntu`) and to call the container CN (`-n CN`). Since no configuration file was specified (which would have been done with ``-f file'`), it will use the default configuration file under `/etc/lxc/lxc.conf`. This gives the container a single veth network interface attached to the `lxcbr0` bridge.

The container creation templates can also accept arguments. These can be listed after `--`. For instance

```
sudo lxc-create -t ubuntu -n oneirc1 -- -r oneirc
```

passes the arguments `'-r oneirc1'` to the `ubuntu` template.

4.3.1.1. Help

Help on the `lxc-create` command can be seen by using **`lxc-create -h`**. However, the templates also take their own options. If you do

```
sudo lxc-create -t ubuntu -h
```

then the general **`lxc-create`** help will be followed by help output specific to the `ubuntu` template. If no template is specified, then only help for **`lxc-create`** itself will be shown.

4.3.1.2. Ubuntu template

The `ubuntu` template can be used to create Ubuntu system containers with any release at least as new as 10.04 LTS. It uses `debootstrap` to create a cached container filesystem which gets copied into place each time a container is created. The cached image is saved and only re-generated when you create a container using the `-F` (flush) option to the template, i.e.:

```
sudo lxc-create -t ubuntu -n CN -- -F
```

The Ubuntu release installed by the template will be the same as that on the host, unless otherwise specified with the *-r* option, i.e.

```
sudo lxc-create -t ubuntu -n CN -- -r lucid
```

If you want to create a 32-bit container on a 64-bit host, pass *-a i386* to the container. If you have the *qemu-user-static* package installed, then you can create a container using any architecture supported by *qemu-user-static*.

The container will have a user named *ubuntu* whose password is *ubuntu* and who is a member of the *sudo* group. If you wish to inject a public ssh key for the *ubuntu* user, you can do so with *-S sshkey.pub*.

You can also *bind* user *jdoe* from the host into the container using the *-b jdoe* option. This will copy *jdoe*'s password and shadow entries into the container, make sure his default group and shell are available, add him to the *sudo* group, and bind-mount his home directory into the container when the container is started.

When a container is created, the *release-updates* archive is added to the container's *sources.list*, and its package archive will be updated. If the container release is older than 12.04 LTS, then the *lxcguest* package will be automatically installed. Alternatively, if the *--trim* option is specified, then the *lxcguest* package will not be installed, and many services will be removed from the container. This will result in a faster-booting, but less upgrade-able container.

4.3.1.3. *Ubuntu-cloud template*

The *ubuntu-cloud* template creates Ubuntu containers by downloading and extracting the published Ubuntu cloud images. It accepts some of the same options as the *ubuntu* template, namely *-r release*, *-S sshkey.pub*, *-a arch*, and *-F* to flush the cached image. It also accepts a few extra options. The *-C* option will create a *cloud* container, configured for use with a metadata service. The *-u* option accepts a cloud-init user-data file to configure the container on start. If *-L* is passed, then no locales will be installed. The *-T* option can be used to choose a tarball location to extract in place of the published cloud image tarball. Finally the *-i* option sets a host id for cloud-init, which by default is set to a random string.

4.3.1.4. *Other templates*

The *ubuntu* and *ubuntu-cloud* templates are well supported. Other templates are available however. The *debian* template creates a Debian based container, using *debootstrap* much

as the ubuntu template does. By default it installs a *debian squeeze* image. An alternate release can be chosen by setting the SUITE environment variable, i.e.:

```
sudo SUITE=sid lxc-create -t debian -n d1
```

To purge the container image cache, call the template directly and pass it the *--clean* option.

```
sudo SUITE=sid /usr/lib/lxc/templates/lxc-debian --clean
```

A fedora template exists, which creates containers based on fedora releases <= 14. Fedora release 15 and higher are based on systemd, which the template is not yet able to convert into a container-bootable setup. Before the fedora template is able to run, you'll need to make sure that **yum** and **curl** are installed. A fedora 12 container can be created with

```
sudo lxc-create -t fedora -n fedora12 -- -R 12
```

A OpenSuSE template exists, but it requires the **zypper** program, which is not yet packaged. The OpenSuSE template is therefore not supported.

Two more templates exist mainly for experimental purposes. The busybox template creates a very small system container based entirely on busybox. The sshd template creates an application container running sshd in a private network namespace. The host's library and binary directories are bind-mounted into the container, though not its /home or /root. To create, start, and ssh into an ssh container, you might:

```
sudo lxc-create -t sshd -n ssh1
ssh-keygen -f id
sudo mkdir /var/lib/lxc/ssh1/rootfs/root/.ssh
sudo cp id.pub /var/lib/lxc/ssh1/rootfs/root/.ssh/authorized_keys
sudo lxc-start -n ssh1 -d
ssh -i id root@ssh1.
```

4.3.1.5. Backing Stores

By default, **lxc-create** places the container's root filesystem as a directory tree at /var/lib/lxc/CN/rootfs. Another option is to use LVM logical volumes. If a volume group named *lxc* exists, you can create an lvm-backed container called CN using:

```
sudo lxc-create -t ubuntu -n CN -B lvm
```

If you want to use a volume group named schroots, with a 5G xfs filesystem, then you would use

```
sudo lxc-create -t ubuntu -n CN -B lvm --vgname schroots --fssize 5G --fstype xfs
```

4.3.2. 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. Given an existing container called C1, a new container called C2 can be created using

```
sudo lxc-clone -o C1 -n C2
```

If `/var/lib/lxc` is a btrfs filesystem, then **lxc-clone** will create C2's filesystem as a snapshot of C1's. If the container's root filesystem is lvm backed, then you can specify the `-s` option to create the new rootfs as a lvm snapshot of the original as follows:

```
sudo lxc-clone -s -o C1 -n C2
```

Both lvm and btrfs snapshots will provide fast cloning with very small initial disk usage.

4.3.3. Starting and stopping

To start a container, use **lxc-start -n CN**. By default **lxc-start** will execute `/sbin/init` in the container. You can provide a different program to execute, plus arguments, as further arguments to **lxc-start**:

```
sudo lxc-start -n container /sbin/init loglevel=debug
```

If you do not specify the `-d` (daemon) option, then you will see a console (on the container's `/dev/console`, see [Τμήμα 4.3.6, “Consoles” \[372\]](#) for more information) on the terminal. If you specify the `-d` option, you will not see that console, and **lxc-start** will immediately exit success - even if a later part of container startup has failed.

You can use **lxc-wait** or **lxc-monitor** (see *Τμήμα 4.3.5, “Monitoring container status”*; [371]) to check on the success or failure of the container startup.

To obtain LXC debugging information, use `-o filename -l debuglevel`, for instance:

```
sudo lxc-start -o lxc.debug -l DEBUG -n container
```

Finally, you can specify configuration parameters inline using `-s`. However, it is generally recommended to place them in the container's configuration file instead. Likewise, an entirely alternate config file can be specified with the `-f` option, but this is not generally recommended.

While **lxc-start** runs the container's `/sbin/init`, **lxc-execute** uses a minimal init program called **lxc-init**, which attempts to mount `/proc`, `/dev/mqueue`, and `/dev/shm`, executes the programs specified on the command line, and waits for those to finish executing. **lxc-start** is intended to be used for *system containers*, while **lxc-execute** is intended for *application containers* (see *this article*²³ for more).

You can stop a container several ways. You can use **shutdown**, **poweroff** and **reboot** while logged into the container. To cleanly shut down a container externally (i.e. from the host), you can issue the **sudo lxc-shutdown -n CN** command. This takes an optional timeout value. If not specified, the command issues a SIGPWR signal to the container and immediately returns. If the option is used, as in **sudo lxc-shutdown -n CN -t 10**, then the command will wait the specified number of seconds for the container to cleanly shut down. Then, if the container is still running, it will kill it (and any running applications). You can also immediately kill the container (without any chance for applications to cleanly shut down) using **sudo lxc-stop -n CN**. Finally, **lxc-kill** can be used more generally to send any signal number to the container's init.

While the container is shutting down, you can expect to see some (harmless) error messages, as follows:

```
$ sudo poweroff
[sudo] password for ubuntu: =
```

```
$ =
```

```
Broadcast message from ubuntu@cn1
(/dev/lxc/console) at 18:17 ...
```

```
The system is going down for power off NOW!
* Asking all remaining processes to terminate...
```

²³ <https://www.ibm.com/developerworks/linux/library/l-lxc-containers/>


```
...done.  
* All processes ended within 1 seconds....  
...done.  
* Deconfiguring network interfaces...  
...done.  
* Deactivating swap...  
...fail!  
umount: /run/lock: not mounted  
umount: /dev/shm: not mounted  
mount: / is busy  
* Will now halt
```

A container can be frozen with **sudo lxc-freeze -n CN**. This will block all its processes until the container is later unfrozen using **sudo lxc-unfreeze -n CN**.

4.3.4. 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.

See *Τμήμα 4.4.5, “Other configuration options” [377]* 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.

4.3.5. 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.

4.3.6. 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 $1 \leq N \leq 4$). 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`.

4.3.7. Container Inspection

Several commands are available to gather information on existing containers. **`lxc-ls`** will report all existing containers in its first line of output, and all running containers in the second line. **`lxc-list`** provides the same information in a more verbose format, listing running containers first and stopped containers next. **`lxc-ps`** will provide lists of processes in containers. To provide **`ps`** arguments to **`lxc-ps`**, prepend them with `--`. For instance, for listing of all processes in container `plain`,

```
sudo lxc-ps -n plain -- -ef
```

lxc-info provides the state of a container and the pid of its init process. **lxc-cgroup** can be used to query or set the values of a container's control group limits and information. This can be more convenient than interacting with the **cgroup** filesystem. For instance, to query the list of devices which a running container is allowed to access, you could use

```
sudo lxc-cgroup -n CN devices.list
```

or to add `mknod`, `read`, and `write` access to `/dev/sda`,

```
sudo lxc-cgroup -n CN devices.allow "b 8:* rwm"
```

and, to limit it to 300M of RAM,

```
lxc-cgroup -n CN memory.limit_in_bytes 300000000
```

lxc-netstat executes **netstat** in the running container, giving you a glimpse of its network state.

lxc-backup will create backups of the root filesystems of all existing containers (except lvm-based ones), using **rsync** to back the contents up under `/var/lib/lxc/CN/rootfs.backup.1`. These backups can be restored using **lxc-restore**. However, **lxc-backup** and **lxc-restore** are fragile with respect to customizations and therefore their use is not recommended.

4.3.8. Destroying containers

Use **lxc-destroy** to destroy an existing container.

```
sudo lxc-destroy -n CN
```

If the container is running, **lxc-destroy** will exit with a message informing you that you can force stopping and destroying the container with

```
sudo lxc-destroy -n CN -f
```

4.3.9. Advanced namespace usage

One of the Linux kernel features used by LXC to create containers is private namespaces. Namespaces allow a set of tasks to have private mappings of names to resources for things like pathnames and process IDs. (See [Τμήμα 4.10, Πόροι](#); [383] for a link to more information). Unlike control groups and other mount features which are also used to create containers, namespaces cannot be manipulated using a filesystem interface. Therefore, LXC ships with the **lxc-unshare** program, which is mainly for testing. It provides the ability to create new tasks in private namespaces. For instance,

```
sudo lxc-unshare -s 'MOUNT|PID' /bin/bash
```

creates a bash shell with private pid and mount namespaces. In this shell, you can do

```
root@ubuntu:~# mount -t proc proc /proc
root@ubuntu:~# ps -ef
UID    PID  PPID  C  STIME TTY      TIME CMD
root    1    0  6 10:20 pts/9    00:00:00 /bin/bash
root   110    1  0 10:20 pts/9    00:00:00 ps -ef
```

so that **ps** shows only the tasks in your new namespace.

4.3.10. Ephemeral containers

Ephemeral containers are one-time containers. Given an existing container CN, you can run a command in an ephemeral container created based on CN, with the host's jdoe user bound into the container, using:

```
lxc-start-ephemeral -b jdoe -o CN -- /home/jdoe/run_my_job
```

When the job is finished, the container will be discarded.

4.3.11. Container Commands

Following is a table of all container commands:

Πίνακας 20.1. Container commands

Command	Synopsis
lxc-attach	(NOT SUPPORTED) Run a command in a running container
lxc-backup	Back up the root filesystems for all lvm-backed containers

Command	Synopsis
<code>lxc-cgroup</code>	View and set container control group settings
<code>lxc-checkconfig</code>	Verify host support for containers
<code>lxc-checkpoint</code>	(NOT SUPPORTED) Checkpoint a running container
<code>lxc-clone</code>	Clone a new container from an existing one
<code>lxc-console</code>	Open a console in a running container
<code>lxc-create</code>	Create a new container
<code>lxc-destroy</code>	Destroy an existing container
<code>lxc-execute</code>	Run a command in a (not running) application container
<code>lxc-freeze</code>	Freeze a running container
<code>lxc-info</code>	Print information on the state of a container
<code>lxc-kill</code>	Send a signal to a container's init
<code>lxc-list</code>	List all containers
<code>lxc-ls</code>	List all containers with shorter output than <code>lxc-list</code>
<code>lxc-monitor</code>	Monitor state changes of one or more containers
<code>lxc-netstat</code>	Execute <code>netstat</code> in a running container
<code>lxc-ps</code>	View process info in a running container
<code>lxc-restart</code>	(NOT SUPPORTED) Restart a checkpointed container
<code>lxc-restore</code>	Restore containers from backups made by <code>lxc-backup</code>
<code>lxc-setcap</code>	(NOT RECOMMENDED) Set file capabilities on LXC tools
<code>lxc-setuid</code>	(NOT RECOMMENDED) Set or remove <code>setuid</code> bits on LXC tools
<code>lxc-shutdown</code>	Safely shut down a container
<code>lxc-start</code>	Start a stopped container
<code>lxc-start-ephemeral</code>	Start an ephemeral (one-time) container
<code>lxc-stop</code>	Immediately stop a running container
<code>lxc-unfreeze</code>	Unfreeze a frozen container
<code>lxc-unshare</code>	Testing tool to manually unshare namespaces
<code>lxc-version</code>	Print the version of the LXC tools
<code>lxc-wait</code>	Wait for a container to reach a particular state

4.4. Configuration File

LXC containers are very flexible. The Ubuntu `lxc` package sets defaults to make creation of Ubuntu system containers as simple as possible. If you need more flexibility, this chapter will show how to fine-tune your containers as you need.

Detailed information is available in the **lxc.conf(5)** man page. Note that the default configurations created by the ubuntu templates are reasonable for a system container and usually do not need customization.

4.4.1. Choosing configuration files and options

The container setup is controlled by the LXC configuration options. Options can be specified at several points:

- During container creation, a configuration file can be specified. However, creation templates often insert their own configuration options, so we usually specify only network configuration options at this point. For other configuration, it is usually better to edit the configuration file after container creation.
- The file `/var/lib/lxc/CN/config` is used at container startup by default.
- **lxc-start** accepts an alternate configuration file with the `-f filename` option.
- Specific configuration variables can be overridden at **lxc-start** using `-s key=value`. It is generally better to edit the container configuration file.

4.4.2. Διαμόρφωση Δικτύου

Container networking in LXC is very flexible. It is triggered by the **lxc.network.type** configuration file entries. If no such entries exist, then the container will share the host's networking stack. Services and connections started in the container will be using the host's IP address. If at least one **lxc.network.type** entry is present, then the container will have a private (layer 2) network stack. It will have its own network interfaces and firewall rules. There are several options for **lxc.network.type**:

- **lxc.network.type=empty**: The container will have no network interfaces other than loopback.
- **lxc.network.type=veth**: This is the default when using the ubuntu or ubuntu-cloud templates, and creates a veth network tunnel. One end of this tunnel becomes the network interface inside the container. The other end is attached to a bridged on the host. Any number of such tunnels can be created by adding more **lxc.network.type=veth** entries in the container configuration file. The bridge to which the host end of the tunnel will be attached is specified with **lxc.network.link = lxcbr0**.
- **lxc.network.type=phys** A physical network interface (i.e. eth2) is passed into the container.

Two other options are to use vlan or macvlan, however their use is more complicated and is not described here. A few other networking options exist:

- **lxc.network.flags** can only be set to `up` and ensures that the network interface is up.
- **lxc.network.hwaddr** specifies a mac address to assign to the nic inside the container.
- **lxc.network.ipv4** and **lxc.network.ipv6** set the respective IP addresses, if those should be static.

- **lxc.network.name** specifies a name to assign inside the container. If this is not specified, a good default (i.e. eth0 for the first nic) is chosen.
- **lxc.network.lxcscript.up** specifies a script to be called after the host side of the networking has been set up. See the **lxc.conf(5)** manual page for details.

4.4.3. Control group configuration

Cgroup options can be specified using **lxc.cgroup** entries. **lxc.cgroup.subsystem.item = value** instructs LXC to set cgroup **subsystem**'s **item** to **value**. It is perhaps simpler to realize that this will simply write **value** to the file **item** for the container's control group for subsystem **subsystem**. For instance, to set the memory limit to 320M, you could add

```
lxc.cgroup.memory.limit_in_bytes = 320000000
```

which will cause 320000000 to be written to the file `/sys/fs/cgroup/memory/lxc/CN/limit_in_bytes`.

4.4.4. Rootfs, mounts and fstab

An important part of container setup is the mounting of various filesystems into place. The following is an example configuration file excerpt demonstrating the commonly used configuration options:

```
lxc.rootfs = /var/lib/lxc/CN/rootfs
lxc.mount.entry=proc /var/lib/lxc/CN/rootfs/proc proc nodev,noexec,nosuid 0 0
lxc.mount = /var/lib/lxc/CN/fstab
```

The first line says that the container's root filesystem is already mounted at `/var/lib/lxc/CN/rootfs`. If the filesystem is a block device (such as an LVM logical volume), then the path to the block device must be given instead.

Each **lxc.mount.entry** line should contain an item to mount in valid fstab format. The target directory should be prefixed by `/var/lib/lxc/CN/rootfs`, even if **lxc.rootfs** points to a block device.

Finally, **lxc.mount** points to a file, in fstab format, containing further items to mount. Note that all of these entries will be mounted by the host before the container init is started. In this way it is possible to bind mount various directories from the host into the container.

4.4.5. Other configuration options

- **lxc.cap.drop** can be used to prevent the container from having or ever obtaining the listed capabilities. For instance, including

lxc.cap.drop = sys_admin

will prevent the container from mounting filesystems, as well as all other actions which require `cap_sys_admin`. See the **capabilities(7)** manual page for a list of capabilities and their meanings.

- **lxc.aa_profile = lxc-CN-profile** specifies a custom Apparmor profile in which to start the container. See *Τμήμα 4.2.6, “Apparmor” [364]* for more information.
- **lxc.console=/path/to/consolefile** will cause console messages to be written to the specified file.
- **lxc.arch** specifies the architecture for the container, for instance `x86`, or `x86_64`.
- **lxc.tty=5** specifies that 5 consoles (in addition to `/dev/console`) should be created. That is, consoles will be available on `/dev/tty1` through `/dev/tty5`. The ubuntu templates set this value to 4.
- **lxc.pts=1024** specifies that the container should have a private (Unix98) devpts filesystem mount. If this is not specified, then the container will share `/dev/pts` with the host, which is rarely desired. The number 1024 means that 1024 ptys should be allowed in the container, however this number is currently ignored. Before starting the container init, LXC will do (essentially) a

sudo mount -t devpts -o newinstance devpts /dev/pts

inside the container. It is important to realize that the container should not mount devpts filesystems of its own. It may safely do bind or move mounts of its mounted `/dev/pts`. But if it does

sudo mount -t devpts devpts /dev/pts

it will remount the host's devpts instance. If it adds the `newinstance` mount option, then it will mount a new private (empty) instance. In neither case will it remount the instance which was set up by LXC. For this reason, and to prevent the container from using the host's ptys, the default Apparmor policy will not allow containers to mount devpts filesystems after the container's init has been started.

- **lxc.devttydir** specifies a directory under `/dev` in which LXC will create its console devices. If this option is not specified, then the ptys will be bind-mounted over `/dev/console` and `/dev/ttyN`. However, rare package updates may try to blindly `rm -f` and then `mknod` those devices. They will fail (because the file has been bind-mounted), causing the package

update to fail. When **lxc.devtttydir** is set to LXC, for instance, then LXC will bind-mount the console ptys onto `/dev/lxc/console` and `/dev/lxc/ttyN`, and subsequently symbolically link them to `/dev/console` and `/dev/ttyN`. This allows the package updates to succeed, at the risk of making future gettys on those consoles fail until the next reboot. This problem will be ideally solved with device namespaces.

- The **lxc.hook** options specify programs to run at various points in a container's life cycle. See *Τμήμα 4.3.4, “Lifecycle management hooks” [371]* for more information on these hooks. To have multiple hooks called at any point, list them in multiple entries. The possible values, whose precise meanings are described in *Τμήμα 4.3.4, “Lifecycle management hooks” [371]*, are
 - **lxc.hook.pre-start**
 - **lxc.hook.pre-mount**
 - **lxc.hook.mount**
 - **lxc.hook.start**
 - **lxc.hook.post-stop**
- The **lxc.include** option specifies another configuration file to be loaded. This allows common configuration sections to be defined once and included by several containers, simplifying updates of the common section.
- The **lxc.seccomp** option (introduced with Ubuntu 12.10) specifies a file containing a *seccomp* policy to load. See *Τμήμα 4.9, “Ασφάλεια” [382]* for more information on seccomp in lxc.

4.5. Updates in Ubuntu containers

Because of some limitations which are placed on containers, package upgrades at times can fail. For instance, a package install or upgrade might fail if it is not allowed to create or open a block device. This often blocks all future upgrades until the issue is resolved. In some cases, you can work around this by chrooting into the container, to avoid the container restrictions, and completing the upgrade in the chroot.

Some of the specific things known to occasionally impede package upgrades include:

- The container modifications performed when creating containers with the `--trim` option.
- Actions performed by `lxcguest`. For instance, because `/lib/init/fstab` is bind-mounted from another file, `mountall` upgrades which insist on replacing that file can fail.
- The over-mounting of console devices with ptys from the host can cause trouble with `udev` upgrades.
- Apparmor policy and devices cgroup restrictions can prevent package upgrades from performing certain actions.
- Capabilities dropped by use of **lxc.cap.drop** can likewise stop package upgrades from performing certain actions.

4.6. Libvirt LXC

Libvirt is a powerful hypervisor management solution with which you can administer Qemu, Xen and LXC virtual machines, both locally and remote. The libvirt LXC driver is a separate implementation from what we normally call *LXC*. A few differences include:

- Configuration is stored in xml format
- There no tools to facilitate container creation
- By default there is no console on `/dev/console`
- There is no support (yet) for container reboot or full shutdown

4.6.1. Converting a LXC container to libvirt-lxc

Τμήμα 4.3.1, *Creating Containers*; [366] showed how to create LXC containers. If you've created a valid LXC container in this way, you can manage it with libvirt. Fetch a sample xml file from

```
wget http://people.canonical.com/~serge/o1.xml
```

Edit this file to replace the container name and root filesystem locations. Then you can define the container with:

```
virsh -c lxc:/// define o1.xml
```

4.6.2. Creating a container from cloud image

If you prefer to create a pristine new container just for LXC, you can download an ubuntu cloud image, extract it, and point a libvirt LXC xml file to it. For instance, find the url for a root tarball for the latest daily Ubuntu 12.04 LTS cloud image using

```
url1=`ubuntu-cloudimg-query precise daily $arch --format "%{url}\n"`  
url=`echo $url1 | sed -e 's/.tar.gz/-root\0/'`  
wget $url  
filename=`basename $url`
```

Extract the downloaded tarball, for instance

```
mkdir $HOME/c1  
cd $HOME/c1
```

```
sudo tar xzf $filename
```

Download the xml template

```
wget http://people.canonical.com/~serge/o1.xml
```

In the xml template, replace the name o1 with c1 and the source directory `/var/lib/lxc/o1/rootfs` with `$HOME/c1`. Then define the container using

```
virsh define o1.xml
```

4.6.3. Interacting with libvirt containers

As we've seen, you can create a libvirt-lxc container using

```
virsh -c lxc:/// define container.xml
```

To start a container called *container*, use

```
virsh -c lxc:/// start container
```

To stop a running container, use

```
virsh -c lxc:/// destroy container
```

Note that whereas the **lxc-destroy** command deletes the container, the **virsh destroy** command stops a running container. To delete the container definition, use

```
virsh -c lxc:/// undefine container
```

To get a console to a running container, use

```
virsh -c lxc:/// console container
```

Exit the console by simultaneously pressing control and].

4.7. The lxcguest package

In the 11.04 (Natty) and 11.10 (Oneiric) releases of Ubuntu, a package was introduced called *lxcguest*. An unmodified root image could not be safely booted inside a container, but an image with the lxcguest package installed could be booted as a container, on bare hardware, or in a Xen, kvm, or VMware virtual machine.

As of the 12.04 LTS release, the work previously done by the lxcguest package was pushed into the core packages, and the lxcguest package was removed. As a result, an unmodified 12.04 LTS image can be booted as a container, on bare hardware, or in a Xen, kvm, or VMware virtual machine. To use an older release, the lxcguest package should still be used.

4.8. Python api

As of 12.10 (Quantal) a python3-lxc package is available which provides a python module, called **lxc**, for managing lxc containers. An example python session to create and start an Ubuntu container called c1, then wait until it has been shut down, would look like:

```
# 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 point in the future.
>>> c=lxc.Container("C1")
>>> c.create("ubuntu")
True
>>> c.start()
True
>>> c.wait("STOPPED")
True
```

Debug information for containers started with the python API will be placed in `/var/log/lxccontainer.log`.

4.9. Ασφάλεια

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. However, while stronger security is a goal for future releases, in 12.04 LTS the goal of the Apparmor policy is not to stop malicious actions but rather to stop accidental harm of the host by the guest. The details of AppArmor integration with lxc are in section *Τμήμα 4.2.6, “Apparmor” [364]*

4.9.1. 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 *Τμήμα 4.4.5, “Other configuration options” [377]* for details of how to configure a container to use seccomp. By default, no seccomp policy is loaded.

4.10. Πόροι

- The DeveloperWorks article *LXC: Linux container tools*²⁴ was an early introduction to the use of containers.
- The *Secure Containers Cookbook*²⁵ demonstrated the use of security modules to make containers more secure.
- Manual pages referenced above can be found at:

*capabilities*²⁶
*lxc.conf*²⁷

²⁴ <https://www.ibm.com/developerworks/linux/library/l-lxc-containers/>

²⁵ <http://www.ibm.com/developerworks/linux/library/l-lxc-security/index.html>

²⁶ <http://manpages.ubuntu.com/manpages/en/man7/capabilities.7.html>

²⁷ <http://manpages.ubuntu.com/manpages/en/man5/lxc.conf.5.html>

- The upstream LXC project is hosted at *Sourceforge*²⁸.
- LXC security issues are listed and discussed at *the LXC Security wiki page*²⁹
- 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.

²⁸ <http://lxc.sf.net>

²⁹ <http://wiki.ubuntu.com/LxcSecurity>

Κεφάλαιο 21. Συστοίχιση

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.

Για να ξεκινήσετε να χρησιμοποιείτε το drbd, πρώτα εγκαταστήστε τα απαραίτητα πακέτα. Σε ένα τερματικό πληκτρολογήστε:

```
sudo apt-get install drbd8-utils
```



Αν χρησιμοποιείτε τον *εικονικό πυρήνα* ως μέρος μιας εικονικής μηχανής, θα πρέπει να μεταγλωττίσετε (compile) χειροκίνητα την μονάδα drbd. Μπορεί να είναι ευκολότερο να εγκαταστήσετε το πακέτο linux-server στην εικονική μηχανή.

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. Ρυθμίσεις

Οι δύο υπολογιστές σε αυτό το παράδειγμα θα ονομαστούν *drbd01* και *drbd02*. Θα πρέπει να έχουν ρυθμισμένη επίλυση ονομάτων (name resolution) είτε μέσα από DNS ή με το αρχείο `/etc/hosts`. Δείτε το *Κεφάλαιο 8, Υπηρεσία ονομάτων τομέα (DNS) [145]* για λεπτομέρειες.

- Για να ρυθμίσετε το drbd, στο πρώτο μηχάνημα επεξεργαστείτε το `/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;
    }
}

```



Υπάρχουν πολλές άλλες επιλογές στο `/etc/drbd.conf`, αλλά για αυτό το παράδειγμα, οι προεπιλεγμένες τιμές είναι καλές.

- Τώρα αντιγράψτε το `/etc/drbd.conf` στο δεύτερο μηχάνημα:

```
scp /etc/drbd.conf drbd02:~
```

- Και στο `drbd02` μετακινήστε το αρχείο στο `/etc`:

```
sudo mv drbd.conf /etc/
```

- Τώρα, χρησιμοποιώντας το εργαλείο `drbdadm`, αρχικοποιήστε την αποθήκευση μετα-δεδομένων. Σε κάθε εξυπηρετητή εκτελέστε:

```
sudo drbdadm create-md r0
```

- Μετά, και στα δύο μηχανήματα, εκκινήστε την υπηρεσία `drbd`:

```
sudo service drbd start
```

- Στο `drbd01`, ή σε οποιοδήποτε σύστημα θέλετε να είναι το πρωτεύον (primary), πληκτρολογήστε το ακόλουθο:

```
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
```

Για να σταματήσετε να παρακολουθείτε τα αποτελέσματα, πιάστε `Ctrl+c`.

- Τέλος, προσθέστε ένα σύστημα αρχείων στο `/dev/drbd0` και προσαρτήστε το:

```

sudo mkfs.ext3 /dev/drbd0
sudo mount /dev/drbd0 /srv

```

1.2. Δοκιμή

Για να ελέγξετε πως τα δεδομένα συγχρονίζονται πραγματικά μεταξύ των υπολογιστών, αντιγράψτε κάποια αρχεία στον `drbd01`, τον πρωτεύοντα, στο `/srv`:

```
sudo cp -r /etc/default /srv
```

Μετά, αποπροσαρτήστε το /srv:

```
sudo umount /srv
```

Υποβιβάστε τον κύριο εξυπηρετητή στον ρόλο του δευτερεύοντος:

```
sudo drbdadm secondary r0
```

Τώρα στον *δευτερεύοντα* εξυπηρετητή *προβιβάστε* το στον ρόλο του *κύριου*:

```
sudo drbdadm primary r0
```

Τέλος, προσαρτήστε την κατάτμηση:

```
sudo mount /dev/drbd0 /srv
```

Χρησιμοποιώντας την εντολή *ls* θα πρέπει να δείτε το /srv/default αντιγραμμένο από τον πρώην *πρωτεύοντα* υπολογιστή *drbd01*.

1.3. Αναφορές

- Για περισσότερες πληροφορίες για το DRBD, δείτε τον *ιστότοπο του DRBD*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/raring/en/man5/drbd.conf.5.html>

³ <http://manpages.ubuntu.com/manpages/raring/en/man8/drbdadm.8.html>

⁴ <https://help.ubuntu.com/community/DRBD>

Κεφάλαιο 22. 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. Εγκατάσταση διακομιστή

Για να εγκαταστήσετε το openvpn πληκτρολογήστε σε ένα τερματικό:

```
sudo apt-get install openvpn
```

1.2. Δημόσιο κλειδί εγκατάστασης υποδομής

The first step in building an OpenVPN configuration is to establish a PKI (public key infrastructure). The PKI consists of:

- ένα ξεχωριστό πιστοποιητικό (επίσης γνωστό ως ένα δημόσιο κλειδί) και ιδιωτικό κλειδί για το διακομιστή και τον κάθε πελάτη, και
- 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. Πιστοποιητικό εγκατάστασης συγγραφέα

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/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
```

Μετά, επεξεργαστείτε το `/etc/openvpn/easy-rsa/vars` προσαρμόζοντας τα ακόλουθα στο περιβάλλον σας:

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="NC"
export KEY_CITY="Winston-Salem"
export KEY_ORG="Example Company"
export KEY_EMAIL="steve@example.com"
```

Πληκτρολογήστε τα παρακάτω για να δημιουργήσετε τον κύριο πιστοποιητικό συγγραφέα (CA) πιστοποιητικό και κλειδί:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-ca
```

1.2.2. Πιστοποιητικά Διακομιστή

Στη συνέχεια, θα δημιουργήσει ένα πιστοποιητικό και το ιδιωτικό κλειδί για το διακομιστή:

```
./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
```

Όλα τα πιστοποιητικά και τα κλειδιά έχουν δημιουργηθεί στον υποκατάλογο κλειδιά/. Η κοινή πρακτική είναι να τα αντιγράψετε στο `/etc/openvpn/`:

```
cd keys/
cp myservername.crt myservername.key ca.crt dh1024.pem /etc/openvpn/
```

1.2.3. Πιστοποιητικά Πελάτη

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
```

Αντιγράψτε τα ακόλουθα αρχεία στον πελάτη χρησιμοποιώντας μια ασφαλή μέθοδο:

- /etc/openvpn/ca.crt
- /etc/openvpn/easy-rsa/keys/client1.crt
- /etc/openvpn/easy-rsa/keys/client1.key

Δεδομένου ότι μόνο τα πιστοποιητικά πελάτη και τα κλειδιά απαιτούνται στο μηχάνημα του πελάτη, θα πρέπει να τα αποσύρετε από τον διακομιστή.

1.3. Απλή ρύθμιση παραμέτρων διακομιστή

Μαζί με την εγκατάσταση OpenVPN πήρατε για δείγμα αυτά τα αρχεία ρυθμίσεων (και πολλά περισσότερα, αν, αν επιλέξετε):

```
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
```

Ξεκινήστε με την αντιγραφή και την αποσυμπίεση του server.conf.gz στο φάκελο /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 dh1024.pem
```

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 syslog.

```
root@server:/etc/openvpn# service openvpn start
* Starting virtual private network daemon(s)...
* Autostarting VPN 'server' [ OK ]
```

Τώρα, ελέγξτε αν το OpenVPN δημιούργησε ένα περιβάλλον tun0.

```
root@server:/etc/openvpn# ifconfig tun0
tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.8.0.1 P-t-P:10.8.0.2 Mask:255.255.255.255
```

```
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
[...]
```

1.4. Απλή διαμόρφωση πελάτη

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-get install openvpn
```

Αυτή την φορά αντιγράψτε το αρχείο `client.conf` δείγμα αρχείου ρυθμίσεων στο φάκελο `/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
```

Τώρα ξεκινήστε τον πελάτη OpenVPN:

```
root@client:/etc/openvpn# service openvpn start
* Starting virtual private network daemon(s)...
* Autostarting VPN 'client' [ OK ]
```

Ελέγξτε αν δημιουργήθηκε ένα περιβάλλον `tun0` :

```
root@client:/etc/openvpn# ifconfig tun0
tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
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.

Ελέγξτε τις διαδρομές σας:

```
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. Πρώτη αντιμετώπιση προβλημάτων

Πρώτη αντιμετώπιση προβλημάτων

- Ελέγξτε το syslog σας , π.χ. `grep -i vpn /var/log/syslog`
- Μπορεί ο πελάτης να συνδεθεί με το μηχάνημα του διακομιστή; Ίσως ένα τείχος προστασίας εμποδίζει την πρόσβαση; Ελέγξτε το syslog του διακομιστή.
- Πελάτης και διακομιστής πρέπει να χρησιμοποιούν το ίδιο πρωτόκολλο και θύρα, π.χ. θύρα UDP 1194, δείτε θύρα και επιλογές ρυθμίσεων πρωτοκόλλου
- Πελάτης και διακομιστής πρέπει να χρησιμοποιούν ίδιες ρυθμίσεις σχετικά με τη συμπίεση, δείτε το αρχείο `comp-lzo` επιλογή ρυθμίσεων
- 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. Προηγμένες ρυθμίσεις δρομολογητή VPN στο διακομιστή

Το παραπάνω είναι πολύ απλό εργάζομενος με VPN. Ο πελάτης μπορεί να έχει πρόσβαση στις υπηρεσίες της μηχανής διακομιστή VPN μέσα από μια κρυπτογραφημένη σήραγγα. Αν θέλετε να προσεγγίσετε περισσότερους διακομιστές ή οτιδήποτε σε άλλα δίκτυα, ωθήστε ορισμένες γραμμές προς τους πελάτες. Π.χ. Εάν το δίκτυο της εταιρείας σας μπορεί να συνοψιστεί στο δίκτυο 192.168.0.0/16, θα μπορούσατε να ωθήσετε αυτή τη γραμμή προς τους πελάτες. Αλλά θα πρέπει επίσης να αλλάξει η δρομολόγηση για το δρόμο της επιστροφής - διακομιστές σας πρέπει να γνωρίζουν μια διαδρομή προς το δίκτυο του πελάτη VPN.

Ή μπορεί να ωθήσει μια προεπιλεγμένη πύλη για όλους τους πελάτες να στείλει όλη την κυκλοφορία τους στο διαδίκτυο μέσω της πύλης VPN πρώτα και από εκεί μέσω του τείχους προστασίας της εταιρείας στο διαδίκτυο. Αυτό το τμήμα σας δείχνει μερικές πιθανές επιλογές.

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
```

Πιέστε διακομιστές DNS για τον πελάτη.

```
push "dhcp-option DNS 10.0.0.2"  
push "dhcp-option DNS 10.1.0.2"
```

Επιτρέψτε την επικοινωνία πελάτη σε πελάτη

```
client-to-client
```

Ενεργοποίηση συμπίεσης στη σύνδεση VPN.

```
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-auth-pam.so login
```



Παρακαλούμε διαβάστε το OpenVPN *οδηγό καλύτερης ασφάλειας*¹ για περαιτέρω συμβουλές σε θέματα ασφαλείας.

1.6.2. Προηγμένη γεφυρωμένη διαμόρφωση VPN στο διακομιστή

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. Ετοιμάστε το περιβάλλον ρυθμίσεων για τη γεφύρωση του διακομιστή

Make sure you have the `bridge-utils` package installed:

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

¹ <http://openvpn.net/index.php/open-source/documentation/howto.html#security>

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

auto br0
iface br0 inet static
address 10.0.0.4
netmask 255.255.255.0
bridge_ports eth1
```

Σε αυτό το σημείο θα πρέπει να επανεκκινήσετε τη δικτύωση. Να είστε προετοιμασμένοι ότι αυτό δεν θα μπορέσει να λειτουργήσει όπως αναμένετε και ότι θα χάσετε την απομακρυσμένη σύνδεση. Βεβαιωθείτε ότι μπορείτε να λύσετε τα προβλήματα έχοντας τοπική πρόσβαση.

sudo service network restart

1.6.2.2. Ετοιμάστε τις ρυθμίσεις του διακομιστή για τη γεφύρωση

Επεξεργασθείτε το `/etc/openvpn/server.conf` αλλάζοντας τις ακόλουθες επιλογές σε:

```
;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
```

Στη συνέχεια το κάνετε εκτελέσιμο:

```
sudo chmod 755 /etc/openvpn/up.sh
```

Αφού διαμορφώσετε το διακομιστή, επανεκκινήστε το *openvpn* πληκτρολογώντας:

```
sudo service openvpn restart
```

1.6.2.3. Διαμόρφωση Πελάτη

Πρώτα εγκαταστήστε το *openvpn* στον (υπολογιστή) πελάτη:

```
sudo apt-get install openvpn
```

Στη συνέχεια με το διακομιστή ρυθμισμένο και τα πιστοποιητικά του πελάτη αντιγραμμένα στον κατάλογο */etc/openvpn/*, δημιουργήστε ένα αρχείο διαμόρφωσης πελάτη, αντιγράφοντας το παράδειγμα. Σε ένα τερματικό στο μηχάνημα πελάτη εισάγετε:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn
```

Τώρα επεξεργαστείτε το */etc/openvpn/client.conf* αλλάζοντας τις ακόλουθες επιλογές:

```
dev tap
;dev tun
```

Τέλος, επανεκκινήστε το *openvpn*:

```
sudo service openvpn restart
```

Τώρα θα πρέπει να μπορείτε να συνδεθείτε στο απομακρυσμένο LAN μέσω του VPN.

1.7. Εφαρμογές λογισμικού πελάτη

1.7.1. Linux διαχειριστής δικτύου GUI για το 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-get 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]?
```

Για να ενημερώνει το διαχειριστή δικτύου για την εγκατάσταση νέων πακέτων θα πρέπει να γίνει η επανεκκίνησή του:

```
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 or other special settings you set on the server. Now try to establish your VPN.

1.7.2. OpenVPN με GUI για 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 launch Tunnelblick from your Application folder.

```
# Δείγμα client.ovpn για το 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 με GUI για Win 7

First download and install the latest *OpenVPN Windows Installer*². OpenVPN 2.2.1 was the latest when this was written. Additionally download an alternative Open VPN Windows GUI. The OpenVPN MI GUI from <http://openvpn-mi-gui.inside-security.de> seems to be a nice one for Windows 7. Download the latest version. 20110624 was the latest version when this was written.

You need to start the OpenVPN service. Goto Start > Computer > Manage > Services and Applications > Services. Find the OpenVPN service and start it. Set its 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 following example.

```
# 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
```

² <http://www.openvpn.net/index.php/open-source/downloads.html>

```
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
```

1.7.4. OpenVPN για 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>

Συνδεθείτε στο OpenWRT δρομολογητή σας και εγκαταστήστε το OpenVPN:

opkg ενημέρωση
opkg install openvpn

Check out `/etc/config/openvpn` and put your client config in there. Copy certificated 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
```

Επανεκκίνηση OpenVPN:

service openvpn restart

Θα πρέπει να δείτε εάν πρέπει να ρυθμίσετε τη δρομολόγηση του δρομολογητή σας και τους κανόνες του τείχους προστασίας.

³ <http://wiki.openwrt.org/doc/howto/vpn.overview>

1.8. Αναφορές

- Δείτε την ιστοσελίδα *OpenVPN*⁴ για περισσότερες πληροφορίες.
- *OpenVPN hardening security guide*⁵
- Επίσης, το *OpenVPN: Building and Integrating Virtual Private Networks*⁶ είναι ένας καλός πόρος.

⁴ <http://openvpn.net/>

⁵ <http://openvpn.net/index.php/open-source/documentation/howto.html#security>

⁶ <http://www.packtpub.com/openvpn/book>

Κεφάλαιο 23. Άλλες Χρήσιμες Εφαρμογές

Υπάρχουν πολλές πολύ χρήσιμες εφαρμογές αναπτυγμένες από την Ομάδα Διακομιστή Ubuntu, και άλλες η οποίες είναι καλά ενσωματωμένες στην Έκδοση Διακομιστή Ubuntu, οι οποίες μπορεί να μην είναι γνωστές. Αυτό το κεφάλαιο θα δείξει μερικές χρήσιμες εφαρμογές που μπορεί να κάνει τη διαχείριση του διακομιστή Ubuntu, ή πολλών διακομιστών Ubuntu, πολύ πιο εύκολη.

1. pam_motd

Όταν εισέρχεστε σε ένα διακομιστή Ubuntu μπορεί να έχετε προσέξει το ενημερωτικό Μήνυμα της Ημέρας (MTH). Αυτές οι πληροφορίες αποκτούνται και προβάλλονται χρησιμοποιώντας μερικά πακέτα:

- *landscape-common*: παρέχει τις βιβλιοθήκες πυρήνα του landscape-client, που μπορεί να χρησιμοποιηθεί για τη διαχείριση συστημάτων χρησιμοποιώντας την εφαρμογή βασισμένη στον ιστό *Landscape*. Το πακέτο περιλαμβάνει τη λειτουργία `/usr/bin/landscape-sysinfo` η οποία χρησιμοποιείται για τη συλλογή πληροφοριών που προβάλλονται στο MTM.
- *update-notifier-common*: is used to automatically update the MOTD via `pam_motd` module.

`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`.

Μπορείτε να προσθέσετε τις δικές σας δυναμικές πληροφορίες στο MTM. Για παράδειγμα, για να προσθέσετε πληροφορίες για τον τοπικό καιρό:

- Πρώτον, εγκαταστήστε το πακέτο `weather-util`:

```
sudo apt-get install weather-util
```

- Η λειτουργία καιρού χρησιμοποιεί δεδομένα METAR από την Εθνική Ωκεάνια και Ατμοσφαιρική Διαχείριση και προβλέψεις από την Εθνική Υπηρεσία Καιρού. Για να βρείτε τοπικές πληροφορίες θα χρειαστείτε την τετραψήφια ένδειξη τοποθεσίας ICAO. Αυτό μπορεί να προσδιοριστεί κάνοντας περιήγηση της ιστοσελίδας *Εθνικής Υπηρεσίας Καιρού*¹.

Παρόλο που η Εθνική Υπηρεσία Καιρού είναι αντιπροσωπεία της κυβέρνησης των Ηνωμένων Πολιτειών υπάρχουν σταθμοί καιρού διαθέσιμοι σε όλο τον κόσμο. Παρ' όλα αυτά μπορεί να είναι διαθέσιμες πληροφορίες για όλες τις τοποθεσίες εκτός Η.Π.

- Δημιουργήστε το `/usr/local/bin/local-weather`, ένα απλό σενάριο πυρήνα για να χρησιμοποιήσει το καιρός με την τοπική ένδειξη ICAO:

```
#!/bin/sh
#
#
# Prints the local weather information for the MOTD.
#
#
```

¹ <http://www.weather.gov/tg/siteloc.shtml>

```
# 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
```

- Κάντε το σενάριο εκτελέσιμο:

```
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`.

2. etckeeper

Το `etckeeper` επιτρέπει τα περιεχόμενα του `/etc` να αποθηκεύονται εύκολα στο αποθετήριο Συστήματος Ελέγχου Έκδοσης (ΣΕΕ). Αγκιστρώνει στο `apt` για να παραδίδει αυτόματα αλλαγές στο `/etc` όταν εγκαθιστώνται ή αναβαθμίζονται πακέτα. Τοποθετώντας το `/etc` κάτω από τον έλεγχο έκδοσης θεωρείται βέλτιστη πρακτική του κλάδου, και ο στόχος του `etckeeper` είναι να κάνει αυτή τη διαδικασία όσο πιο ανώδυνη γίνεται.

Εγκαταστήστε το `etckeeper` πληκτρολογώντας τα ακόλουθα σε ένα τερματικό:

```
sudo apt-get install etckeeper
```

Το κύριο αρχείο διαμόρφωσης `/etc/etckeeper/etckeeper.conf`, είναι σχετικά απλό. Η κύρια επιλογή είναι ποιος ΕΕΣ να χρησιμοποιηθεί. Εξορισμού το `etckeeper` είναι διαμορφωμένο να χρησιμοποιεί το `bzr` για έλεγχο έκδοσης. Το αποθετήριο αρχικοποιείται αυτόματα (και παραδίδεται για πρώτη φορά) κατά την εγκατάσταση του πακέτου. Είναι πιθανό να το αναιρέσετε αυτό πληκτρολογώντας την ακόλουθη εντολή:

```
sudo etckeeper uninit
```

Εξορισμού, το `etckeeper` θα παραδώσει μη παραδοτέες αλλαγές που γίνονται στο `/etc` καθημερινά. Αυτό μπορεί να απενεργοποιηθεί χρησιμοποιώντας την επιλογή διαμόρφωσης `AVOID_DAILY_AUTOCOMMITS`. Θα παραδίδει επίσης αυτόματα αλλαγές πριν και μετά την εγκατάσταση πακέτου. Για μία πιο ακριβή καταγραφή αλλαγών, συστήνεται να παραδίνεται τις αλλαγές χειροκίνητα, μαζί με ένα μήνυμα παράδοσης, χρησιμοποιώντας:

```
sudo etckeeper commit "...Λόγος για αλλαγή διαμόρφωσης.."
```

Χρησιμοποιώντας επιλογές ΕΕΣ μπορείτε να προβάλετε πληροφορίες ιστορικού στο `/etc`:

```
sudo bzr log /etc/passwd
```

Για να επιδείξετε την ολοκλήρωση με το σύστημα διαχείρισης πακέτου, εγκαταστήστε το `postfix`:

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

Όταν η εγκατάσταση ολοκληρωθεί, όλα τα αρχεία διαμόρφωσης `postfix` θα πρέπει να παραδοθούν στο αποθετήριο:

```
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.
```

Για ένα παράδειγμα για το πως το `etckeeper` ανιχνεύει χειροκίνητες αλλαγές, προσθέστε ένα νέο κεντρικό υπολογιστή στο `/etc/hosts`. Χρησιμοποιώντας το `bzr` μπορείτε να δείτε ποια αρχεία έχουν τροποποιηθεί:

```
sudo bzr status /etc/
modified:
  hosts
```

Τώρα παραδώστε τις αλλαγές:

```
sudo etckeeper commit "new host"
```

Για περισσότερες πληροφορίες για το `bzr` βλ. *Τμήμα 1, “Bazaar” [291]*.

3. Byobu

One of the most useful applications for any system administrator is screen. It allows the execution of multiple shells in one terminal. To make some of the advanced screen features more user friendly, and provide some useful information about the system, the byobu package was created.

When executing byobu pressing the *F9* key will bring up the Configuration menu. This menu will allow you to:

- Προβολή του μενού Βοήθειας
- Change Byobu's background color
- Change Byobu's foreground color
- Toggle status notifications
- Αλλαγή του συνόλου των δεσμευτικών κλειδιών
- Αλλαγή της συχνότητας απόδρασης
- Create new windows
- Διαχείριση των προεπιλεγμένων παραθύρων
- 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* - Μετακίνηση του κέρσορα αριστερά κατά έναν χαρακτήρα
- *j* - Μετακίνηση του κέρσορα κάτω κατά μια γραμμή
- *k* - Μετακίνηση του κέρσορα πάνω κατά μία γραμμή
- *l* - Μετακίνηση του κέρσορα δεξιά κατά ένα χαρακτήρα
- *O* - Μετακίνηση στην αρχή της τρέχουσας γραμμής
- *\$* - Μετακίνηση στο τέλος της τρέχουσας γραμμής
- *G* - Μετακίνηση στην ορισμένη γραμμή (εξορισμού στο τέλος της διαθέσιμης μνήμης)

- \backslash - Αναζήτηση μπροστά
- $?$ - Αναζήτηση πίσω
- n - Μετακίνηση στο επόμενο ταίριασμα, είτε μπροστά είτε πίσω

4. Αναφορές

- See the *update-motd man page*² for more options available to update-motd.
- Το άρθρο για Debian Πακέτο της Ημέρας *καιρός*³ έχει περισσότερες λεπτομέρειες για τη χρήση της λειτουργίας καιρού
- Δείτε την ιστοσελίδα *etckeeper*⁴ για περισσότερες λεπτομέρειες για τη χρήση του etckeeper.
- The *etckeeper Ubuntu Wiki*⁵ page.
- Για τα τελευταία νέα και πληροφορίες για το bzr δείτε την ιστοσελίδα *bzr*⁶.
- Για περισσότερες πληροφορίες για την οθόνη δείτε την ιστοσελίδα *οθόνης*⁷.
- And the *Ubuntu Wiki screen*⁸ page.
- Also, see the *byobu project page*⁹ for more information.

² <http://manpages.ubuntu.com/manpages/raring/en/man1/update-motd.1.html>

³ <http://debaday.debian.net/2007/10/04/weather-check-weather-conditions-and-forecasts-on-the-command-line/>

⁴ <http://kitenet.net/~joey/code/etckeeper/>

⁵ <https://help.ubuntu.com/community/etckeeper>

⁶ <http://bazaar-vcs.org/>

⁷ <http://www.gnu.org/software/screen/>

⁸ <https://help.ubuntu.com/community/Screen>

⁹ <https://launchpad.net/byobu>

Παράρτημα Α. Appendix

1. Reporting Bugs in Ubuntu Server Edition

While the Ubuntu Project attempts to release software with as few bugs as possible, they do occur. You can help fix these bugs by reporting ones that you find to the project. The Ubuntu Project uses *Launchpad*¹ to track its bug reports. In order to file a bug about Ubuntu Server on Launchpad, you will need to *create an account*².

1.1. Reporting Bugs With ubuntu-bug

The preferred way to report a bug is with the `ubuntu-bug` command. The `ubuntu-bug` tool gathers information about the system useful to developers in diagnosing the reported problem that will then be included in the bug report filed on Launchpad. Bug reports in Ubuntu need to be filed against a specific software package, thus the name of the package that the bug occurs in needs to be given to `ubuntu-bug`:

`ubuntu-bug PACKAGENAME`

For example, to file a bug against the `openssh-server` package, you would do:

`ubuntu-bug openssh-server`

You can specify either a binary package or the source package for `ubuntu-bug`. Again using `openssh-server` as an example, you could also generate the report against the source package for `openssh-server`, `openssh`:

`ubuntu-bug openssh`



See *Κεφάλαιο 3, Διαχείριση Πακέτων [22]* for more information about packages in Ubuntu.

The `ubuntu-bug` command will gather information about the system in question, possibly including information specific to the specified package, and then ask you what you would like to do with collected information:

`ubuntu-bug postgresql`

*** Collecting problem information

The collected information can be sent to the developers to improve the application. This might take a few minutes.

.....

¹ <https://launchpad.net/>

² <https://help.launchpad.net/YourAccount/NewAccount>

*** 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 (1.7 KiB)

V: View report

K: Keep report file for sending later or copying to somewhere else

C: Cancel

Please choose (S/V/K/C):

The options available are:

- **Send Report** Selecting Send Report submits the collected information to Launchpad as part of the process of filing a bug report. You will be given the opportunity to describe the situation that led up to the occurrence of the bug.

*** Uploading problem information

The collected information is being sent to the bug tracking system.

This might take a few minutes.

91%

*** To continue, you must visit the following URL:

<https://bugs.launchpad.net/ubuntu/+source/postgresql-8.4/+filebug/kc6eSnTLnLxF8u0t3e56EukFeqJ?>

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):

If you choose to start a browser, by default the text based web browser w3m will be used to finish filing the bug report. Alternately, you can copy the given URL to a currently running web browser.

- **View Report** Selecting View Report causes the collected information to be displayed to the terminal for review.

Package: postgresql 8.4.2-2

PackageArchitecture: all

Tags: lucid

ProblemType: Bug

ProcEnviron:

LANG=en_US.UTF-8

SHELL=/bin/bash

```
Uname: Linux 2.6.32-16-server x86_64
Dependencies:
  adduser 3.112ubuntu1
  base-files 5.0.0ubuntu10
  base-passwd 3.5.22
  coreutils 7.4-2ubuntu2
...
```

After viewing the report, you will be brought back to the same menu asking what you would like to do with the report.

- **Keep Report File** Selecting Keep Report File causes the gathered information to be written to a file. This file can then be used to later file a bug report or transferred to a different Ubuntu system for reporting. To submit the report file, simply give it as an argument to the `ubuntu-bug` command:

```
What would you like to do? Your options are:
S: Send report (1.7 KiB)
V: View report
K: Keep report file for sending later or copying to somewhere else
C: Cancel
Please choose (S/V/K/C): k
Problem report file: /tmp/apport.postgresql.v4MQas.apport
```

```
ubuntu-bug /tmp/apport.postgresql.v4MQas.apport
```

```
*** Send problem report to the developers?
...
```

- **Cancel** Selecting Cancel causes the collected information to be discarded.

1.2. Reporting Application Crashes

The software package that provides the `ubuntu-bug` utility, `apport`, can be configured to trigger when applications crash. This is disabled by default, as capturing a crash can be resource intensive depending on how much memory the application that crashed was using as `apport` captures and processes the core dump.

Configuring `apport` to capture information about crashing applications requires a couple of steps. First, `gdb` needs to be installed; it is not installed by default in Ubuntu Server Edition.

```
sudo apt-get install gdb
```

See *Κεφάλαιο 3, Διαχείριση Πακέτων [22]* for more information about managing packages in Ubuntu.

Once you have ensured that `gdb` is installed, open the file `/etc/default/apport` in your text editor, and change the *enabled* setting to be **1** like so:

```
# set this to 0 to disable apport, or to 1 to enable it
# you can temporarily override this with
# sudo service apport start force_start=1
enabled=1

# set maximum core dump file size (default: 209715200 bytes == 200 MB)
maxsize=209715200
```

Once you have completed editing `/etc/default/apport`, start the apport service:

sudo start apport

After an application crashes, use the `apport-cli` command to search for the existing saved crash report information:

apport-cli

```
*** dash closed unexpectedly on 2010-03-11 at 21:40:59.
```

If you were not doing anything confidential (entering passwords or other private information), you can help to improve the application by reporting the problem.

What would you like to do? Your options are:

R: Report Problem...

I: Cancel and ignore future crashes of this program version

C: Cancel

Please choose (R/I/C):

Selecting *Report Problem* will walk you through similar steps as when using `ubuntu-bug`. One important difference is that a crash report will be marked as private when filed on Launchpad, meaning that it will be visible to only a limited set of bug triagers. These triagers will review the gathered data for private information before making the bug report publicly visible.

1.3. Πόροι

- See the *Reporting Bugs*³ Ubuntu wiki page.
- Also, the *Apport*⁴ page has some useful information. Though some of it pertains to using a GUI.

³ <https://help.ubuntu.com/community/ReportingBugs>

⁴ <https://wiki.ubuntu.com/Apport>