

# Οδηγός Διακομιστή **Ubuntu**

---

# Οδηγός Διακομιστή Ubuntu

Πνευματικό Δικαίωμα © 2012 Contributors to the document

## Περλήψη

Καλ#ς #ρθατε στον #####μ##### Ubuntu! Περι#χει πληροφορ#ες για το πως να εγκαταστ#σετε και να διαμορφ#σετε προηγ#μενες εφαρμογ#ς διακομιστ# στο σ#στημα Ubuntu σας για να ταιρι#ζει στις αν#γκες σας. Ε#ναι #νας β#μα#προςβ#μα, προσανατολισμ#νος σε διεργασ#ες οδηγ#ς για να διαμορφ#σετε και να προσαρμ#σετε το σ#στημ# σας.

## Συντελεστ#ς και #δεια Χρ#σης

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).

Ε#στε ελε#θεροι να τροποποι#σετε, να επεκτε#νετε, και να βελτι#σετε τον πηγα#ο κ#δικα του Ubuntu υπ# τους #ρους της παρο#σας #δειας. #λα τα παραγ#μενα #ργα πρ#πει να δημοσιε#ονται με αυτ# την #δεια.

Αυτ# η τεκμηρ#ωση διαν#μεται με την ελπ#δα #τι θα ε#ναι χρ#σιμη, αλλ# ΧΩΡΙΣ ΚΑΜΙΑ ΕΓΓΥΗΣΗ, χωρ#ς ακ#μη και την #μμεση εγγ#ηση ΕΜΠΟΡΕΥΣΙΜΟΤΗΤΑΣ # ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ ΓΙΑ ΕΝΑ ΣΥΓΚΕΚΡΙΜΕΝΟ ΣΚΟΠΟ ΟΠΩΣ ΠΕΡΙΓΡΑΦΕΤΑΙ ΣΤΗΝ ΑΠΟΠΟΙΗΣΗ.

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

Contributors to this document are:

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

---

<sup>1</sup> <http://creativecommons.org/licenses/by-sa/3.0/>

<sup>2</sup> <https://launchpad.net/~ubuntu-core-doc>

<sup>3</sup> <https://launchpad.net/~ubuntu-server>

<sup>4</sup> <https://help.ubuntu.com/community/>

<sup>5</sup> <https://code.launchpad.net/serverguide>

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

---

## Πίνακας Περιεχομένων

1. Εισαγωγή	1
1. Υποστήριξη	2
2. Εγκατάσταση	3
1. Προετοιμασία εγκατάστασης	4
2. Εγκατάσταση απ CD	6
3. Αναβίθμιση	9
4. Εγκατάσταση για προχωρημένους	10
5. Kernel Crash Dump	18
3. Διαχείριση Πακέτων	21
1. Εισαγωγή	22
2. dpkg	23
3. Apt-Get	25
4. Aptitude	27
5. Αυτμάτες Ενημερώσεις	29
6. Ρυθμίσεις	31
7. Αναφορές	33
4. Δίκτυωση	34
1. Διαμόρφωση Δικτύου	35
2. TCP/IP	44
3. Πρωτόκολλο Δυναμικής Διαμόρφωσης Κεντρικού Υπολογιστή (Dynamic Host Configuration Protocol (DHCP))	49
4. Συγχρονισμός ραβδών με NTP	52
5. DM-Multipath	54
1. Device Mapper Multipathing	55
2. Multipath Devices	58
3. Setting up DM-Multipath Overview	61
4. The DM-Multipath Configuration File	65
5. DM-Multipath Administration and Troubleshooting	77
6. Απομακρυσμένη Διαχείριση	82
1. OpenSSH Server	83
2. Puppet	86
3. Zentyal	89
7. Πιστοποίηση δικτύου	93
1. Εξυπηρέτηση OpenLDAP	94
2. Samba και LDAP	120
3. Kerberos	126
4. Kerberos και LDAP	134
8. Υπηρεσία ονομάτων τομέα (DNS)	141
1. Εγκατάσταση	142
2. Ρυθμίσεις	143

3. Επ#λυση Προβλημ#των .....	149
4. Αναφορ#ς .....	153
9. Ασφ#λεια .....	155
1. Διαχε#ριση Χρηστ#ν .....	156
2. Ασφ#λεια Κονσ#λας .....	162
3. Τε#χος Προστασ#ας .....	163
4. AppArmor .....	171
5. Πιστοποιητικ# .....	175
6. eCryptfs .....	181
10. Παρακολο#θηση .....	184
1. Επισκ#πηση .....	185
2. Nagios .....	186
3. Munin .....	191
11. Διακομιστ#ς Ιστο# .....	193
1. HTTPD - Apache2 Διακομιστ#ς Ιστο# .....	194
2. PHP5 - Γλ#σσα Σεναρ#ου .....	203
3. Squid - Διακομιστ#ς Διαμεσολαβητ# .....	206
4. Ruby on Rails .....	209
5. Apache Tomcat .....	211
12. Β#σεις δεδομ#νων .....	215
1. MySQL .....	216
2. PostgreSQL .....	221
13. Εφαρμογ#ς LAMP .....	224
1. Επισκ#πηση .....	225
2. Moin Moin .....	226
3. MediaWiki .....	228
4. phpMyAdmin .....	230
5. WordPress .....	232
14. Εξυπηρετητ#ς αρχε#ων .....	235
1. Εξυπηρετητ#ς FTP .....	236
2. Σ#στημα Αρχε#ων Δικτ#ου (NFS) .....	240
3. #ρχικοποιητ#ς iSCSI .....	242
4. CUPS - Εξυπηρετητ#ς εκτυπ#σεων .....	245
15. Υπηρεσ#ες Ηλ. Αλληλογραφ#ας .....	248
1. Postfix .....	249
2. Exim4 .....	257
3. Εξυπηρετητ#ς Dovecot .....	260
4. Mailman .....	262
5. Φ#λτρα ηλ. αλληλογραφ#ας .....	269
16. Εφαρμογ#ς συζ#τησης .....	276
1. Επισκ#πηση .....	277
2. Εξυπηρετητ#ς IRC .....	278

3. Εξυπηρετητής μέσης ανταλλαγής μηνυμάτων Jabber .....	280
17. Σύστημα Ελέγχου Κώδους .....	282
1. Bazaar .....	283
2. Subversion .....	284
3. Διακομιστής CVS .....	290
4. Αναφορές .....	292
18. Samba .....	293
1. Εισαγωγή .....	294
2. File Server .....	295
3. Διακομιστής Εκτύπωσης .....	298
4. Securing File and Print Server .....	300
5. As a Domain Controller .....	305
6. Active Directory Integration .....	310
19. Αντιγραφή ασφαλείας .....	313
1. Σενάριο εντολών κελύφους .....	314
2. Archive Rotation .....	319
3. Bacula .....	322
20. Εικονικοποίηση .....	328
1. libvirt .....	329
2. JeOS και vmbuilder .....	335
3. Ubuntu Cloud .....	345
4. LXC .....	352
21. Σύστοχιση .....	375
1. DRBD .....	376
22. VPN .....	379
1. OpenVPN .....	380
23. Άλλες Χρήσιμες Εφαρμογές .....	392
1. pam_motd .....	393
2. etckeeper .....	395
3. Byobu .....	397
4. Αναφορές .....	399
A. Appendix .....	400
1. Reporting Bugs in Ubuntu Server Edition .....	401

---

## Κατ#λογος Πιν#κων

2.1. Προτειν#μενες ελ#χιστες απαιτ#σεις .....	4
5.1. Priority Checker Conversion .....	55
5.2. DM-Multipath Components .....	56
5.3. Multipath Configuration Defaults .....	69
5.4. Multipath Attributes .....	73
5.5. Device Attributes .....	75
5.6. Useful multipath Command Options .....	80
17.1. Μ#θοδοι Πρ#σβασης .....	285
20.1. Container commands .....	365

---

# Κεφάλαιο 1. Εισαγωγή

Καλωσορίσατε στον *##### Ubuntu!*

Εάν μπορείτε να βρείτε πληροφορίες για το πώς θα εγκαταστήσετε και θα ρυθμίσετε διάφορες εφαρμογές εξυπηρετητών. Είναι ένας εργοστροφός 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 *##### 2, ##### [3]*, but if you need detailed instructions installing Ubuntu please refer to the *Ubuntu Installation Guide*<sup>1</sup>.

A HTML version of the manual is available online at *the Ubuntu Documentation website*<sup>2</sup>.

---

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

<sup>2</sup> <https://help.ubuntu.com>

## **1. #####**

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*<sup>3</sup> page.

Παράχεται επίσης υποστήριξη κοινότητας από ξεχωριστά άτομα και εταιρίες, που επιθυμούν να κνουν το Ubuntu την καλύτερη δυνατή διανομή. Η υποστήριξη παράχεται μέσω πολλών λιστών αλληλογραφίας, καναλιών IRC, φθρουμ, ιστολογίων, wiki, κτλ. Το μεγάλο ποσό διαθέσιμης πληροφορίας μπορεί να γίνει αφρητο, αλλά να καλ# ερ#τημα σε κάποια μηχανή αναζήτησης μπορεί συνθως να απαντήσει στις ερωτήσεις σας. Δείτε την ##### ##### ##### ## Ubuntu<sup>4</sup> # την αγγλική σελίδα Ubuntu Support<sup>5</sup> για περισσότερες πληροφορίες.

---

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

<sup>4</sup> <http://wiki.ubuntu-gr.org/Support>

<sup>5</sup> <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*<sup>1</sup>.

---

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

## 1. #####μ#####

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

### 1.1. #####μ#####

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	Κεντρικός μονάδα επεξεργασίας (CPU)	RAM	Χρόνος 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 παρήχει μια κοινή βάση για όλων των ειδών τις εφαρμογές εξυπηρέτησης. Είναι ένας μινιμαλιστικός σχεδιασμός που παρήχει μια πλατφόρμα για τις επιθυμητές υπηρεσίες, όπως υπηρεσίες αρχείων/εκτυπώσεων, φιλοξενία ιστοσελίδων, φιλοξενία ηλεκτρονικών αλληλογραφιών, κτλ.

### 1.2. #####μ##### Server ### 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. #####μ#####:

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.



ήταν εκτελέσει μια έκδοση 64-bit του Ubuntu σε επεξεργαστές 64-bit δεν περιορίζετε απ 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*<sup>2</sup> is a great resource on the options available.

### 1.3. #####

- Πριν εγκαταστήσετε το Ubuntu Server Edition, θα πρέπει να σιγουρευτείτε πως έχετε κρατήσει αντιγραφο ασφαλείας απ' όλα τα δεδομένα στο σύστημα. Δείτε το [19, ##### \[313\]](#) για επιλογές διατήρησης αντιγράφων ασφαλείας.

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

Κάθε φορά που δημιουργείτε κατατμήσεις στον δίσκο σας, θα πρέπει να έχετε προετοιμασμένοι να χύσετε τα πάντα στον δίσκο αν κνέτε κάποιο λάθος ή κάτι πει στραβί κατά την κατάτμηση. Τα προγράμματα που χρησιμοποιούνται στην εγκατάσταση είναι αρκετά αξιόπιστα και τα περισσότερα χρησιμοποιούνται για χρόνια, αλλά εκτελούν επεργασίες και καταστρεπτικές ενέργειες.

---

<sup>2</sup> <http://www.kroah.com/lkn/>

## 2. ##### ## 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*<sup>3</sup>.
- Εκκιν#στε το σ#στημα απ# τον οδηγ# 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 πρ#γραμμά εγκατ#στασης μετ# εξερευνε# τις ρυθμ#σεις του υλικο# σας και ρυθμ#ζει τις επιλογ#ς δικτ#ου χρησιμοποιντας DHCP. Αν δεν επιθυμε#τε να χρησιμοποισετε DHCP, στην επ#μενη οθ#νη επιλ#ξτε #Π#σω# και θα #χετε την επιλογ# να ρυθμ#σετε το δ#κτυο χειροκ#νητα.
- Μετ#, το πρ#γραμμά εγκατ#στασης ζητ#ει το #νομά του συστ#ματος και τη ζ#νη #ρας.
- 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 #μ#μ# 4, &#x201C;#####  
### #####μ#####&#x201D; [10].
- Το βασικ# σ#στημα του Ubuntu ε#ναι τ#τε εγκατεστημ#νο.
- 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 επ#μενο β#μα στην διαδικασ#α εγκατ#στασης ε#ναι να αποφασ#σετε π#ς θ#λετε να ενημερ#νεται το σ#στημα. Υπ#ρχουν τρεις επιλογ#ς:
  - #####μ#####μ#####: αυτ# χρει#ζεται #ναν διαχειριστ# να συνδ#εται στο μηχ#νημα και να εγκαθιστ# τις ενημερ#σεις χειροκ#νητα.
  - *Install security updates automatically*: this will install the unattended-upgrades package, which will install security updates without the intervention of an administrator. For more details see #μ#μ# 5, &#x201C;#####μ#####μ#####&#x201D; [29].

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

- ##### μ# ## Landscape: Το Landscape είναι μια υπηρεσία επιπληρωμ# που παρ#χεται απ# την Canonical για να βοηθ#σει στη διαχε#ριση των μηχανημ#των Ubuntu σας. Δε#τε τον ιστ#τοπο του Landscape<sup>4</sup> για λεπτομ#ρειες.
- Τ#ρα #χετε την επιλογ# να εγκαταστ#σετε, # να μην εγκαταστ#σετε, αρκετ#ς εργασ#ες πακ#των. Δε#τε το μ#μ# 2.1, &#x201C;#####&#x201D; [7] για λεπτομ#ρειες. Επ#σης, υπ#ρχει μια επιλογ# που εκκινε# το aptitude #στε να επιλ#ξετε συγκεκριμ#να πακ#τα για εγκατ#σταση. Για περισσ#τερες πληροφορ#ες δε#τε το μ#μ# 4, &#x201C;Aptitude&#x201D; [27].
- Τ#λος, το τελευτα#ο β#μα πριν την επανεκκ#νηση, ε#ναι να ρυθμιστε# το ρολ#ι σε UTC.



Αν σε οποιοδ#ποτε σημειο κατ# την εγκατ#σταση δεν ε#σαστε ικανοποιημ#νοι απ# τις προεπιλεγμ#νες ρυθμ#σεις, χρησιμοποιο#στε τη λειτουργ#α #Π#σω#, σε οποιοδ#ποτε σημειο, για να μεταβε#τε σε #να λεπτομερ#ς μενο# εγκατ#στασης που θα σας επιτρ#ψει να τροποποι#σετε τις προεπιλεγμ#νες ρυθμ#σεις.

Σε κ#ποιο σημειο κατ# την διαδικασ#α εγκατ#στασης, μπορε# να θ#λετε να διαβ#σετε την οθ#νη βο#θειας που παρ#χεται απ# το σ#στημα εγκατ#στασης. Για να το κ#νετε αυτ#, πι#στε F1.

Once again, for detailed instructions see the *Ubuntu Installation Guide*<sup>5</sup>.

## 2.1. #####

Κατ# την εγκατ#σταση της Server Edition, #χετε την επιλογ# να εγκαταστ#σετε επιπλ#ον πακ#τα απ# το CD. Τα πακ#τα ομαδοποιο#νται σμ#φωνα με το ε#δος των υπηρεσι#ν που προσφ#ρουν.

- Εξυπηρετητ#ς DNS: Επιλ#γει τον εξυπηρετητ# BIND DNS και την τεκμηρ#ωσ# του.
- Εξυπηρετητ#ς LAMP: Επιλ#γει #ναν #τοίμο εξυπηρετητ# Linux/Apache/MySQL/PHP.
- Mail server: This task selects a variety of packages useful for a general purpose mail server system.
- Εξυπηρετητ#ς OpenSSH: Επιλ#γει πακ#τα που χρει#ζονται για #ναν εξυπηρετητ# OpenSSH.
- Β#ση δεδομ#νων PostgreSQL: Αυτ# η εργασ#α επιλ#γει πακ#τα πελ#τη και εξυπηρετητ# για τη β#ση δεδομ#νων PostgreSQL.
- Εξυπηρετητ#ς εκτυπ#σεων: Αυτ# η εργασ#α ρυθμ#ζει το σ#στημ# σας #στε να ε#ναι #νας εξυπηρετητ#ς εκτυπ#σεων.
- Εξυπηρετητ#ς αρχε#ων Samba: Αυτ# η εργασ#α ρυθμ#ζει το σ#στημ# σας #στε να ε#ναι #νας εξυπηρετητ#ς αρχε#ων Samba, που ε#ναι ειδικ# κατ#λληλος σε δ#κτυα με συστ#ματα Windows και Linux.
- Tomcat Java server: Installs Apache Tomcat and needed dependencies.

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

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

- 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 provide a fully integrated service.

Με τις διαδικασίες εγκατάστασης ολοκληρωθεί μπορείτε να εμφανίσετε μια λίστα με διαθέσιμες εργασίες πληκτρολογώντας το ακόλουθο σε ένα τερματικό:

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



Το αποτέλεσμα θα εμφανίσει εργασίες απλές 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 διαθέσιμες εργασίες.

Μπορείτε να δείτε μια λίστα των πακέτων που έχουν εγκατασταθεί με κάθε εργασία χρησιμοποιώντας την επιλογή *--task-packages*. Για παράδειγμα, για να δείτε τα πακέτα που εγκαταστήθηκαν με τον *##### 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. #####μ###

Υπάρχουν αρκετοί τρόποι για να αναβαθμίσετε μια έκδοση του Ubuntu σε μια 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 γραφική περιβάλλον και είναι εγκατεστημένο απ' 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 πληκτρολογείτε:

```
do-release-upgrade
```

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

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



Η αναβάθμιση σε έκδοση που βρίσκεται υπ' ανάπτυξη <sup>###</sup> συνιστάται για περιβάλλοντα παραγωγής.

## 4. ##### μ#####

### 4.1. RAID #####

Redundant Array of Independent Disks "RAID" is a method of using multiple disks to provide different balances of increasing data reliability and/or increasing input/output performance, depending on the RAID level being used. RAID is implemented in either software (where the operating system knows about both drives and actively maintains both of them) or hardware (where a special controller makes the OS think there's only one drive and maintains the drives 'invisibly').

Το λογισμικ# RAID που περι#χεται στις τρ#χουσες εκδ#σεις του Linux (και του Ubuntu) βασ#ζεται στον οδηγ# 'mdadm' και δουλε#ει πολ# καλ#, καλ#τερα ακ#μη απ# πολλο#ς ξακουστο#ς ελεγκτ#ς RAID υλικο#. Αυτ# η εν#τητα θα σας καθοδηγ#σει στην εγκατ#σταση του Ubuntu Server Edition χρησιμοποιντας δ#ο κατατμ#σεις RAID1 σε δ#ο φυσικο#ς σκληρο#ς δ#σκους, #ναν για το / και τον #λλον για το *swap*.

#### 4.1.1. #####

Ακολουθ#στε τα β#ματα εγκατ#στασης μ#χρι να φτ#σετε στο β#μα #####, μετ#:

1. Επιλ#ξτε ##### ως την μ#θοδο διαμ#ρισης.
2. Επιλ#ξτε τον πρ#το σκληρ# δ#σκο, και συμφων#στε στη "#####  
#####".

Επαναλ#βετε αυτ# το β#μα για κ#θε συσκευ# που επιθυμε#τε να ε#ναι μ#ρος της δι#ταξης RAID.

3. Επιλ#ξτε το "#####" στην πρ#τη συσκευ# και μετ# επιλ#ξτε "#####  
#####".
4. Μετ# επιλ#ξτε το ##### της κατ#τμησης. Αυτ# η κατ#τμηση θα ε#ναι η κατ#τμηση του *swap* και #νας γενικ#ς καν#νας για το μ#γεθος του *swap* ε#ναι το διπλ#σιο εκε#νου της RAM. Εισαγ#γετε το μ#γεθος της κατ#τμησης, μετ# επιλ#ξτε ##### και μετ# #####.



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. Επιλ#ξτε τη γραμμ# "##### #:." στην κορυφ#. Απ# προεπιλογ# αυτ# ε#ναι "#####μ#  
##### ext4 μ# journal", αλλ#ξτε το σε "##### μ# ## RAID" και μετ# επιλ#ξτε "#####  
#####".
6. Για την κατ#τμηση / για μ#α ακ#μη φορ#, επιλ#ξτε "#####" στην πρ#τη συσκευ# και μετ# "#####μ#".
7. Χρησιμοποι#στε τον υπ#λοιπο ελε#θερο χ#ρο της συσκευ#ς και επιλ#ξτε ##### και μετ# #####.



8. #πως με την κατ#τμηση του *swap*, επιλ#ξτε τη γραμμ# "##### #:" στην κορυφ#, αλλ#ζοντ#ς την σε "##### μ### ## RAID". Επ#σης επιλ#ξτε τη γραμμ# "#####μ#:" για να αλλ#ξτε την τιμ# σε "###". Μετ# επιλ#ξτε "##### ## μ##### ## μ#####".
9. Επαναλ#βετε τα β#ματα τρ#α #ως οκτ# για τους #λλους δ#σκους και κατατμ#σεις.

#### 4.1.2. ##### RAID

Με τις κατατμ#σεις να #χουν δημιουργηθε#, οι διατ#ξεις ε#ναι #τοιμες να ρυθμιστο#ν:

1. Π#σω στην κ#ρια σελ#δα #Διαμ#ριση δ#σκων#, επιλ#ξτε "###μ### RAID #####μ#####" στην κορυφ#.
2. Επιλ#ξτε "####" για να εγγραφο#ν οι αλλαγ#ς στον δ#σκο.
3. Επιλ#ξτε "##μ##### μ##### MD".
4. Για αυτ# το παρ#δειγμα, επιλ#ξτε "RAID1", αλλ# αν χρησιμοποιε#τε διαφορετικ# εγκατ#σταση, επιλ#ξτε τον κατ#λληλο τ#πο (RAID0 RAID1 RAID5).



Για να χρησιμοποι#σετε *RAID5* χρει#ζεστε τουλ#χιστον ##### συσκευ#ς. Χρησιμοποι#ντας RAID0 # RAID1, απαιτο#νται μ#νο ### συσκευ#ς.

5. Πληκτρολογ#στε τον αριθμ# των ενεργ#ν συσκευ#ν - "2", # τον αριθμ# των σκληρ#ν δ#σκων που #χετε - για τη συστοιχ#α. Μετ# επιλ#ξτε "#####".
6. Μετ#, πληκτρολογ#στε τον αριθμ# των εφεδρικ#ν συσκευ#ν - "0" απ# προεπιλογ# - και επιλ#ξτε "#####".
7. Επιλ#ξτε ποιες κατατμ#σεις θα χρησιμοποιηθο#ν. Γενικ#, αυτ#ς θα ε#ναι *sda1*, *sdb1*, *sdc1*, κτλ. Οι αριθμο# συν#θως θα ταιρι#ζουν, και τα διαφορετικ# γρ#μματα αντιστοιχο#ν σε διαφορετικο#ς σκληρο#ς δ#σκους.

Για την κατ#τμηση του *swap* επιλ#ξτε τα *sda1* και *sdb1*. Επιλ#ξτε "#####" για να προχωρ#σετε στο επ#μενο β#μα.

8. Επαναλ#βετε τα β#ματα ##### #ως ##### για την κατ#τμηση / επιλ#γοντας τα *sda2* και *sdb2*.
9. Μ#λεις τελει#σετε, επιλ#ξτε "#####".

#### 4.1.3. #####

Τρ#α θα πρ#πει να υπ#ρχει μια λ#στα σκληρ#ν δ#σκων και συσκευ#ν RAID. Το επ#μενο β#μα ε#ναι να διαμορφ#σετε και να ορ#σετε το σημειο προσ#ρτησης για τις συσκευ#ς RAID. Αντιμετωπ#στε τη συσκευ# RAID ως #ναν τοπικ# σκληρ# δ#σκο, διαμορφ#στε και προσαρτ#στε αναλ#γως.

1. Επιλ#ξτε "#1" κ#τω απ# την κατ#τμηση "RAID1 device #0"
2. Επιλ#ξτε "##### #:". Μετ# επιλ#ξτε "##### μ###μ###", μετ# "##### ## μ##### ## μ#####".

3. Μετ# επιλ#ξτε "#1" κ#τω απ# την κατ#τμηση "RAID1 device #1".
4. Επιλ#ξτε "##### #: ". Μετ# επιλ#ξτε "#####μ# ##### ext4 μ# journal".
5. Μετ# επιλ#ξτε το "###μ### #####" και επιλ#ξτε "/ - ## ##### #####μ# #####".  
Αλλ#ξτε οποιαδ#ποτε #λλη επιλογ# καταλλ#λως και μετ# επιλ#ξτε "##### ##  
###μ##### ## #####μ#####".
6. Τ#λος, επιλ#ξτε "##### ##μ##### ## ##### ##### ## ##".

Αν επιλ#ξτε να τοποθετ#σετε την κατ#τμηση του βασικο# συστ#ματος (root) σε μ#α συστοιχ#α RAID, το πρ#γραμμά εγκατ#στασης θα ρωτ#σει αν θ#λετε να γ#νεται εκκ#νηση σε #####μ###μ### κατ#σταση. Δε#τε το #μ#μ# 4.1.4, &#x201C;#####μ###μ### RAID&#x201D; [12] για περισσ#τερες λεπτομ#ρειες.

Η διαδικασ#α εγκατ#στασης θα συνεχιστε# τ#τε κανονικ#.

#### 4.1.4. #####μ###μ### RAID

Σε κ#ποιο σημει#ο της ζω#ς του υπολογιστ#, μπορε# να προκ#ψει κ#ποια βλ#βη στον δ#σκο. #ταν συμβα#νει αυτ#, εν# χρησιμοποιε#τε RAID λογισμικο#, το λειτουργικ# σ#στημα θα τοποθετ#σει τη συστοιχ#α σε αυτ# που ε#ναι γνωστ# ως #####μ###μ### κατ#σταση.

Αν η δι#ταξη #χει γ#νει υποβαθμισμ#νη, λ#γω της πιθαν#τητας απ#λειας δεδομ#νων, απ# προεπιλογ# το Ubuntu Server Edition θα εκκιν#σει σε *initramfs* μετ# απ# τρι#ντα δευτερ#λεπτα. Μ#λις εκκινηθε# το *initramfs*, υπ#ρχει μια ερ#τηση για πεν#ντα δευτερ#λεπτα που σας δ#νει τη δυνατ#τητα να προχωρ#σετε και να εκκιν#σετε το σ#στημα, # να επιχειρ#σετε χειροκ#νητη αν#κτηση. Η εκκ#νηση στο *initramfs* μπορε# να ε#ναι # #χι η επιθυμητ# συμπεριφορ#, ειδικ# αν το μηχ#νημα ε#ναι σε απομακρυσμ#νη τοποθεσ#α. Η εκκ#νηση σε μια υποβαθμισμ#νη δι#ταξη μπορε# να ρυθμιστε# με πολλο#ς τρ#πους:

- Το εργαλε#ο *dpkg-reconfigure* μπορε# να χρησιμοποιηθε# για να ρυθμιστε# η προεπιλεγμ#νη συμπεριφορ# και κατ# τη διαδικασ#α θα ερωτηθε#τε για επιπλ#ον ρυθμ#σεις σχετικ#ς με τη συστοιχ#α. #πως παρακολο#θηση, ειδοποι#σεις μ#σω email, κτλ. Για να επαναρρυθμ#σετε το *mdadm*, πληκτρολογ#στε το ακ#λουθο:

```
sudo dpkg-reconfigure mdadm
```

- Η διαδικασ#α ***dpkg-reconfigure mdadm*** θα αλλ#ξει το αρχε#ο ρυθμ#σεων */etc/initramfs-tools/conf.d/mdadm*. Το αρχε#ο #χει το πλεον#κτημα πω# #χει τη δυνατ#τητα να προ# ρυθμ#σει τη συμπεριφορ# του συστ#ματος και μπορε#τε επ#σης να το επεξεργαστε#τε χειροκ#νητα:

```
BOOT_DEGRADED=true
```



Το αρχε#ο ρυθμ#σεων μπορε# να παρακαμφθε# χρησιμοποι#ντας κ#ποια παρ#μετρο με τον πυρ#να.

- Η χρήση μιας παραμέτρου πυρνα θα επιτρέπει στο σύστημα να εκκινήσει σε μια υποβαθμισμένη διατάξη επσης:
  - 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.

Μέλις το σύστημα εκκινήθηκε, μπορείτε είτε να επισκευσετε τη συστοιχία - δεχτείτε το μήνυ 4.1.5, &#x201C;##### RAID&#x201D; [13] για λεπτομρείες -, ή να αντιγράψετε σημαντικά δεδομένα σε ένα άλλο μηχάνημα λόγω σημαντικής βλάβης υλικού.

#### 4.1.5. ##### RAID

Το εργαλείο `mdadm` μπορεί να χρησιμοποιηθεί για να προβλλετε την κατάσταση μιας συστοιχίας, για να προσθέσετε δίσκους σε μια συστοιχία, να αφαιρέσετε δίσκους, κτλ:

- Για να προβλλετε την κατάσταση μιας συστοιχίας, σε ένα τερματικό πληκτρολογείτε:

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

Η επιλογή `-D` λεί στο `mdadm` να εμφανίσει ##### πληροφορίες για την συσκευή /dev/md0. Αντικαταστήστε το /dev/md0 με την κατάλληλη συσκευή RAID.

- Για να προβλλετε 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 παρουσιάζει βλάβη και πρέπει να αφαιρεθεί απή μια συστοιχία, πληκτρολογείτε:

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

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

- Παρόμοιος, για να προσθέσετε έναν νέο δίσκο:

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

Κάποιες φορές ένας δίσκος μπορεί να μεταβεί σε κατάσταση ##### ακμή και αν δεν υπάρχει κάποιο φυσικό πρόβλημα με τη συσκευή. Συνθως αζζει τον κπο να αφαιρέσετε τη συσκευή απ τη διατάξη και μετ να την επανατοποθετήσετε. Αυτό θα κνει τη συσκευή να επανασυγχρονιστεί με τη διατάξη. Αν η συσκευή δεν συγχρονιστεί με τη διατάξη, είναι μια καλή νδειξη ελαττωματικό υλικό.

Το αρχείο `/proc/mdstat` περιχει επ'σης χρ#σιμες πληροφορ#ες για τις συσκευ#ς RAID του συστ#ματος:

```
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 ακ#λουθη εντολ# ε#ναι πολ# καλ# για την παρακολο#θηση της κατ#στασης μιας συσκευ#ς που συγχρον#ζεται:

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

Πι#στε *Ctrl+c* για να τερματ#σετε την εντολ# watch.

Ε#ν χρει#ζεται να αντικαταστ#σετε μ#α προβληματικ# συσκευ#, αφο# η συσκευ# #χει αντικατασταθε# και συγχρονιστε#, θα χρειαστε# να ε#ναι εγκατεστημ#νο το grub. Για να εγκαταστ#σετε το grub στη ν#α συσκευ#, πληκτρολογ#στε το ακ#λουθο:

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

Αντικαταστ#στε το `/dev/md0` με το κατ#λληλο #νομα της συσκευ#ς συστοιχ#ας.

#### 4.1.6. #####

Το θ#μα των συστοιχι#ν RAID ε#ναι πολ#πλοκο λ#γω της πληθ#ρας των τρ#πων που μπορε# να ρυθμιστε# το RAID. Παρακαλο#με δε#τε τους ακ#λουθους συνδ#σµους για περισσ#τερες πληροφορ#ες:

- *Ubuntu Wiki Articles on RAID*<sup>6</sup>.
- *Software RAID HOWTO*<sup>7</sup>
- ##### RAID ## Linux<sup>8</sup>

#### 4.2. ##### ##µ## (LVM)

Ο διαχειριστ#ς λογικ#ν τ#µων, # LVM, επιτρ#πει στους διαχειριστ#ς να δημιουργ#σουν ##### τ#µους απ# #ναν # πολλο#ς φυσικο#ς σκληρο#ς δ#σκους. Οι τ#µοι LVM μπορο#ν να δημιουργηθ#ν και σε κατατµ#σεις RAID λογισµικο# και σε τυπικ#ς κατατµ#σεις που βρ#σκονται σε #ναν δ#σκο. Οι τ#µοι μπορο#ν επ#σης να επεκταθ#ν, δ#νοντας μεγαλ#τερη ευελιξ#α στα συστ#µατα καθ#ς οι απαιτ#σεις αλλ#ζουν.

<sup>6</sup> <https://help.ubuntu.com/community/Installation#raid>

<sup>7</sup> <http://www.faqs.org/docs/Linux-HOWTO/Software-RAID-HOWTO.html>

<sup>8</sup> <http://oreilly.com/catalog/9781565927308/>



πληκτρολογείτε ένα νόμα, επιλέξτε την κατ#τμηση που ρυθμ#στηκε για LVM και επιλέξτε "#####".

8. Π#σω στην οθ#νη "##### μ##### LVM", επιλέξτε "μ##### μ##### μ###". Επιλέξτε την ν#α ομ#δα τ#μου που δημιουργ#σατε, και πληκτρολογ#στε ένα νόμα για το ν#ο LV, για παρ#δειγμα *srv* μιας και αυτ# ε#ναι το προοριζ#μενο σημει#ο προσ#ρτησης. Μετ# επιλέξτε ν#α μ#γεθος, που μπορε# να ε#ναι ολ#κληρη η κατ#τμηση καθ#ς μπορε# π#ντα να επεκταθε# αργ#τερα. Επιλέξτε "#####" και θα πρ#πει να μεταφερθε#τε π#σω στην κ#ρια οθ#νη "μ##### μ#####".
9. Τ#ρα προσθ#στε ν#α σ#στημα αρχε#ων στο ν#ο LVM. Επιλέξτε την κατ#τμηση κ#τω απ# το "LVM VG vg01, LV srv", # #ποιο νόμα #χετε διαλ#ξει, μετ# επιλέξτε το ##### #. Ρυθμ#στε ν#α σ#στημα αρχε#ων ως συν#θως επιλ#γοντας */srv* ως το σημει#ο προσ#ρτησης. Μ#λις τελει#σετε, επιλέξτε "##### μ##### μ##### μ#####".
10. Τ#λος, επιλέξτε "##### μ##### μ##### μ##### μ##### μ#####". Μετ# επιβεβαι#στε τις αλλαγ#ς και συνεχ#στε με την υπ#λοιπη εγκατ#σταση.

Υπ#ρχουν κ#ποια χρ#σιμα εργαλε#α για να προβ#λλετε πληροφοριες για το LVM:

- *pvdisk*: shows information about Physical Volumes.
- *vgdisplay*: εμφαν#ζει πληροφοριες για τις ομ#δες τ#μων.
- *lvdisplay*: shows information about Logical Volumes.

#### 4.2.3. ##### μ##### μ###

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. Πρ#τα, δημιουργ#στε τον φυσικ# τ#μο, σε ν#α τερματικ# εκτελ#στε:

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

2. Τ#ρα επεκτε#νετε την ομ#δα τ#μων (VG):

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

3. Χρησιμοποι#στε το *vgdisplay* για να βρε#τε τις ελε#θερες φυσικ#ς εκτ#σεις - Ελε#θερο PE / μ#γεθος (το μ#γεθος που μπορε#τε να προσδ#σετε). Θα υποθ#σουμε πως υπ#ρχει ελε#θερο μ#γεθος 511 PE (ισο#ται με 2GB με μ#γεθος PE 4MB) και θα χρησιμοποι#σουμε ολ#κληρο τον διαθ#σιμο ελε#θερο χ#ρο. Χρησιμοποι#στε το δικ# σας μ#γεθος PE και /# ελε#θερο χ#ρο.

Ο λογικός τ#μος (LV) μπορε# τ#ρα να επεκταθε# με διαφορετικ#ς μεθ#δους, εμε#ς θα δο#με μ#νο π#ς να χρησιμοποιη#σετε το PE για να επεκτε#νετε το LV:

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

Η επιλογ# <sup>-l</sup> επιτρ#πει στο LV να επεκταθε# με τη χρ#ση του PE. Η επιλογ# <sup>-L</sup> επιτρ#πει στο LV να επεκταθε# χρησιμοποι#ντας 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 ακ#λουθες εντολ#ς ε#ναι για συστ#ματα αρχε#ων *EXT3* # *EXT4*. Αν χρησιμοποιη#τε #λλο σ#στημα αρχε#ων, μπορε# να υπ#ρχουν #λλα εργαλε#α διαθ#σιμα.

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

Η επιλογ# <sup>-f</sup> του e2fsck κ#νει εξαναγκαστικ# #λεγχο, ακ#μη και αν το σ#στημα φ##νεται καθαρ#.

5. Τ#λος, αλλ#ξτε το μ#γεθος του συστ#ματος αρχε#ων:

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

6. Τ#ρα προσαρτ#στε την κατ#τμηση και ελ#γξτε το μ#γεθος της.

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

#### 4.2.4. #####

- See the *Ubuntu Wiki LVM Articles*<sup>9</sup>.
- Δε#τε το *HOWTO ### LVM*<sup>10</sup> για περισσ#τερες πληροφοριες.
- #να #λλο καλ# #ρθρο ε#ναι το *Managing Disk Space with LVM*<sup>11</sup> στον ιστ#τοπο του O'Reilly linuxdevcenter.com.
- For more information on fdisk see the *fdisk man page*<sup>12</sup>.

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

<sup>10</sup> <http://tldp.org/HOWTO/LVM-HOWTO/index.html>

<sup>11</sup> <http://www.linuxdevcenter.com/pub/a/linux/2006/04/27/managing-disk-space-with-lvm.html>

<sup>12</sup> <http://manpages.ubuntu.com/manpages/raring/en/man8/fdisk.8.html>

## **5. Kernel Crash Dump**

### **5.1. #####**

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. #####**

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

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

A reboot is then needed.

### **5.4. #####**

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

### **5.5. #####**

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. #####

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*<sup>13</sup>.
- *The crash tool*<sup>14</sup>
- *Analyzing Linux Kernel Crash*<sup>15</sup> (Based on Fedora, it still gives a good walkthrough of kernel dump analysis)

---

<sup>13</sup> <http://www.kernel.org/doc/Documentation/kdump/kdump.txt>

<sup>14</sup> <http://people.redhat.com/~anderson/>

<sup>15</sup> <http://www.dedoimedo.com/computers/crash-analyze.html>

---

## Κεφάλαιο 3. Διαχείριση Πακτών

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 πολλή διαθεσίμα εργαλέα για που αλληλεπιδρο#ν με το σ#στημα διαχε#ρισης πακ#των, απ# απλ#ς λειτουργ#ες γραμμ#ς#εντολ#ν που μπορο#ν να αυτοματοποιηθο#ν ε#κολα απ# τους διαχειριστ#ς συστ#ματος, σε απλ#ς γραφικ#ς διεπαφ#ς με ε#κολη χρ#ση για τους ν#ους στο Ubuntu.

## 1. #####

Το σύστημα διαχείρισης πακέτων Ubuntu προέρχεται απ' το ίδιο σύστημα που χρησιμοποιείται απ' την έκδοση Debian GNU/Linux. Τα αρχεία πακέτων περιέχουν όλα τα κατάλληλα αρχεία, μεταδεδομένα, 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
```

- Αν#λογα με τον #γκο των πακ#των στο σ#στημ# σας, αυτ# μπορε# να παρ#γει #να μεγ#λο #γκο εξ#δου. Διοχετε#στε την #ξοδο μ#σω `grep` για να δε#τε ε#ν #να συγκεκριμ#νο πακ#το #χει εγκατασταθε#:

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

Αντικαταστ#στε το *apache2* με οποιοδ#ποτε #νομα πακ#του, # #λλες κανονικ#ς επεκτ#σεις.

- Για να καταγρ#ψετε τα αρχε#α που #χουν εγκατασταθε# απ# #να πακ#το, σε αυτ# την περ#πτωση το πακ#το `ufw`, πληκτρολογ#στε:

```
dpkg -L ufw
```

- Ε#ν δεν ε#στε σ#γουροι ποιο πακ#το εγκατ#στησε #να αρχε#ο, η `dpkg -S` μπορε# να ε#ναι ικαν# να σας πει. Για παρ#δειγμα:

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

Η #ξοδος δε#χνει #τι το `/etc/host.conf` αν#κει στο πακ#το `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.

- Μπορε#τε να εγκαταστ#σετε #να τοπικ# αρχε#ο *.deb* πληκτρολογ#ντας:

```
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 απεγκατ#σταση εν#ς πακ#του μπορε# να επιτευχθε#:

```
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
```



Πολλά πακέτα: Μπορείτε να προσδιορίσετε πολλά 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 πρόοδο χρόνου, αναβαθμισμένες εκδόσεις πακέτων που είναι εγκαταστημένα στον υπολογιστή σας μπορεί να γίνουν διαθέσιμες από το πακέτο αποθετηρών (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 πώς να αναβαθμίσετε μια καινούρια έκδοση Ubuntu δείτε [#μ#μ# 3, &#x201C;#####μ###&#x201D; \[9\]](#).

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*<sup>1</sup> or type:

`apt-get help`

---

<sup>1</sup> <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 σχετική απλή, και η διεπαφή του χρηστή κίνει απλές διεργασίες έκολες να εκτελεστον. Τα ακόλουθα είναι παραδείγματα κοινών λειτουργιών διαχείρισης πακέτων όπως εκτελούνται 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 προβλέπεται στη λίστα πακέτων στο πρώτο παράθυρο, όταν προβλέπετε 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**: Ασυσκεπαστα αρχεία, αλλά χωρίς να έχει διαμορφωθεί το πακέτο ακόμα
- **C**: Μισοδιαμορφωμένα - Η διαμόρφωση απτυχε και απαιτείται διρθωση
- **H**: Μισοεγκαταστημένα - Η αφαίρεση απτυχε και απαιτείται διρθωση

Για να εξέλθετε από το *Aptitude*, απλώς 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. #####

Το πακέτο `unattended-upgrades` μπορεί να χρησιμοποιηθεί για να εγκαθίσταται αυτόματα οι ενημερώσεις πακέτων, και μπορεί να διαμορφωθεί να ενημερώνει όλα τα πακέτα απλώς να εγκαθιστούν 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";
};
```

Ορίστε ένα πακέτο που μπορεί να ~~μην ενημερωθεί~~ και έτσι να μην ενημερωθεί αυτόματα. Για να βλέπετε ένα πακέτο στη μαύρη λίστα, προσθέστε το στη λίστα:

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



Η γραμμή με διπλή `&#x201C; // &#x201D;` λειτουργεί ως σχόλιο, έτσι τι ακολουθεί μετά απ' `"/` 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. #####

Η διαμόρφωση του *Unattended-Upgrade::Mail* στο `/etc/apt/apt.conf.d/50unattended-upgrades` θα ενεργοποιήσει το `unattended-upgrades` να στέλνει email σε #να διαχειριστ# δ#νοντας λεπτομ#ρειες για κ#θε πακ#το που χρει#ζεται αναβ#θμιση # χει προβλ#ματα.

#να #λλο χρ#σιμο πακ#το ε#ναι το `apticron`. Το `apticron` θα διαμορφ#σει μια δουλει# `cron` να στέλνει email σε #να διαχειριστ# πληροφορ#ες για πακ#τα στο σ#στημα που #χουν διαθ#σιμες ενημερ#σεις, καθ#ς και μια περ#ληψη αλλαγ#ν σε κ#θε πακ#το.

Για να εγκαταστ#σετε το πακ#το `apticron`, σε #να τερματικ# πληκτρολογ#στε:

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

#ταν το πακ#το εγκατασταθε# επεξεργαστε#τε το `/etc/apticron/apticron.conf`, για να δε#τε τη διε#θυνση ηλεκτρονικο# ταχυδρομε#ου και #λλες επιλογ#ς:

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

## 6. #####

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 #ποτε προκύπτουν λειτουργίες πακέτου, απλώς αποσχολήστε 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. #####

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 δειάς που τα αποτρέπει απ' το να διανέμονται με ένα ελεuthero λειτουργικό στήμα, και μπορεί να είναι παράνομα στην τοποθέσας σας.



Πληροφορηθείτε τι ότε το *Universe* ότε *Multiverse* αποθετήριο περιχουν επισμως υποστηριζμενα πακέτα. Συγκεκριμένα, μπορεί να μην υπρχουν ενημερσεις ασφαλεας για τα συγκεκριμένα πακέτα.

Πολλές άλλες πηγές πακέτων είναι διαθέσιμες, μερικές ακόμα προσφέρουν μνο να πακτο, #πως στην περπτωση των πηγν πακέτων που παρχονται απ τον προγραμματιστ μιας εφαρμογς. Θα πρπει πντα να εστε πολ# προσεκτικο# και επιφυλακτικο# ταν χρησιμοποιετε μ#-κοινς πηγς πακέτων, #μως. Ερευνστε την πηγ# και τα πακέτα προσεκτικ# πριν εκτελ#σετε κ#ποια εγκατ#σταση, καθς μερικς πηγς πακέτων και τα πακέτα τους μπορεί να καταστ#σουν το σ#στημ# σας ασταθς # μ#-λειτουργικ# σε ορισμνες απψεις.

Εξορισμο#, τα αποθετήρια *Universe* και *Multiverse* είναι ενεργοποιημένα αλλ# ε#ν θα θέλατε να τα απενεργοποιήσετε επεξεργαστείτε το `/etc/apt/sources.list` και σχολήστε τις ακλουθες 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. #####

Το περισσότερο απ# το υλικ# που καλ#πτεται σε αυτ# το κεφ#λαιο ε#ναι διαθ#σιμο στις σελ#δες `man`, πολλ#ς απ# τις οπο#ες ε#ναι διαθ#σιμες online.

- The *InstallingSoftware*<sup>2</sup> Ubuntu wiki page has more information.
- For more `dpkg` details see the *dpkg man page*<sup>3</sup>.
- The *APT HOWTO*<sup>4</sup> and *apt-get man page*<sup>5</sup> contain useful information regarding `apt-get` usage.
- See the *aptitude man page*<sup>6</sup> for more `aptitude` options.
- Η σελ#δα *Adding Repositories HOWTO (Ubuntu Wiki)*<sup>7</sup> περι#χει περισσ#τερες λεπτομ#ρειες για την προσθ#κη αποθετηρ#ων.

---

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

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

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

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

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

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

---

## Κεφάλαιο 4. Δικτύωση

Τα δίκτυα απαρτίζονται από πολλές περισσότερες συσκευές, όπως υπολογιστικά συστήματα, εκτυπωτές και σχετικές εξοπλισμένες τα οποία είναι συνδεδεμένα είτε με φυσικά καλώδια 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 των δικτύων και λεπτομερή συζήτηση δημοφιλών πρωτοκόλλων δικτύου.



## 1. #####

Το Ubuntu στ#λνεται με #ναν αριθμ# γραφικ#ν λειτουργ#ν για να διαμορφ#σετε τις συσκευ#ς δικτ#ου σας. Αυτ# το #γγραφο ε#ναι προσανατολισμ#νο σε διαχειριστ#ς διακομιστ# και θα εστι#σει στη διαχε#ριση του δικτ#ου σας στη γραμμ# εντολ#ν.

### 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. #####

Η γλωσσική πολλαπλήν διεπαφήν είναι μια πιο προηγμένη διαμρφωση, αλλά είναι πολύχρησιμη για πολλήν σενάρια. ένα σενάριο είναι το στίσιμο μιας γφύρας με πολλαπλές

διεπαφής δικτύου, μετά η χρησιμοποίηση ενός τέτοιου προστάσας για να φιλτράρετε την κίνηση μεταξύ δομημάτων δικτύου. #να #λλο σενάριο είναι η χρησιμοποίηση γέφυρας σε #να σ#στημα με #να διεπαφή για να επιτ#ψετε σε εικονικές μηχανές #μεση πρ#σβαση στο εξωτερικό δ#κτυο. Το ακ#λουθο παρ#δειγμα καλ#πτει το δε#τερο σενάριο.

Πριν διαμορφ#σετε μια γέφυρα θα πρ#πει να εγκαταστ#σετε το πακ#το `bridge-utils`. Για να εγκαταστ#σετε το πακ#το, σε #να τερματικό πληκτρολογ#στε:

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

Μετ#, διαμορφ#στε τη γέφυρα κ#νοντας επεξεργασ#α 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
```



Εισ#γετε τις κατ#λληλες τιμές για τη φυσική σας διεπαφή και δ#κτυο.

Τ#ρα επανεκκιν#στε τη δικτύωση για να ενεργοποι#σετε τη γέφυρα διεπαφής:

```
sudo service networking restart
```

Η καινο#ρια διεπαφή γέφυρας θα πρ#πει τ#ρα να εκτελε#τε. Το `brctl` παρ#χει χρ#σιμες πληροφορίες για την κατ#σταση της γέφυρας, ελ#γχει ποιες διεπαφές είναι μ#ρος της γέφυρας, κλπ. Δε#τε το **man brctl** για περισσ#τερες πληροφορίες.

## 1.5. #####

- The *Ubuntu Wiki Network page*<sup>1</sup> has links to articles covering more advanced network configuration.
- The *resolvconf man page*<sup>2</sup> has more information on resolvconf.

---

<sup>1</sup> <https://help.ubuntu.com/community/Network>

<sup>2</sup> <http://manpages.ubuntu.com/manpages/man8/resolvconf.8.html>



- The *interfaces man page*<sup>3</sup> has details on more options for `/etc/network/interfaces`.
- The *dhclient man page*<sup>4</sup> has details on more options for configuring DHCP client settings.
- For more information on DNS client configuration see the *resolver man page*<sup>5</sup>. Also, Chapter 6 of O'Reilly's *Linux Network Administrator's Guide*<sup>6</sup> is a good source of resolver and name service configuration information.
- For more information on *bridging* see the *brctl man page*<sup>7</sup> and the Linux Foundation's *Net:Bridge*<sup>8</sup> page.

---

<sup>3</sup> <http://manpages.ubuntu.com/manpages/man5/interfaces.5.html>

<sup>4</sup> <http://manpages.ubuntu.com/manpages/man8/dhclient.8.html>

<sup>5</sup> <http://manpages.ubuntu.com/manpages/man5/resolver.5.html>

<sup>6</sup> <http://oreilly.com/catalog/linag2/book/ch06.html>

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

<sup>8</sup> <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 Μηνάς Προηγμένης Έρευνας (DARPA) σαν μέσο επικοινωνίας μεταξύ 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. ##### TCP/IP

Τα δύο συστατικά πρωτόκολλα του TCP/IP αντιμετωπίζουν διαφορετικές πτυχές της δικτύωσης υπολογιστών. Το #####, το "IP" του TCP/IP είναι ένα πρωτόκολλο χωρής 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 ##### 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 στέλθηκαν από έναν άλλο κεντρικό υπολογιστή δικτύου.

### 2.2. ##### TCP/IP

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

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

- **IP διεθυσση** Η διεθυσση IP είναι μια μοναδική συμβολοσειρά εκφρασμένη σαν τήσερις δεκαδικό αριθμό με εμβέλεια από μηδέν <sup>(0)</sup> μέχρι διακόσια πενήντα πέντε (255), χωρισμένοι με τελείες, με κάθε ένα από τους τήσερις αριθμούς να εκπροσωπούν οχτώ (8) bits της διεθυσσης για ένα συνολικό μέγεθος τριάντα δύο (32) bits για όλη τη διεθυσση. Αυτή η μορφή ονομάζεται #####.
- **Μέσκα Δικτύου** Η Μέσκα Υποδικτύου (ή απλά #####) είναι μια τοπική μέσκα bit, # σύνολο σημαίων που χωρίζει τα μέχρι μια IP διεθυσσης σημαντικές για το δίκτυο από τα bits που είναι σημαντικές για το #####. Για παράδειγμα, σε ένα υποδίκτυο Κλάσης Γ, η κανονική μέσκα δικτύου είναι 255.255.255.0 η οποία καλύπτει τα πρώτα τρία bytes μιας διεθυσσης IP και επιτρέπει στο τελευταίο byte της διεθυσσης 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 χρησιμοποιήσει την 12.0.0.0 ως διεύθυνση δικτύου, όπου το δεκά (12) αντιπροσωπεύει το πρώτο byte της διεύθυνσης IP, (το μέρος δικτύου) και τα μηδενικά (0) σε όλα 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 χρησιμοποιήσει 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 χροστής. Η πρωτότυπη 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 ντεντ γιατ 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 Επύλωσης Διεύθυνσης (ARP) και το Πρωτόκολλο Πληροφοριών Δρομολόγησης (RIP)
- Διεύθυνση Πύλης Μια Διεύθυνση Πύλης είναι η διεύθυνση IP μέσω της οποίας ένα συγκεκριμένο δίκτυο, ή κεντρικός υπολογιστής σε δίκτυο, μπορεί να βρεθεί. 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 #####. Σε πολλές περιπτώσεις, η Διεύθυνση Πύλης θα είναι αυτός εντός δρομολογητή στο ίδιο δίκτυο, ο οποίος εν συνεχεία θα μεταφέρει κλήση σε άλλα δίκτυα ή κεντρικούς υπολογιστές, όπως κεντρικός υπολογιστής ντεντ. Η τιμή της ρύθμισης Διεύθυνσης Πύλης πρέπει να είναι σωστή, αλλιώς το σύστημά σας δε θα μπορεί να βρει κανέναν κεντρικό υπολογιστή πέρα από αυτός του ίδιου δικτύου.
- Διεύθυνση Ονόματος Διακομιστή Οι Διευθύνσεις Ονόματος Διακομιστή εκπροσωπούν το σύστημα Υπηρεσίας Ονόματος Τομέα (DNS), το οποίο επιλέγει ονόματα κεντρικών υπολογιστών δικτύου σε διευθύνσεις IP. Υπάρχουν τρία επίπεδα Διευθύνσεων Ονόματος Διακομιστή, που μπορούν να προσδιοριστούν με σειρά προτεραιότητας: Το ##### #νομα Διακομιστή, το ##### #νομα Διακομιστή, και το ##### #νομα Διακομιστή. Για να μπορεί το σύστημά σας να επιλέγει ονόματα κεντρικών υπολογιστών δικτύου στις αντίστοιχες διευθύνσεις IP, πρέπει να προσδιορίσετε γκνρες Διευθύνσεις Ονομάτων Διακομιστή τις οποίες έχετε 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 πολλές διαθέσιμες δωρεάν και προσβέσιμες δημοσώς 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 Μσκά Δικτύου, η Διεθυσση Δικτύου, η Διεθυσση Εκπομπς, και η Διεθυσση Πυλνα ε#ναι τυπικ# προσδιορισμ#νες μ#σω των κατ#λληλων κωδικ#ν παραπομπς στο αρχε#ο `/etc/network/interfaces`. Οι Διευθύνσεις Ον#ματος Διακομιστ# ε#ναι προσδιορισμ#νες μ#σω κωδικ#ν παραπομπς `nameserver` στο αρχε#ο `/etc/resolv.conf`. Για περισ#τερες πληροφορ#ες, δε#τε τη σελ#δα εγχειριδ#ου συστ#ματος για `#####` `resolv.conf` αντ#στοιχα, με τις ακ#λουθες εντολ#ς σε #να τερματικ# εντολ#ν:

Δε#τε τη σελ#δα εγχειριδ#ου για `#####` με την ακ#λουθη εντολ#:

```
man interfaces
```

Δε#τε τη σελ#δα εγχειριδ#ου `resolv.conf` με την ακ#λουθη εντολ#:

```
man resolv.conf
```

### 2.3. ##### IP

Η δρομολ#γηση IP ε#ναι #να μ#σω προσδιορισμ# και ανακ#λυσης μονοπατι#ν στο δ#κτυο TCP/IP μαζ# με το ποια δεδομ#να μπορε# να αποσταλο#ν. Η δρομολ#γηση χρησιμοποιε# #να σ#νολο `#####` για να κατευθ#νει την προ#θηση πακ#των δεδομ#νων δικτ#ου απ# την πηγ# στον προορισμ#, συχν# μ#σω ενδι#μεσων κ#μβων δικτ#ου γνωστ#ν ως `#####`. Υπ#ρχουν δ#ο κ#ριες μορφ#ς δρομολ#γησης IP: `#####` και `#####`.

Η Στατικ# Δρομολ#γηση περιλαμβ#νει χειροκ#νητη πρ#σθεση δρομολογητ#ν IP στον π#νακα δρομολ#γησης, και αυτ# γ#νεται συν#θως χειραγωγ#ντας τον π#νακα δρομολ#γησης με τον εντολ# `route`. Η στατικ# δρομολ#γηση #χει πολλ# πλεονεκτ#ματα σε σχ#ση με τη δυναμικ# δρομολ#γηση, #πως η απλ#τητα υλοπο#ησης για μικρ#τερα δ#κτυα, η προβλεψιμ#τητα (ο π#νακας δρομολ#γησης π#ντα υπολογ#ζεται εκ των προτ#ρων, και #τσι η διαδρομ# ε#ναι ακριβ#ς η #δια κ#θε φορ# που χρησιμοποιε#ται), και η χαμηλ# επιβ#ρυνση στους #λλους δρομολογητ#ς και συνδ#σεις του δικτ#ου λ#γω της #λλειψης μιας δυναμικ#ς δρομολ#γησης του πρωτοκ#λλου. Ωστ#σο, η στατικ# δρομολ#γηση εν#χει κ#ποια μειονεκτ#ματα, επ#σης. Για παρ#δειγμα, η στατικ# δρομολ#γηση περιορ#ζεται σε μικρ# δ#κτυα και δεν κλιμακ#νεται καλ#. Η στατικ# δρομολ#γηση επ#σης αποτυγχ#νει εντελ#ς να προσαρμοστε# στις διακοπ#ς του δικτ#ου και τις αποτυχ#ες κατ# μ#κος της διαδρομ#ς, λ#γω της σταθερ#ς φ#σης της διαδρομ#ς.

Η Δυναμικ# Δρομολ#γηση βασ#ζεται σε μεγ#λα δ#κτυα με πολλ#ς πιθαν#ς διαδρομ#ς IP απ# μια πηγ# σε #ναν προορισμ# και κ#νει χρ#ση μερικ#ν ειδικ#ν πρωτοκ#λλων, #πως το Πρωτ#κολλο Πληροφορ#ας Δρομολ#γησης (RIP), το οπο#ο διαχειρ#ζεται αναπροσαρμογ#ς στους π#νακες δρομολ#γησης που κ#νει τη δυναμικ# δρομολ#γηση εφικτ#. Η δυναμικ# δρομολ#γηση #χει αρκετ# πλεονεκτ#ματα σε σχ#ση με τη στατικ# δρομολ#γηση, #πως

εξαιρετικ# επεκτασιμ#τητα και την ικαν#τητα προσαρμογ#ς στις αποτυχ#ες και διακοπ#ς κατ# μ#κος των διαδρομ#ν του δικτ#ου. Επιπλ#ον, υπ#ρχει λιγ#τερη χειρωνακτικ# διαμ#ρφωση των πιν#κων δρομολ#γησης, επειδ# οι δρομολογητ#ς μαθα#νουν ο #νας απ# τον #λλο για την #παρξ# τους και τις διαθ#σιμες διαδρομ#ς. Αυτ# το χαρακτηριστικ# καταργε# επ#σης τη δυνατ#τητα θ#σπισης λ#θους στους π#νακες δρομολ#γησης μ#σω ανθρ#πινου λ#θους. Η δυναμικ# δρομολ#γηση δεν ε#ναι τ#λεια, #μως, και παρουσι#ζει μειονεκτ#ματα, #πως η αυξημ#νη πολυπλοκ#τητα και η πρ#σθετη επιβ#ρυνση του δικτ#ου απ# επικοινων#ες δρομολογητ#ν, η οπο#α δεν ωφελε# #μεσα τους τελικο#ς χρ#στες, αλλ# εξακολουθε# να καταναλ#νει ε#ρος ζ#νης δικτ#ου.

## 2.4. TCP ### UDP

Το TCP ε#ναι #να πρωτ#κόλλο βασισμ#νο στη σ#νδεση, το οπο#ο προσφ#ρει δι#ρθωση σφαλμ#των και εγγυημ#νη παρ#δοση δεδομ#νων μ#σω αυτο# που ε#ναι γνωστ# ως #####. Ο #λεγχος ρο#ς καθορ#ζει π#τε η ρο# εν#ς ρε#ματος δεδομ#νων πρ#πει να σταματ#σει, και π#τε πακ#τα δεδομ#νων που #χουν σταλε# πριν πρ#πει να ξανασταλο#ν λ#γω προβλημ#των #πως οι #####, για παρ#δειγμα, διασφαλ#ζοντας #τσι πλ#ρη και ακριβ# παρ#δοση δεδομ#νων. Το TCP χρησιμοποιε#ται τυπικ# στην ανταλλαγ# σημαντικ#ν πληροφορι#ν #πως συναλλαγ#ς β#σης δεδομ#νων.

Το Πρωτ#κόλλο Διαγραμμ#των Δεδομ#νων Χρ#στη (UDP), απ# την #λλη, ε#ναι #να πρωτ#κόλλο ##### το οπο#ο σπ#νια ασχολε#ται με τη μεταφορ# σημαντικ#ν δεδομ#νων επειδ# δεν #χει #λεχο ρο#ς # οποιαδ#ποτε #λλη μ#θοδο για να διασφαλ#σει την αξι#πιστη μεταφορ# δεδομ#νων. Το UDP χρησιμοποιε#ται συν#θως σε αναπαραγωγ# #χου και β#ντεο, #που θεωρε#τε πιο γρ#γορο απ# το TCP λ#γω της #λλειψης δι#ρθωσης σφαλμ#των και ελ#γχου ρο#ς, και #που η απ#λεια κ#ποιων πακ#των δεν ε#ναι γενικ# καταστροφικ#.

## 2.5. ICMP

Το Πρωτ#κόλλο Ελ#γχου Μηνυμ#των #ντερνετ (ICMP) ε#ναι μια προ#κταση του Πρωτοκ#λλου Διαδικτ#ου (IP) #πως ορ#ζετε στην Α#τηση για Σχ#λια (RFC) #792 και υποστηρ#ζει πακ#τα δικτ#ου που περι#χουν μηνμ#ματα ελ#γχου, σφαλμ#των, και πληροφοριακ# μηνμ#ματα. Το ICMP χρησιμοποιε#ται απ# εφαρμογ#ς δικτ#ου #πως η λειτουργια ping, η οπο#α μπορε# να προσδιορ#σει τη διαθεσιμ#τητα εν#ς κεντρικο# υπολογιστ# # συσκευ#ς δικτ#ου. Παραδε#γματα μερικ#ν μηνυμ#των σφαλμ#των που επιστρ#φονται απ# το ICMP τα οπο#α ε#ναι χρ#σιμα και για κεντρικο#ς υπολογιστ#ς δικτ#ου και για συσκευ#ς #πως δρομολογητ#ς, περιλαμβ#νουν τα #####μ## και #####.

## 2.6. ###μ###

Οι δα#μονες ε#ναι ειδικ#ς εφαρμογ#ς συστ#ματος η οπο#ες τυπικ# εκτελο#νται συνεχ#ς στο παρασκ#νιο και περιμ#νουν αιτμ#ματα για τις λειτουργ#ες που παρ#χουν απ# #λλες

εφαρμογές. Πολλοί δαίμονες είναι δίκτυο-κεντρικοί, αυτό σημαίνει ότι ένας μεγάλος αριθμός δαίμωνων που εκτελούνται στο παρασκήνιο σε ένα σύστημα Ubuntu μπορεί να παρχει λειτουργικότητα σχετική με το δίκτυο. Μερικά παραδείγματα περιλαμβάνουν το `#####` (`httpd`), ο οποίος παρχει λειτουργικότητα διακομιστή ιστο, το `#####` (`sshd`), ο οποίος παρχει ασφαλ απομακρυσμένη πρόσδο κελύφους και δυνατήτες μεταφορές αρχείων, και το `#####` (`imapd`), ο οποίος παρχει υπηρεσίες Ηλεκτρονικές Αλληλογραφίας.

## 2.7. #####

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

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

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

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

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

### 3. ##### μ##### μ##### ##### **(Dynamic Host Configuration Protocol (DHCP))**

Το Πρωτόκολλο Δυναμικής Διαμόρφωσης Κεντρικού Υπολογιστή είναι μια υπηρεσία δικτύου που επιτρέπει στους κεντρικούς υπολογιστές να τους εκχωρηθούν ρυθμίσεις απάναν διακομιστή αυτόματα σε αντήθεση 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

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

- Όνομα Κεντρικού Υπολογιστή
- Όνομα Τομέα
- Διακομιστής Χρήνου
- Διακομιστής Εκτύπωσης

Το πλεονέκτημα της χρήσης DHCP είναι ότι οι αλλαγές στο δίκτυο, για παράδειγμα μια αλλαγή στη διεθύνση 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 καταγράφουν τον διακομιστή DHCP. Σαν επιπλέον πλεονέκτημα, είναι επίσης εύκολο να ενσωματώσετε καινούργιους υπολογιστές στο δίκτυο, καθώς δεν υπάρχει ανάγκη να ελεγγετε την διαθεσιμότητα μιας διεθύνσης IP. Οι συγκροσεις 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 its 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. #####

Σε #να τερματικ# εντολ#ν, πληκτρολογ#στε την ακ#λουθη εντολ# για να εγκαταστ#σετε 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 μην#ματα του `dhcpcd` αποστ#λνονται στο `syslog`. Κοιτ#ξτε εκε# για διαγνωστικ# μην#ματα.

### 3.2. ###μ#####

Το μ#νυμα σφ#λματος με το οπο#ο τελει#νει η εγκατ#σταση μπορε# να σας μπερδε#ει λ#γο, αλλ# τα ακ#λουθα β#ματα θα σας βοηθ#σουν να διαμορφ#σετε την υπηρεσ#α:

Κοιν#, αυτ# που θ#λετε να κ#νετε ε#ναι να ορ#σετε τυχα#α μια διε#θυνση IP. Αυτ# μπορε# να γ#νει με ρυθμ#σεις ως εξ#ς:

```
# 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. #####

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

---

<sup>13</sup> <https://help.ubuntu.com/community/dhcp3-server>

<sup>14</sup> <http://manpages.ubuntu.com/manpages/raring/en/man5/dhcpd.conf.5.html>

<sup>15</sup> <http://www.isc.org/software/dhcp>

## 4. #####μ## #### μ# NTP

Το NTP είναι ένα πρωτοκόλλο TCP/IP για να συγχρονίζεται την ώρα σε ένα δίκτυο. Βασικός ο πελάτης κνεί ατήση για την τρχοντα ώρα απ# έναν διακομιστ#, και τον χρησιμοποιεί για να ρυθμσει το δικ# του ρολ#ι.

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. #####

To install ntpd, from a terminal prompt enter:

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

### 4.4. ###μ#####

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. #####

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

---

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

<sup>17</sup> <http://www.ntp.org/>

---

## Κεφ#λαιο 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* [55] for a complete listing

## Π#vακας 5.1. Priority Checker Conversion

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

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. #####

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.

## Π#vακκς 5.2. DM-Multipath Components

Component	Description
<b>dm_multipath kernel module</b>	Reroutes I/O and supports <b>failover</b> for paths and path groups.
<b>multipath command</b>	Lists and configures <b>multipath</b> 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.
<b>multipathd daemon</b>	Monitors paths; as paths fail and come back, it may initiate path group switches. Provides for interactive changes to <b>multipath</b> devices. This daemon must be restarted for any changes to the <code>/etc/multipath.conf</code> file to take effect.
<b>kpartx command</b>	Creates device mapper devices for the partitions on a device It is necessary to use this command for DOS-based partitions with DM-Multipath. The <code>kpartx</code> is provided in its own package, but the <b>multipath-tools</b> 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*<sup>1</sup> use

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

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

---

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

### 3.3. Ignoring Local Disks When Generating Multipath Devices

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

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

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

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

create: 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* [74].

## **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 [65]*
- *Configuration File Blacklist [66]*
- *Configuration File Defaults [68]*
- *Configuration File Multipath Attributes [72]*
- *Configuration File Devices [74]*

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* [66]
- By device name, as described in *Blacklisting By Device Name* [66]
- By device type, as described in *Blacklisting By Device Type* [67]

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* [66]

### 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 [67]*

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

#### 4.2.3. Blacklisting By Device Type

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

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

#### 4.2.4. Blacklist Exceptions

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

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

```
blacklist {
    wwid "*"
}
```

```
blacklist_exceptions {  
    wwid "3600d0230000000000e13955cc3757803"  
}
```

When specifying devices in the **blacklist\_exceptions** section of the configuration file, you must specify the exceptions in the same way they were specified in the **blacklist**. For example, a WWID exception will not apply to devices specified by a **devnode** blacklist entry, even if the blacklisted device is associated with that WWID. Similarly, devnode exceptions apply only to devnode entries, and device exceptions apply only to device entries.

### 4.3. Configuration File Defaults

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

```
defaults {  
    user_friendly_names yes  
}
```

This overwrites the default value of the **user\_friendly\_names** parameter.

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

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

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

```
defaults {  
    user_friendly_names    yes
```

```

    path_grouping_policy    multibus
}

```

Table *Multipath Configuration Defaults* [69] 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.

### Π#vακας 5.3. Multipath Configuration Defaults

Attribute	Description
<b>polling_interval</b>	Specifies the interval between two path checks in seconds. For properly functioning paths, the interval between checks will gradually increase to (4 * <b>polling_interval</b> ). The default value is <b>5</b> .
<b>udev_dir</b>	The directory where udev device nodes are created. The default value is <code>/dev</code> .
<b>multipath_dir</b>	The directory where the dynamic shared objects are stored. The default value is system dependent, commonly <code>/lib/multipath</code> .
<b>verbosity</b>	The default verbosity. Higher values increase the verbosity level. Valid levels are between 0 and 6. The default value is 2.
<b>path_selector</b>	<p>Specifies the default algorithm to use in determining what path to use for the next I/O operation. Possible values include:</p> <ul style="list-style-type: none"> <li>• <b>round-robin 0</b>: Loop through every path in the path group, sending the same amount of I/O to each.</li> <li>• <b>queue-length 0</b>: Send the next bunch of I/O down the path with the least number of outstanding I/O requests.</li> <li>• <b>service-time 0</b>: 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.</li> </ul> <p>The default value is <b>round-robin 0</b>.</p>
<b>path_grouping_policy</b>	<p>Specifies the default path grouping policy to apply to unspecified multipaths. Possible values include:</p> <ul style="list-style-type: none"> <li>• <b>failover</b> = 1 path per priority group</li> <li>• <b>multibus</b> = all valid paths in 1 priority group</li> <li>• <b>group_by_serial</b> = 1 priority group per detected serial number</li> <li>• <b>group_by_prio</b> = 1 priority group per path priority value</li> <li>• <b>group_by_node_name</b> = 1 priority group per target node name.</li> </ul>

Attribute	Description
	The default value is <b>failover</b> .
<b>getuid_callout</b>	<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 <b>/lib/udev/scsi_id --whitelisted --device=/dev/%n</b>.</p>
<b>prio</b>	<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"> <li>• <b>const</b>: Set a priority of 1 to all paths.</li> <li>• <b>emc</b>: Generate the path priority for EMC arrays.</li> <li>• <b>alua</b>: Generate the path priority based on the SCSI-3 ALUA settings.</li> <li>• <b>netapp</b>: Generate the path priority for NetApp arrays.</li> <li>• <b>rdac</b>: Generate the path priority for LSI/Engenio RDAC controller.</li> <li>• <b>hp_sw</b>: Generate the path priority for Compaq/HP controller in active/standby mode.</li> <li>• <b>hds</b>: Generate the path priority for Hitachi HDS Modular storage arrays.</li> </ul> <p>The default value is <b>const</b>.</p>
<b>prio_args</b>	The arguments string passed to the prio function. Most prio functions do not need arguments. The datacore prioritizer needs one. Example, " <b>timeout=1000 preferredsds=foo</b> ". The default value is (null) "".
<b>features</b>	The extra features of multipath devices. The only existing feature is <b>queue_if_no_path</b> , which is the same as setting <b>no_path_retry</b> to <b>queue</b> . For information on issues that may arise when using this feature, see Section, " <i>Issues with queue_if_no_path feature</i> ".
<b>path_checker</b>	<p>Specifies the default method used to determine the state of the paths. Possible values include:</p> <ul style="list-style-type: none"> <li>• <b>readsector0</b>: Read the first sector of the device.</li> <li>• <b>tur</b>: Issue a TEST UNIT READY to the device.</li> <li>• <b>emc_clariion</b>: Query the EMC Clariion specific EVPD page 0xC0 to determine the path.</li> <li>• <b>hp_sw</b>: Check the path state for HP storage arrays with Active/Standby firmware.</li> </ul>

Attribute	Description
	<ul style="list-style-type: none"> <li>• <b>rdac</b>: Check the path stat for LSI/Engenio RDAC storage controller.</li> <li>• <b>directio</b>: Read the first sector with direct I/O.</li> </ul> <p>The default value is <b>directio</b>.</p>
<b>failback</b>	<p>Manages path group failback.</p> <ul style="list-style-type: none"> <li>• A value of <b>immediate</b> specifies immediate failback to the highest priority path group that contains active paths.</li> <li>• A value of <b>manual</b> specifies that there should not be immediate failback but that failback can happen only with operator intervention.</li> <li>• A numeric value greater than zero specifies deferred failback, expressed in seconds.</li> </ul> <p>The default value is <b>manual</b>.</p>
<b>rr_min_io</b>	<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>
<b>rr_weight</b>	<p>If set to <b>priorities</b>, then instead of sending <b>rr_min_io</b> requests to a path before calling <b>path_selector</b> to choose the next path, the number of requests to send is determined by <b>rr_min_io</b> times the path's priority, as determined by the prio function. If set to <b>uniform</b>, all path weights are equal.</p> <p>The default value is <b>uniform</b>.</p>
<b>no_path_retry</b>	<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 <b>immediate</b> failure, without queueing. A value of <b>queue</b> indicates that queueing should not stop until the path is fixed.</p> <p>The default value is 0.</p>
<b>user_friendly_names</b>	<p>If set to yes, specifies that the system should use the <code>/etc/multipath/bindings</code> file to assign a persistent and unique <b>alias</b> to the <b>multipath</b>, in the form of mpathn. If set to no, specifies that the system should use the WWID as the <b>alias</b> for the <b>multipath</b>. 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>

Attribute	Description
	The default value is <b>no</b> .
<b>queue_without_daemon</b>	<p>If set to no, the <b>multipathd</b> daemon will disable queueing for all devices when it is shut down.</p> <p>The default value is <b>yes</b>.</p>
<b>flush_on_last_del</b>	<p>If set to yes, then <b>multipath</b> will disable queueing when the last path to a device has been deleted.</p> <p>The default value is <b>no</b>.</p>
<b>max_fds</b>	Sets the maximum number of open file descriptors that can be opened by <b>multipath</b> and the <b>multipathd</b> daemon. This is equivalent to the <code>ulimit -n</code> command. A value of <code>max</code> will set this to the system limit from <code>/proc/sys/fs/nr_open</code> . 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.
<b>checker_timer</b>	<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 <code>/sys/block/sdx/device/timeout</code>, which is 30 seconds as of 12.04 LTS</p>
<b>fast_io_fail_tmo</b>	<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 <code>dev_loss_tmo</code>. Setting this to off will disable the timeout.</p> <p>The default value is determined by the OS.</p>
<b>dev_loss_tmo</b>	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* [73] 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.

## Π#vακκς 5.4. Multipath Attributes

Attribute	Description
<b>wwid</b>	Specifies the WWID of the <b>multipath</b> device to which the <b>multipath</b> attributes apply. This parameter is mandatory for this section of the <code>multipath.conf</code> file.
<b>alias</b>	Specifies the symbolic name for the <b>multipath</b> device to which the <b>multipath</b> attributes apply. If you are using <b>user_friendly_names</b> , 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* [75] 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* [73].

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.



## Π#vακκς 5.5. Device Attributes

Attribute	Description
<b>vendor</b>	Specifies the vendor name of the storage device to which the device attributes apply, for example <b>COMPAQ</b> .
<b>product</b>	Specifies the product name of the storage device to which the device attributes apply, for example <b>HSV110 (C)COMPAQ</b> .
<b>revision</b>	Specifies the product revision identifier of the storage device.
<b>product_blacklist</b>	Specifies a regular expression used to blacklist devices by product.
<b>hardware_handler</b>	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"> <li>• <b>1 emc</b>: hardware handler for EMC storage arrays</li> <li>• <b>1 alua</b>: hardware handler for SCSI-3 ALUA arrays.</li> <li>• <b>1 hp_sw</b>: hardware handler for Compaq/HP controllers.</li> <li>• <b>1 rdac</b>: hardware handler for the LSI/Engenio RDAC controllers.</li> </ul>

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*<sup>2</sup> command. When quotes are used, the vendor, product, and revision fields will be interpreted strictly according to the spec. Regular expressions may be integrated into the quoted strings. Should a field be defined without the requisite spacing, multipath will copy the string into the properly sized buffer and pad with the appropriate number of spaces. The specification expects the entire field to be populated by printable characters or spaces, as seen in the example above

- 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
```

---

<sup>2</sup> [http://en.wikipedia.org/wiki/SCSI\\_Inquiry\\_Command](http://en.wikipedia.org/wiki/SCSI_Inquiry_Command)

## **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:

```
3600d023000000000000e13955cc3757800 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* [80] describes some options of the **multipath** command that you might find useful.

## Π#vακας 5.6. Useful multipath Command Options

Option	Description
<b>-l</b>	Display the current multipath configuration gathered from <b>sysfs</b> and the device mapper.
<b>-ll</b>	Display the current multipath configuration gathered from <b>sysfs</b> , the device mapper, and all other available components on the system.
<b>-f device</b>	Remove the named multipath device.
<b>-F</b>	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-LogVol101 (253, 1)
mpathf (253, 7)
VolGroup00-LogVol100 (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*"<sup>3</sup> 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
```

---

<sup>3</sup> <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. #####

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 εργαλέα πελάτη. Όταν προκύπτει ένα αίτημα σύνδεσης, το `sshd` στέλνει 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 στέλνει μια συνεδρία απομακρυσμένου ελέγχου μετά την πιστοποίηση. Εάν ένας απομακρυσμένος χρήστης συνδεθεί σε ένα διακομιστή OpenSSH με `scp`, ο δαίμονας διακομιστή OpenSSH ξεκινάει μια ασφαλής αντιγραφή αρχείων ανάμεσα στον διακομιστή και τον πελάτη μετά την πιστοποίηση. Το OpenSSH μπορεί να χρησιμοποιήσει πολλούς μεθόδους πιστοποίησης, περιλαμβάνοντας απλά κωδικό, δημόσιο κλειδί, και εισιτήριο Kerberos.

### 1.2. #####

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

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

Το πακέτο `openssh-server` μπορεί επίσης να επιλεγεί να εγκατασταθεί κατά τη διαδικασία εγκατάστασης της έκδοσης Διακομιστή.

### 1.3. #####

Μπορείτε να διαμορφώσετε την προεπιλεγμένη συμπεριφορά της εφαρμογής διακομιστή OpenSSH, `sshd`, κλώνοντας επεξεργασά στο αρχείο `/etc/ssh/sshd_config`. Για περισσότερες

πληροφορίες για τη διαμόρφωση κωδικών παραπομπών που χρησιμοποιούνται σε αυτό το αρχείο, μπορείτε να δείτε την κατάλληλη σελίδα εγχειριδίου με την ακόλουθη εντολή σε ένα τερματικό εντολόν:

```
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 προστατίψετε από επεξεργασία ώστε να έχετε τις αρχικές ρυθμίσεις σας αναφορά και να τις επαναχρησιμοποιήσετε που χρειάζεται.

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

```
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 παραπομπών που μπορείτε να αλλάξετε:

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

```
Port 2222
```

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

```
PubkeyAuthentication yes
```

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

- Για να κνέτε το διακομιστή OpenSSH να προβλίνει περιεχόμενα του αρχείου `/etc/issue.net` σαν ένα λήβαρο πριν τη σύνδεση, απλώς προσθέστε # τροποποιήστε τη γραμμή:

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

Στο αρχείο `/etc/ssh/sshd_config`.

Αφού κνέτε 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 εντολόν:

```
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. ##### 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 παρ#γείτε κλειδι#, απ# να τερματικ# εντολ#ν πληκτρολογε#στε:

```
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.

Εξορισμο# το ##μ#### κλειδ# αποθηκε#εται στο αρχε#ο `~/.ssh/id_dsa.pub`, εν# το `~/.ssh/id_dsa` ε#ναι το ##### κλειδ#. Τ#ρα αντιγρ#ψτε το αρχε#ο `id_dsa.pub` στον απομακρυσμ#νο κεντρικ# υπολογιστ# και επισυν#ψτε το στο `~/.ssh/authorized_keys` πληκτρολογ#ντας:

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

Τ#λος, επανελ#γξτε τα δικαι#ματα στο αρχε#ο `authorized_keys`, μ#νο ο πιστοποιημ#νος χρ#στης θα πρ#πει να #χει διακαι#ματα αν#γνωσης και επεξεργασ#ας. Ε#ν τα δικαι#ματα δεν ε#ναι σωστ# αλλ#ξτε τα:

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

Τ#ρα θα πρ#πει να μπορε#τε να συνδ#εστε με SSH στον κεντρικ# υπολογιστ# χωρ#ς να σας ζητηθε# κωδικ#ς.

## 1.5. #####

- *Ubuntu Wiki SSH<sup>1</sup> page.*
- ##### *OpenSSH<sup>2</sup>*
- #####μ#### ##### *Wiki OpenSSH<sup>3</sup>*

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

<sup>2</sup> <http://www.openssh.org/>

<sup>3</sup> <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 [##### 8, ##### μ##### μ## \(DNS\) \[141\]](#) 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. #####

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. #####

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 [Puppet 2.4, Chapter 2.4, \[88\]](#).

## 2.4. #####

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

---

<sup>4</sup> <http://docs.puppetlabs.com/>

<sup>5</sup> <http://forge.puppetlabs.com/>

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

<sup>7</sup> <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. #####**

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*<sup>8</sup>. 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)*<sup>9</sup>.



Not present on Ubuntu Universe repositories, but on *Zentyal Team PPA*<sup>10</sup> 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.
- **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.

<sup>8</sup> <https://launchpad.net/~zentyal/>

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

<sup>10</sup> <https://launchpad.net/~zentyal/>



- 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. #####

*Zentyal Official Documentation*<sup>11</sup> page.

See also *Zentyal Community Documentation*<sup>12</sup> page.

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

---

<sup>11</sup> <http://doc.zentyal.org/>

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

<sup>13</sup> <http://forum.zentyal.org/>

---

## Κεφάλαιο 7. Πιστοποίηση δικτύου

This section applies LDAP to network authentication and authorization.

## 1. ##### 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*<sup>1</sup>, 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*<sup>2</sup>.

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)

<sup>1</sup> <http://tools.ietf.org/html/rfc4510>

<sup>2</sup> <http://tools.ietf.org/html/rfc2849>

backend. Examples include an address book, a list of email addresses, and a mail server's configuration.

## 1.1. #####

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. #####

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*<sup>3</sup> 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
```

## 1.6. #####

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*.

---

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

Replication is achieved via the *Sync REPL* 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-sync REPL*. 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 [μ#μ# 1.1, &#x201C;#####&#x201D; \[95\]](#). 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. #####μ#

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 its 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*<sup>4</sup>.

## 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
```

---

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

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 /
```

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
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 \ -
```

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 `#μ#μ# 1.6, &#x201C;#####&#x201D; [102]` and have configured TLS for authentication on the Provider by following `#μ#μ# 1.8, &#x201C;TLS&#x201D; [108]`.

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
```

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. ##### 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 διλόγο 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 [μ#μ# 2, &#x201C;Samba ### LDAP&#x201D; \[120\]](#) 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. ##### #μ####

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 `&#x201C;secret&#x201D;` 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 χρ#στη:

```
sudo ldapdeleteuser george
```

- Προσθήκη ομ#δας:

```
sudo ldapaddgroup qa
```

- Διαγραφή ομ#δας:

```
sudo ldapdeletigroup qa
```

- Προσθήκη χρ#στη σε ομ#δα:

```
sudo ldapaddusertogroup george qa
```

Θα πρ#πει να #χει εμφανιστε# #να γν#ρισμα *memberUid* για την ομ#δα *qa*, με τιμ# *george*.

- Αφα#ρεση χρ#στη απ# ομ#δα:

```
sudo ldapdeleteuserfromgroup george qa
```

Το γν#ρισμα *memberUid* θα πρ#πει να #χει αφαιρεθε# απ# την ομ#δα *qa*.

- Το σεν#ριο `ldapmodifyuser` σας επιτρ#πει να προσθε#τετε, να αφαιρε#τε και να αντικαθιστ#τε τα γνωρ#σματα εν#ς χρ#στη. The Το σεν#ριο αυτ# χρησιμοποιε# την #δια σ#νταξη με το `ldapmodify`. Π.χ.:

```
sudo ldapmodifyuser george
```

```
# ## ##### # ##### :
```

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

```
objectClass: account
```

```
objectClass: posixAccount
```

```
cn: george
```

```
uid: george
```

```
uidNumber: 1001
```

```
gidNumber: 1001
```

```
homeDirectory: /home/george
```

```
loginShell: /bin/bash
```

```
gecos: george
```

```
description: User account
```

```
userPassword:: e1NTSEF9eXFstFcyWlhwWkFleGUybVdFWHZKRzJVMjFTSG9vcHk=
```

```
# ##### ## ##### ## ## ## ##### μ# CTRL-D.
```

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

```
replace: geocos
```

```
gecos: George Carlin
```

Το *gecos* θα πρέπει να έχει γινεί [George Carlin](#).

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

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

Στον κατάλογο `/etc/ldapscripts` υπάρχουν `#####μ###` προτύπων. Αντιγράψτε `# μετονομάστε το αρχείο ldapadduser.template.sample` σε `/etc/ldapscripts/ldapadduser.template`:

```
sudo cp /usr/share/doc/ldapscripts/examples/ldapadduser.template.sample \
/etc/ldapscripts/ldapadduser.template
```

Edit the new template to add the desired attributes. The following will create new users with an `objectClass` of `inetOrgPerson`:

```
dn: uid=<user>,<usuffix>,<suffix>
objectClass: inetOrgPerson
objectClass: posixAccount
cn: <user>
sn: <ask>
uid: <user>
uidNumber: <uid>
gidNumber: <gid>
homeDirectory: <home>
loginShell: <shell>
gecos: <user>
description: User account
title: Employee
```

Notice the `<ask>` option used for the `sn` attribute. This will make `ldapadduser` prompt you for its value.

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

```
ldaprenamemachine5
ldapadduser6
ldapdeleteuserfromgroup7
ldapfinger8
ldapid9
```

<sup>5</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldaprenamemachine.1.html>

<sup>6</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapadduser.1.html>

<sup>7</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuserfromgroup.1.html>

<sup>8</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapfinger.1.html>

<sup>9</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapid.1.html>

```

ldapgid10
ldapmodifyuser11
ldaprenameuser12
lsldap13
ldapaddusertogroup14
ldapsetpasswd15
ldapinit16
ldapaddgroup17
ldapdeletgroup18
ldapmodifygroup19
ldapdeletemachine20
ldaprenamegroup21
ldapaddmachine22
ldapmodifymachine23
ldapsetprimarygroup24
ldapdeleteuser25

```

## 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

```

- 
- <sup>10</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapgid.1.html>
  - <sup>11</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapmodifyuser.1.html>
  - <sup>12</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldaprenameuser.1.html>
  - <sup>13</sup> <http://manpages.ubuntu.com/manpages/en/man1/lsldap.1.html>
  - <sup>14</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapaddusertogroup.1.html>
  - <sup>15</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapsetpasswd.1.html>
  - <sup>16</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapinit.1.html>
  - <sup>17</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapaddgroup.1.html>
  - <sup>18</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapdeletgroup.1.html>
  - <sup>19</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapmodifygroup.1.html>
  - <sup>20</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapdeletemachine.1.html>
  - <sup>21</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldaprenamegroup.1.html>
  - <sup>22</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapaddmachine.1.html>
  - <sup>23</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapmodifymachine.1.html>
  - <sup>24</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapsetprimarygroup.1.html>
  - <sup>25</sup> <http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuser.1.html>



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
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. #####

- The primary resource is the upstream documentation: [www.openldap.org](http://www.openldap.org)<sup>26</sup>
- 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`<sup>27</sup>  
`slapd-config`<sup>28</sup>  
`slapd.access`<sup>29</sup>  
`slapo-syncprov`<sup>30</sup>

- Other man pages:

`auth-client-config`<sup>31</sup>  
`pam-auth-update`<sup>32</sup>

<sup>26</sup> <http://www.openldap.org/>

<sup>27</sup> <http://manpages.ubuntu.com/manpages/en/man8/slapd.8.html>

<sup>28</sup> <http://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html>

<sup>29</sup> <http://manpages.ubuntu.com/manpages/en/man5/slapd.access.5.html>

<sup>30</sup> <http://manpages.ubuntu.com/manpages/en/man5/slapo-syncprov.5.html>

<sup>31</sup> <http://manpages.ubuntu.com/manpages/en/man8/auth-client-config.8.html>

<sup>32</sup> <http://manpages.ubuntu.com/manpages/en/man8/pam-auth-update.8.html>

- Zytrax's *LDAP for Rocket Scientists*<sup>33</sup>; a less pedantic but comprehensive treatment of LDAP
- A Ubuntu community *OpenLDAP wiki*<sup>34</sup> page has a collection of notes
- O'Reilly's *LDAP System Administration*<sup>35</sup> (textbook; 2003)
- Packt's *Mastering OpenLDAP*<sup>36</sup> (textbook; 2007)

---

<sup>33</sup> <http://www.zytrax.com/books/ldap/>

<sup>34</sup> <https://help.ubuntu.com/community/OpenLDAPServer>

<sup>35</sup> <http://www.oreilly.com/catalog/ldapsa/>

<sup>36</sup> <http://www.packtpub.com/OpenLDAP-Developers-Server-Open-Source-Linux/book>

## **2. Samba and LDAP**

This section covers the integration of Samba with LDAP. The Samba server's role will be that of a "standalone" server and the LDAP directory will provide the authentication layer in addition to containing the user, group, and machine account information that Samba requires in order to function (in any of its 3 possible roles). The pre-requisite is an OpenLDAP server configured with a directory that can accept authentication requests. See [Figure 1, &#x201C;OpenLDAP and Samba; \[94\]](#) 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 [Figure 1.4, &#x201C;Modifying the slapd Configuration Database; \[99\]](#).

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 `smblldap-tools` package to match your environment. The package is supposed to come with a configuration helper script (`smblldap-config.pl`, formerly `configure.pl`) that will ask questions about the needed options but there is a *bug*<sup>37</sup> whereby it is not installed (but found in the source code; `'apt-get source smblldap-tools'`).

---

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



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. ##### Samba

There are multiple ways to configure Samba. For details on some common configurations see ##### 18, *Samba* [293]. 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

# ##### 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.

Επανεκκιν#στε το *samba* για να ενεργοποι#σετε τις ν#ες ρυθμ#σεις:

```
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-groupadd38
smbldap-groupdel39
smbldap-groupmod40
smbldap-groupshow41
smbldap-passwd42
smbldap-populate43
smbldap-useradd44
smbldap-userdel45
smbldap-userinfo46
smbldap-userlist47
smbldap-usermod48
smbldap-usershow49
```

## 2.4. #####

- For more information on installing and configuring Samba see ##### 18, *Samba* [293] of this Ubuntu Server Guide.
- There are multiple places where LDAP and Samba is documented in the upstream *Samba HOWTO Collection*<sup>50</sup>.
- Regarding the above, see specifically the *passdb* section<sup>51</sup>.
- Although dated (2007), the *Linux Samba-OpenLDAP HOWTO*<sup>52</sup> contains valuable notes.
- The main page of the *Samba Ubuntu community documentation*<sup>53</sup> has a plethora of links to articles that may prove useful.

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### 3. Kerberos

Το Kerberos είναι ένα σύστημα πιστοποίησης δικτύου που βασίζεται στην αρχή του εμπιστού του τρίτου μέρους. Που τα άλλα δύο μέρη είναι ο χρήστης και η υπηρεσία στην οποία θάλει 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 ακριβές 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. #####

Αν έχετε καινούριο στο Kerberos, υπάρχουν ορισμένοι ρόλοι που είναι καλό να γνωρίζετε πριν στρώσετε έναν εξυπηρετητή Kerberos. Οι περισσότεροι από αυτούς τους ρόλους μπορεί να σας θυμίζουν άλλα περιβάλλοντα:

- *Principal (#####)*: Όλοι οι χρήστες, υπολογιστές και υπηρεσίες που παρόνται 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 - ##### μ#)*: αποτελείται από 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 (#####)*: 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 (##### - TGS): ##### μ#*.  
##### μ#
- *Tickets (#####)*: επιβεβαιώνουν την ταυτότητα των δύο διευθυντών. Που ο ένας διευθυντής είναι χρήστης και ο άλλος μια υπηρεσία που έχει ζητήσει ο χρήστης. Τα δελτία χρησιμοποιούν ένα κλειδί κρυπτογράφησης που διασφαλίζει την επικοινωνία κατά τη διάρκεια της πιστοποιημένης συνεδρίας.
- *##### Keytab*: είναι αρχεία που εξάγονται από τη βάση δεδομένων διευθυντών του KDC και περιέχουν το κλειδί κρυπτογράφησης μιας υπηρεσίας # 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. ##### Kerberos

### 3.2.1. #####

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 [μμμ 2.3, &#x201C;##### Master&#x201D; \[144\]](#) 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 [μμμ 4, &#x201C;#####μμμ ##### μμ NTP&#x201D; \[52\]](#).

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 συν#χεια, δημιουργ#στε το ν#ο realm χρησιμοποι#ντας το `kdb5_newrealm`:

```
sudo krb5_newrealm
```

### 3.2.2. #####

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 #νομα χρηστη του διαχειριστ#.

2. Στη συνέχεια, ο ν#ος χρηστης - διαχειριστ#ς πρ#πει να αποκτήσει τα κατάλληλα δικαι#ματα ACL. Τα δικαι#ματα ορ#ζονται στο αρχε#ο `/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. Τ#ρα, επανεκκιν#στε το `krb5-admin-server` για να ενεργοποι#σετε το ACL:

```
sudo service krb5-admin-server restart
```

4. Μπορε#τε να δοκιμ#σετε το ν#ο principal χρησιμοποιντας το εργαλε#ο `kinit`:

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

Αφού εισήγαγε 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 #νομα του domain, το πρωτεύον KDC και το δευτερεύον KDC.

Δείτε το ##### 8, ##### ##μ#### μ## (DNS) [141] για λεπτομέρες οδηγίες ρυθμίσεις του DNS.

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

### 3.3. ##### 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, εισήγαγε το #νομα του πρωτεύοντος KDC:

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

2. Αφού εγκατασταθούν τα πακέτα, δημιουργήστε τον principal του δευτέρου KDC. Απλοποιήστε το τερματικό, δηλαδή:

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



Στη συνέχεια, κάθε φορά που θα εκτελέσετε εντολή kadmin, θα ερωτηστείτε 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 πρώτο όσο και στο δεύτερο KDC, δημιουργήστε ένα αρχείο `/etc/krb5kdc/kpropd.acl`:

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

6. Δημιουργήστε μια βήμα βήμα δεδομένων στο `##### KDC`:

```
sudo kdb5_util -s create
```

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

```
sudo kpropd -s
```

8. Απλοποιήστε το τερματικό στο `##### KDC`, δημιουργήστε ένα αρχείο `dump` της βήμα βήμα 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 *##### KDC*, δημιουργήστε ένα αρχείο *##### (stash)* για το κριό (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. ##### Kerberos ### Linux

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

### 3.4.1. #####

Για να γ#νει η πιστοπο#ηση σε realm Kerberos, απαιτο#νται τα πακ#τα krb5-user και libpam-krb5, καθ#ς και ορισμ#να ακ#μη, που, αν και δεν ε#ναι απολ#τως απαρα#τητα, διευκολ#νουν σημαντικ# το #ργο σας. Για να τα εγκαταστ#σετε, πληκτρολογε#τε στο τερματικ#:

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

Το πακ#το auth-client-config σας επιτρ#πει να ρυθμ#ζεται ε#κολα το PAM για πιστοπο#ηση απ# πολλαπλ#ς πηγ#ς, εν# το libpam-ccreds αποθηκε#ει τα στοιχε#α πιστοπο#ησης, #τσι #στε να μπορε#τε να κ#νετε ε#σοδο σε περ#πτωση που το Κ#ντρο Διανομ#ς Κλειδι#ν (KDC) δεν ε#ναι διαθ#σιμο. Το πακ#το αυτ# ε#ναι χρ#σιμο και για φορητο#ς υπολογιστ#ς που κ#νουν πιστοπο#ηση μ#σω Kerberos #ταν βρ#σκονται στο εταιρικ# δ#κτυο, αλλ# που θα πρ#πει να μπορο#ν να χρησιμοποιηθο#ν και εκτ#ς δικτ#ου.

### 3.4.2. #####

Για να ρυθμ#σετε τον πελ#τη, ε#σαγετε τα παρακ#τω στο τερματικ#:

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

Θα σας ζητηθε# το #νομα του realm του Kerberos. Επ#σης, αν το DNS δεν #χει ρυθμιστε# με τις εγγραφ#ς SRV του Kerberos, θα σας ζητηθε# το hostname του KDC και ο εξυπηρετητ#ς διαχε#ρισης του realm.

Το dpkg-reconfigure προσθ#τει εγγραφ#ς στο αρχε#ο /etc/krb5.conf του realm. Οι εγγραφ#ς σας θα πρ#πει να μοι#ζουν στις ακ#λουθες:

```
[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 [#μ#μ# 3.2.1](#), [#x201C;#####&#x201D](#); [127], 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 να 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 πρόγραμμα **libpam-krb5** έτσι ώστε να ζητεί δελτίο κατά την είσοδο:

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

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

### 3.5. #####

- For more information on MIT's version of Kerberos, see the *MIT Kerberos*<sup>54</sup> site.
- The *Ubuntu Wiki Kerberos*<sup>55</sup> page has more details.
- Το εγχειρίδιο *Kerberos: The Definitive Guide*<sup>56</sup> 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*<sup>57</sup> if you have Kerberos questions.

---

<sup>54</sup> <http://web.mit.edu/Kerberos/>

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

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

<sup>57</sup> <http://freenode.net/>

## 4. Kerberos ### 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 βήσης δεδομένων principal Kerberos μεταξύ δφο εξυπηρετητν μπορε# να ε#ναι πολ#πλοκη διαδικασ#, εν# επ#σης προσθ#τει μ#α ακ#μη β#ση δεδομ#νων χρ#στη στο δ#κτυ# σας. Ευτυχ#, το Kerberos του MIT μπορε# να ρυθμιστε# #τσι #στε να χρησιμοποιε# #ναν κατ#λογο LDAP ως β#ση δεδομ#νων principal. Αυτ# η εν#τητα καλ#πτει τη διαδικασ# ρ#θμισης εν#ς πρωτε#οντος και εν#ς δευτερε#οντος εξυπηρετητ# kerberos #στε να χρησιμοποιο#ν το OpenLDAP για τη β#ση δεδομ#νων principal.



The examples presented here assume MIT Kerberos and OpenLDAP.

### 4.1. ###μ### ### OpenLDAP

Καταρχ#, πρ#πει να φορτωθε# το κατ#λληλο ###μ# ne## #ναν εξυπηρετητ# OpenLDAP με δικτυακ# σ#νδεση στα πρωτε#οντα και δευτερε#οντα KDC. Στο υπ#λοιπο αυτ#ς της εν#τητας υποθ#τούμε #τι #χετε ρυθμ#σει την αντιγραφ# του LDAP μεταξύ δφο τουλ#χιστον εξυπηρετητν. Για πληροφορ#ες σχετικ# με τη ρ#θμιση του OpenLDAP δε#τε το #μ#μ# 1, &#x201C;##### OpenLDAP&#x201D; [94].

Επ#σης, απαιτε#ται η ρ#θμιση του OpenLDAP για συνδ#σεις TLS και SSL, #τσι #στε να κρυπτογραφε#ται η κ#νηση μεταξύ KDC και εξυπηρετητ# LDAP. Δε#τε το #μ#μ# 1.8, &#x201C;TLS&#x201D; [108] για λεπτομ#ρειες.



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 φορτ#σετε το σχ#μα στο LDAP, εγκαταστ#στε το πακ#το krb5-kdc-ldap στον εξυπηρετητ# LDAP. Απ# το τερματικ#, δ#νετε:

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

- Στη συν#χεια, εξ#γετε το αρχε#ο 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 σχ#μα του *kerberos* πρ#πει να προστεθε# στο δ#ντρο του *cn=config*. Η διαδικασ# προσθ#κης ν#ου σχ#ματος στο slapd περιγρ#φεται και στο #μ#μ# 1.4, &#x201C;Modifying the slapd Configuration Database&#x201D; [99].

1. Καταρχ#, δημιουργ#στε #να αρχε#ο ρυθμ#σεων με #νομα *schema\_convert.conf*, #κ#τι εξ#σου περιγραφικ#, που θα περι#χει τις ακ#λουθες γραμμ#ς:

```
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 χρειαστεί χρησιμοποιήσει διαφορετικά.

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

```
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 απλώς βεβαιωθείτε ότι αφαιρέθηκαν τα συγκεκριμένα γνωστά.

5. Φορτίστε 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 γν#ρισμα *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. Τ#λος, ενημερ#στε τις Λ#στες Ελ#γχου Πρ#σβασης (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"
```

Αυτ# #ταν, ο κατ#λογος LDAP ε#ναι τ#ρα #τοιμος να λειτουργ#σει ως β#ση δεδομ#νων principal Kerberos.

## 4.2. ##### KDC

Αφο# ρυθμιστε# το OpenLDAP θα πρ#πει να ρυθμιστε# και το KDC.

- Καταρχ#ς, εγκαταστ#στε τα απαραίτητα πακ#τα απ# το τερματικ#, εισ#γοντας:

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

- Τ#ρα, τροποποι#στε το `/etc/krb5.conf`, προσθ#τοντας τις ακ#λουθες επιλογ#ς στα κατ#λληλα σημει#α:

```
[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 συνδεση με τον εξυπηρετητή LDAP. Προκειμένου 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 δεύτερο KDC, για να επιτρέπει 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 εισήγετε:

```
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 γνωσμάτα `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 νυντώς 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 υπόδντρο του `realm`.

#### 4.3. ##### KDC

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

1. Καταρχής, εγκαταστήστε τα απαραίτητα πακέτα απ το τερματικό, εισήγοντας:

```
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) σ#νδεσης 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. Τ#ρα, στο ##### KDC αντιγρ#ψτε το κρυμ#νο ##### (master) του /etc/krb5kdc/.k5.EXAMPLE.COM στο δευτερε#ον KDC. Θυμηθε#τε να κ#νετε την αντιγραφ# μ#σω κρυπτογραφημ#νης σ#νδεσης, π.χ. με το scp, # χρησιμοποιν#τας φυσικ# μ#σο.

```

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, ακριβή και αν δεν είναι διαθέσιμοι ένας εξυπηρετητής Kerberos, ένας εξυπηρετητής LDAP ή ένας εξυπηρετητής Kerberos και ένας LDAP.

#### 4.4. #####

- Ο ##### Kerberos<sup>58</sup> διαθέτει ορισμένες επιπλέον λεπτομέρειες.
- For more information on kdb5\_ldap\_util see *Section 5.6*<sup>59</sup> and the *kdb5\_ldap\_util man page*<sup>60</sup>.
- Another useful link is the *krb5.conf man page*<sup>61</sup>.
- Also, see the *Kerberos and LDAP*<sup>62</sup> Ubuntu wiki page.

<sup>58</sup> [http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Configuring-Kerberos-with-OpenLDAP-back\\_002dend](http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Configuring-Kerberos-with-OpenLDAP-back_002dend)

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

<sup>60</sup> [http://manpages.ubuntu.com/manpages/raring/en/man8/kdb5\\_ldap\\_util.8.html](http://manpages.ubuntu.com/manpages/raring/en/man8/kdb5_ldap_util.8.html)

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

<sup>62</sup> <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 θυμάμαστε διευθύνσεις IP. Οι υπολογιστές που εκτελούν το DNS ονομαζονται **server**. Το Ubuntu **ρχεται** με το BIND (Berkley Internet Naming Daemon), το πιο κοινό πρόγραμμα που χρησιμοποιείται για τη διατήρηση ενός εξυπηρετητή ονομάτων στο Linux.

## **1. #####**

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. #####

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

- #ταν ε#ναι ρυθμισμ#νο ως εξυπηρετητ#ς ονομ#των προσωριν#ς αποθ#κευσης, το BIND9 θα βρ#σκει την απ#ντηση σε ερωτ#ματα ονομ#των και θα θυμ#ται την απ#ντηση #ταν ερωτ#ται ξαν# για το #νομα.
- 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. #####

Τα αρχε#α ρυθμ#σεων του DNS ε#ναι αποθηκευμ#να στον κατ#λογο `/etc/bind`. Το κ#ριο αρχε#ο ρυθμ#σεων ε#ναι το `/etc/bind/named.conf`.

Η γραμμ# `include` καθορ#ζει το #νομα του αρχε#ου που περι#χει τις επιλογ#ς DNS. Η γραμμ# `directory` στο αρχε#ο `/etc/bind/named.conf.options` λ#ει στο DNS πο# να ψ#ξει για αρχε#α. #λα τα αρχε#α που χρησιμοποιε# το BIND θα ε#ναι σε σχετικ# τοποθεσ#α με αυτ#ν τον κατ#λογο.

Το αρχε#ο με #νομα `/etc/bind/db.root` περιγρ#φει τους κεντρικο#ς (root) εξυπηρετητ#ς ονομ#των σε #λο τον κ#σμο. Οι εξυπηρετητ#ς αλλ#ζουν με την π#ροδο του χρ#νου, οπ#τε το αρχε#ο `/etc/bind/db.root` πρ#πει να συντηρε#ται αν# διαστ#ματα. Αυτ# συν#θως γ#νεται με ενημερ#σεις του πακ#του bind9. Η εν#τητα `zone` ορ#ζει #ναν εξυπηρετητ# master και ε#ναι αποθηκευμ#νη σε #να αρχε#ο που αναφ#ρεται στην επιλογ# `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. #####

Η προεπιλεγμ#νη ρ#θμιση ε#ναι η εγκατ#σταση να λειτουργε# ως εξυπηρετητ#ς προσωριν#ς αποθ#κευσης. Αυτ# που χρει#ζεται ε#ναι απλ# η προσθ#κη των διευθ#νσεων IP των εξυπηρετητ#ν DNS του παρ#χου (ISP) σας. Απλ# αποσχολι#στε και επεξεργαστε#τε τα ακ#λουθα 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 επανεκκινείτε τον εξυπηρετητή DNS, για να ενεργοποιήσετε τις νέες ρυθμίσεις. Σε ένα τερματικό πληκτρολογείτε:

```
sudo service bind9 restart
```

Δείτε το `3.1.2, dig 3.1.2` για πληροφορίες σχετικές με τον έλεγχο ενός εξυπηρετητή DNS προσωρινής αποθήκευσης.

## 2.3. ##### Master

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

### 2.3.1. ##### Forward

Για να προσθήσετε μια ζώνη DNS στο BIND9, μετατρέποντας 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 αυξήσετε τον ##### μ# κάθε φορά που κάνετε αλλαγές στο αρχείο ζώνης. Αν κάνετε πολλές αλλαγές πριν επανεκκινήσετε το BIND9, απλ# αυξήστε τον σειριακ# αριθμ# μ#α φορά.

Τώρα, μπορείτε να προσθέσετε καταγραφές DNS στο κτω μέρος του αρχείου ζώνης. Δείτε το #μ#μ# 4.1, &#x201C;##### &#x201D; [153] 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. ##### Reverse

Τώρα που η ζώνη #χει ρυθμιστε# και επιλ#ει ον#ματα σε διευθ#νσεις IP, χρει#ζεται επ#σης και μ#α ##### Reverse. Μ#α ζώνη Reverse επιτ#πει στο DNS να επιλ#ει διευθ#νσεις σε ον#ματα.

Επεξεργαστε#τε το /etc/bind/named.conf.local και προσθ#στε τα ακ#λουθα:

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



Αντικαταστ#στε το 1.168.192 με τις πρ#τες τρεις οκτ#δες (octets) του δικτ#ου που χρησιμοποιε#τε. Επ#σης, ονομ#στε το αρχείο ζώνης /etc/bind/db.192 κατ#λληλα. Πρ#πει να ε#ναι ταρι#ζει με την πρ#τη οκτ#δα του δικτ#ου σας.

Τώρα δημιουργ#στε το αρχείο /etc/bind/db.192:

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

Μετά επεξεργαστείτε το `/etc/bind/db.192` αλλοζώντας βασικές τις #διες επιλογές #πως 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. ##### Master

Μάλιστα #νας ##### Master εξυπηρετητής #χει ρυθμιστεί, #νας ##### Master χρειάζεται για να διατηρηθεί η διαθεσιμότητα του χ#ρου σε περίπτωση που ο Κ#ριος εξυπηρετητής δεν ε#ναι διαθ#σιμος.

Πρ#τα, στον Κ#ριο Master εξυπηρετητή, η μεταφορ# ζων#ν πρ#πει να επιτραπεί. Προσθ#στε την επιλογ# `allow-transfer` στα παραδε#γματα ζων#ν 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 Κριό. 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 [μ#μ# 4, &#x201C;AppArmor&#x201D; \[171\]](#).

### 3. #####μ####

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

#### 3.1. #####μ#

##### 3.1.1. resolv.conf

Το πρώτο βήμα για να δοκιμάσετε το BIND9 είναι να προσθέσετε τη διεύθυνση IP του εξυπηρετητή ονομάτων σε έναν επιλύτη (hosts resolver). Ο Κρίσιος εξυπηρετητής ονομάτων θα πρέπει να είναι ρυθμισμένος πώς και ένας άλλος υπολογιστής για να ελέγχονται δύο φορές τα πράγματα. Απλώς 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 πρώτος δεν είναι διαθέσιμος.

##### 3.1.2. dig

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

- Αφού εγκαταστήσετε το BIND9 χρησιμοποιήστε το `dig` με την διεύθυνση `loopback` για να σιγουρευτείτε πως αναμνεί για συνδέσεις στην θύρα <sup>53</sup>. Σε ένα τερματικό πληκτρολογήστε:

```
dig -x 127.0.0.1
```

Θα πρέπει να δείτε γραμμές παρμολίες 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 ##### (Caching), κντε# `dig` σε ένα εξωτερικό #νομα τομής 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
```

Μετ# απ# μ#α δε#τερη εκ#λεση του `dig` θα πρέπει να υπ#ρχει βελ#ωση:

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

### 3.1.3. ping

Για να δείτε πως οι εφαρμογές χρησιμοποιούν το DNS για να αναλίσουν 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 επιλέξει 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 κενέτε τις αλλαγές μέσα.

- 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
```

- Παρόμοια, 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 `#####` της ζώνης σας πιθανότατα θα είναι διαφορετικός.

### 3.2. #####

Το BIND<sup>9</sup> έχει μια μεγάλη ποικιλία επιλογών για τη ρύθμιση της καταγραφής. Υπάρχουν δύο κριτές επιλογής. Η επιλογή *channel* ρυθμίζει ποπνε 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 καλππει τη ρύθμιση του BIND<sup>9</sup> στε να στλνει πληροφορίες αποσφάλμωσης σχετικς με τα ερωτματα DNS σε να ξεχωριστ αρχεο.

- Πρτα, χρειζεται να ρυθμσουμε να κανλι (channel) για να ορσουμε σε ποιο αρχεο θα στλνονται τα μηνματα. Επεξεργαστετε το `/etc/bind/named.conf.local` και προσθστε το ακλουθο:

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

- Μετ, ρυθμστε μια κατηγορ (category) που θα στλνει λλα τα ερωτματα DNS στο αρχεο ερωτημτων:

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



Σημεωση: Η επιλογ *debug* μπορε να πρει τιμ απ<sup>1</sup> ως<sup>3</sup>. Αν δεν οριστεί εππεδο, η προεπιλογ είναι το εππεδο<sup>1</sup>.

- Αφο η ##### *named* εκτελεται ως ο χρστης *bind*, το αρχεο `/var/log/query.log` πρπει να δημιουργηθ και να αλλαχθ ο ιδιοκτης 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, επαναφορτίστε το προφίλ:

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

Για περισσότερες πληροφορίες σχετικές με το AppArmor δείτε το [μικροβιβλίο 4, <AppArmor>](#); [171]

- 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 καλύτερη προχωρημένων επιλογών δείτε το [μικροβιβλίο 4.2, <BIND9>](#); [153].

## 4. #####

### 4.1. #####

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

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

```
www      IN      A      192.168.1.12
```

- Καταγραφή *CNAME*: Χρησιμοποιείται για τη δημιουργία μιας συντμευσης σε μια 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 ποιος θα πρέπει να στέλνονται τα email. Πρέπει να δείχνει σε μια 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 μια καταγραφή *A*, όχι σε *CNAME*. Εάν είναι που ορίζονται ο Πρωτεύων και ο Δευτερεύων εξυπηρετητές.

```
          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. #####

- The *BIND9 Server HOWTO*<sup>1</sup> in the Ubuntu Wiki has a lot of useful information.
- The *DNS HOWTO*<sup>2</sup> at The Linux Documentation Project also has lots of information about configuring BIND9.
- Bind9.net*<sup>3</sup> has links to a large collection of DNS and BIND9 resources.
- DNS and BIND*<sup>4</sup> is a popular book now in its fifth edition. There is now also a *DNS and BIND on IPv6*<sup>5</sup> book.

<sup>1</sup> <https://help.ubuntu.com/community/BIND9ServerHowto>

<sup>2</sup> <http://www.tldp.org/HOWTO/DNS-HOWTO.html>

<sup>3</sup> <http://www.bind9.net/>

<sup>4</sup> <http://shop.oreilly.com/product/9780596100575.do>

<sup>5</sup> <http://shop.oreilly.com/product/0636920020158.do>

- να πολλή καλή ιδέα να ζητήσετε βοήθεια για το BIND9, και να συμμετάσχετε στην κοινότητα του Ubuntu Server, είναι το κανάλι IRC *#ubuntu-server* στο δίκτυο *freenode*<sup>6</sup>.

---

<sup>6</sup> <http://freenode.net>



---

## Κεφάλαιο 9. Ασφάλεια

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

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. #####

Η διαχείριση χρηστών είναι ένα κρίσιμο σημείο για να διατηρηθεί η ασφάλεια συστήματος. Αναποτελεσματική διαχείριση χρηστών και προνομίων οδηγούν συχνά πολλών συστημάτων σε κίνδυνο. Επομένως, είναι σημαντικό να καταλάβετε πως μπορείτε να προστατέσετε τον διακομιστή σας μέσω απλών και αποτελεσματικών τεχνικών διαχείρισης του λογαριασμού χρήστη.

### 1.1. #####;

Οι προγραμματιστές Ubuntu πήραν μια ευγενή να απενεργοποιούν το λογαριασμό διαχείρισης βήσης εξορισμού σε όλες τις εγκαταστάσεις Ubuntu. Αυτό δε σημαίνει ότι ο λογαριασμός βήσης έχει διαγραφεί # δεν μπορεί να προσπελαστεί. Απλώς του έχει δοθεί ένας κωδικός ο οποίος δεν ταιριάζει με κάποια κρυπτογραφημένη τιμή, #τσι δεν μπορεί να συνδεθεί #μέσα μ#νος του.

Αν#θετα, οι χ#στες ενθαρρ#νονται να δημιουργ#σουν #να εργαλ#ο με #νομα `sudo` για να εκτελ#σουν διαχειριστικ# καθ#κοντα του συστ#ματος. Το `Sudo` επιτρ#πει σε #ναν εξουσιοδοτημ#νο χ#στη προσωριν# να ανυψ#σει τα δικαι#ματ# του χρησιμοποι#ντας το δικ# τους κωδικ# αντ# να πρ#πει να γνωρ#σουν τον κωδικ# που αν#κει στο λογαριασμ# β#σης. Αυτό η απλ# αλλ# αποτελεσματικ# μεθοδολογ#ας παρ#χει ευθ#νη για #λες τις εν#ργειες χ#στη, και δ#νει στο διαχειριστ# #λεγχο για το ποιες εν#ργειες #νας χ#στης μπορεί να εκτελ#σει με τα συγκεκριμ#να προν#μια.

- Εάν για κάποιο λ#γο θ#λετε να ενεργοποι#σετε τον λογαριασμ# β#σης, απλ#ς δ#στε του #ναν κωδικ#:



Configurations with root passwords are not supported.

```
sudo passwd
```

Το `Sudo` θα σας ζητήσει τον κωδικ# σας, και μετ# θα σας ζητήσει να παρ#χετε #ναν καινο#ριο κωδικ# για τη β#ση #πως φ#νεται παρακ#τω:

```
[sudo] password for username: (#####)
Enter new UNIX password: (#####)
Retype new UNIX password: (#####)
passwd: password updated successfully
```

- Για να απενεργοποι#σετε τον λογαριασμ# β#σης, χρησιμοποιε#στε την ακ#λουθη σ#νταξη `passwd`:

```
sudo passwd -l root
```

- Πρ#πει να διαβ#σετε περισσ#τερα για το `Sudo` κοιτ#ντας την αρχικ# του σελ#δα:

`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. #####

Η διαδικασία διαχείρισης τοπικών χρηστών και ομάδων είναι μείωση και διαφύλαξη πολλών ληγών 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, χρησιμοποιήστε την ακόλουθη συνταγή, και ακολουθήστε τις προτροπές να δώσετε κωδικό στο λογαριασμό και αναγνωρίσιμα χαρακτηριστικά όπως πλάνες, νόμα, τηλέφωνο, κλπ.

`sudo adduser username`

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

`sudo deluser username`

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

Θυμηθείτε, κάθε χρήστης που προστίθεται αργότερα με το ίδιο UID/GID με τον προηγούμενο ιδιοκτήτη τμήρα χειρσβάστη σε αυτόν τον φάκελο εάν δεν έχετε ληβεί τις κατάλληλες προφυλάξεις.

Ήσως θέλετε να αλλάξετε τις τιμές UID/GID σε κάτι πιο κατάλληλο, όπως ο λογαριασμός βήσης, και πιθανόν ακόμα και να μεταφύρετε 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 να ξεκλειδώσετε προσωρινά ένα λογαριασμό χρήστη, χρησιμοποιήστε την ακόλουθη συνταγή, αντίστοιχα:

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

- Για να προσθ#σετε # να διαγρ#ψετε μια προσαρμοσ#νη ομ#δα, χρησιμοποι#στε την ακ#λουθη σ#νταξη, αντ#στοιχα:

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

- Για να προσθ#σετε μια ομ#δα χρηστ#, χρησιμοποι#στε την ακ#λουθη σ#νταξη:

```
sudo adduser username groupname
```

### 1.3. #####

#ταν δημιουργε#τε #νας καινο#ριος χρ#στης, η λειτουργ#α adduser δημιουργε# #ναν ολοκα#νουριο αρχικ# κατ#λογο με #νομα /home/username, αντ#στοιχα. Το προεπιλεγμ#νο προφ#λ δημιουργε#τε απ# τα περιεχ#μενα που βρ#σκονται στον κατ#λογο /etc/skel, που περιλαμβ#νει #λα τα βασικ# στοιχε#α προφ#λ.

E#ν ο διακομιστ#ς σας θα ε#ναι αρχικ#ς για πολλαπλο#ς χρ#στες, θα πρ#πει να προσ#ξετε πολ# τα διακαι#ματα του αρχικο# καταλ#γου χρ#στη για να βεβαιωθε#τε για την εμπιστευτικ#τητα. Εξορισμο#, οι αρχικο# κατ#λογοι χρ#στη στο Ubuntu δημιουργο#νται με δικαι#ματα αν#γνωσης/εκτ#λεσης. Αυτ# σημα#νει, #τι #λοι οι χρ#στες μπορο#ν να περιηγηθο#ν και και να #χουν πρ#σβαση στα περιεχ#μενα αρχικ#ν καταλ#γων #λλων χρηστ#. Αυτ# #σως δεν ε#ναι κατ#λληλο για το περιβ#λλον σας.

- Για να επαληθε#σετε τα διακαι#ματα αρχικ#ν καταλ#γων των τρεχ#ντων χρηστ#ν σας, χρησιμοποι#στε την ακ#λουθη σ#νταξη:

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

Η ακ#λουθη #ξοδος δε#χνει #τι ο κατ#λογος /home/username #χει διακαι#ματα αν#γνωσης για #λους:

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

- Μπορε#τε να αφαιρ#σετε τα δικαι#ματα αν#γνωσης για #λους χρησιμοποι#ντας την ακ#λουθη σ#νταξη:

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



Μερικο# #νθρωποι #χουν την τ#ση να χρησιμοποιο#ν την αναδρομικ# επιλογ# (-R) η οπο#α τροποποιε# αδιακρ#τως #λους τους εξαρτημ#νους φακ#λους και τα αρχε#α, αλλ# αυτ# δεν ε#ναι αναγκα#ο, και μπορε# να αποφ#ρει #λλα ανεπιθ#μητα αποτελ#σματα. Ο γονικ#ς κατ#λογος απ# μ#νος του ε#ναι ικαν#ς να εμποδ#σει την παρ#νομη πρ#σβαση σε οτιδ#ποτε κ#τω απ# το γονικ# κατ#λογο.

Μια πολύ πιο αποτελεσματική προσγγιση του θέματος θα ήταν να τροποποιήσετε τα εξορισμό καθολικά δικαιώματα του `adduser` ήταν δημιουργήτε αρχικούς καταλόγους χρήστην. Απλώς επεξεργαστείτε το `/etc/adduser.conf` και ρυθμίστε τη μεταβλητή `DIR_MODE` σε κάτι κατάλληλο, ώστε όλοι οι καινούριοι αρχικοί καταλόγοι να λαμβάνουν τα σωστά δικαιώματα.

```
DIR_MODE=0750
```

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

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

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

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

## 1.4. #####

Μια ισχυρή πολιτική κωδικού πρόσβασης είναι μία από τις πιο σημαντικές πτυχές της στρώσης ασφαλείας σας. Πολλές επιτυχημένες παραβιάσεις της ασφάλειας περιλαμβάνουν απλώς ωμή βία και επιθέσεις λεξικού εναντίον αδυναμών κωδικών πρόσβασης. Εάν σκοπεύετε να προσφύρετε οποιαδήποτε μορφή απομακρυσμένης πρόσβασης που να αφορά το τοπικό σύστημα κωδικού σας, βεβαιωθείτε ότι αντιμετωπίζετε ικανοποιητικές ελάχιστες απαιτήσεις της πολυπλοκότητας κωδικού πρόσβασης, το αντάτο ριό διάρκειας ζωής κωδικού πρόσβασης, και τους συχνούς ελέγχους των συστημάτων ελέγχου ταυτότητας σας.

### 1.4.1. #####

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. #####

#ταν δημιουργε#τε λογαριασμο#ς χρηστ#ν, θα πρ#πει να δημιουργ#σετε μια πολιτικ# να #χετε ελ#χιστη και μ#γιστη ζω# κωδικο# αναγκ#ζοντας τους χρ#στες να αλλ#ζουν τους κωδικο#ς τους #ταν λ#γουν.

- Για να δε#τε ε#κολα την τρ#χουσα κατ#σταση εν#ς λογαριασμο# χρ#στη, χρησιμοποιε#στε την ακ#λουθη σ#νταξη:

```
sudo chage -l username
```

Η #ξοδος παρακ#τω δε#χνει ενδιαφ#ροντα στοιχε#α για το λογαριασμ# χρ#στη, δηλαδ# #τι δεν υπ#ρχουν πολιτικ#ς που εφαρμ#ζονται:

```
#####          : Jan 20, 2008
# #####          : #####
#####          : #####
# #####μ##       : #####
#####μ## μ##### : 0
#####μ## μ##### : 99999
#####μ## μ##### : 7
```

- Για να ορ#σετε οποιαδ#ποτε απ# αυτ#ς τις τιμ#ς, απλ# χρησιμοποιε#στε την ακ#λουθη σ#νταξη, και ακολουθ#στε τις διαδραστικ#ς προτροπ#ς:

```
sudo chage username
```

Το ακ#λουθο ε#ναι επ#σης #να παρ#δειγμα για το πως να αλλ#ξετε χειροκ#νητα την ρητ# ημερομην#α λ#ξης (-E) σε 01/31/2008, την ελ#χιστη ηλικ#α κωδικο# (-m) σε 5 μ#ρες, την μ#γιστη ηλικ#α κωδικο# (-M) σε 90 μ#ρες, την περ#οδο αδρ#νειας (-I) σε 5 μ#ρες μετ# τη λ#ξη του κωδικο#, και μια περ#οδο προειδοπο#ησης (-W) 14 ημερ#ν πριν λ#ξει ο κωδικ#ς.

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

- Για να επαληθε#σετε τις αλλαγ#ς, χρησιμοποιε#στε την #δια σ#νταξη που χρησιμοποιε#θηκε προηγουμ#νως:

```
sudo chage -l username
```

Η #ξοδος παρακ#τω δε#χνει τις ν#ες πολιτικ#ς που #χουν θεσπιστε# για το λογαριασμ#ς:

```
#####          : Jan 20, 2008
# #####          : Apr 19, 2008
#####          : May 19, 2008
# #####μ##       : Jan 31, 2008
#####μ## μ##### : 5
#####μ## μ##### : 90
```

##### #μ#### ##### # ##### : 14

## 1.5. #####

Πολλές εφαρμογές χρησιμοποιούν εναλλακτικούς μηχανισμούς πιστοποίησης οι οποίοι μπορούν εύκολα να παραβλεφθούν ακόμα και απειρους 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. ##### SSH #####

Με το να απενεργοποιήσετε/κλειδώσετε τον λογαριασμό ενός χρήστη δε θα τον αποτρέψετε απ' το να συνδεθεί στο διακομιστή σας εξ αποστάσεως ενώ χειρίζεται στο παρελθόν ένα δημόσιο κλειδί πιστοποίησης RSA. Θα μπορούσε ακόμα να αποκτή πρόσβαση κελφούς στο διακομιστή, χωρίς να χρειάζεται κωδικό. Θυμηθείτε να ελέγξετε το αρχικό κατάλογο του χρήστη για αρχεία που θα επιτρέψουν αυτό του εδούς την πιστοποιημένη SSH πρόσβαση πχ. `/home/username/.ssh/authorized_keys`.

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

Σιγουρευτείτε ότι ελέγξατε για εγκατεστημένες συνδέσεις SSH απ' τον απενεργοποιημένο χρήστη, καθώς είναι πιθανό να έχουν υπαρκτές εισερχόμενες # εξερχόμενες συνδέσεις. Τερματίστε #ποιες βρέψτε.

Περιορίστε την πρόσβαση SSH μ#νο σε λογαριασμούς χρηστών που πρέπει να την #χουν. Για παράδειγμα, μπορείτε να δημιουργήσετε μια ομάδα με #νομα "sshlogin" και να εισ#γετε το #νομα της ομάδας στην τιμή που είναι συναφής με τη μεταβλητή `AllowGroups` που βρ#σκεται στο αρχείο `/etc/ssh/sshd_config`.

```
AllowGroups sshlogin
```

#στερα προσθήστε 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. #####

Τα περισσότερα δίκτυα επιχειρήσεων απαιτούν κεντρικό #λέγχο ταυτότητας και ελέγχους πρόσβασης για #λους τους π#ρους συστήματος. Εάν #χετε διαμορφώσει το διακομιστή σας να πιστοποιεί τους χρήστες απ' εξωτερικές β#σεις δεδομένων, βεβαιωθείτε ότι #χετε απενεργοποιήσει τους λογαριασμούς χρηστών εξωτερική και τοπική, με αυτόν τον τρόπο εξασφαλίζεται ότι η τοπική επαναφορά ταυτοποίησης δεν είναι δυνατή.

## 2. #####

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 εναντίον σε θύματα που θα μπορούσαν να αποφύγουν σοβαρές συνέπειες.

### 2.1. ##### Ctrl+Alt+Delete

Πρώτο και κυριότερο, ο κάθνας που έχει φυσική πρόσβαση στο πληκτρολόγιο μπορεί απλώς να χρησιμοποιήσει τον συνδυασμό κλειδιών **Ctrl+Alt+Delete** για να επανεκκινήσει το διακομιστή χωρίς να χρειαστεί να συνδεθεί. Σίγουρα, κάποιος μπορεί απλώς να αποσυνδέσει την παροχή ρεύματος, αλλά θα πρέπει ακόμα να εμποδίσουμε την χρήση αυτού του συνδυασμού κλειδιών σε έναν διακομιστή παραγωγής. Αυτό αναγκάζει έναν επιτιθέμενο να λάβει πιο δραστικές μέτρα για να επανεκκινήσει το διακομιστή και θα εμποδίσει τυχόν επανεκκινήσεις της διάδρασης.

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

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



### 3. #####

#### 3.1. #####

Ο πυρήνας Linux περιλαμβάνει το υποσύστημα *Netfilter*, το οποίο χρησιμοποιείται για να χειριστείται η μορφή της κίνησης δικτύου που κινείται προς ή από το διακομιστή σας. Άλλες οι μοντρες λήψεις τέτοιους προστασίας Linux χρησιμοποιούν αυτό το σύστημα για φίλτρωση πακέτων.

Το σύστημα φίλτρωσης πακέτων του πυρήνα θα ήταν ελκυστικής χρήσης για τους διαχειριστές χωρίς μια διεπαφή χρήστη για να το διαχειρίζεται. Αυτός είναι ο σκοπός των πινάκων IP. Είναι ένα πακέτο φτάνει στο διακομιστή σας, θα περάσετε στο υποσύστημα *Netfilter* για αποδοχή, χειραγώγηση, ή απρριψη βήση των κανόνων που παραχωρούνται από το χρορήστη μέσω των πινάκων IP. Έτσι, οι πλάκες IP είναι το μέσο που χρειάζεστε για να διαχειριστείτε το τυχόν προστασίας ή να εστέ εξοικειωμένοι με αυτό, αλλά υπάρχουν και πολλές προσψεις διαθέσιμες για να απλοποιήσετε το έργο.

#### 3.2. ufw - #####

Το προεπιλεγμένο εργαλείο διαμόρφωσης του τυχόν προστασίας για το Ubuntu είναι το *ufw*. Αναπτύγνεται για να διευκολύνει τη διαμόρφωση πινάκων IP τυχόν προστασίας, το *ufw* παρχει έναν φιλικό προς το χρήστη τρόπο να δημιουργήσει ένα IPv4 ή IPv6 τυχόν προστασίας βασισμένο σε κεντρικό υπολογιστή

Το *ufw* εξορισμός είναι αρχικά απενεργοποιημένο. Από την κεντρική σελίδα *ufw*:

>C;## *ufw* δεν προορζεται για να παρχει πλήρη λειτουργικότητα του τυχόν προστασίας μέσω της διεπαφής εντολών, αλλά αντθέτα παρχει έναν εύκολο τρόπο να προσθέτετε ή να αφαιρεθεί απλός κανόνες. Προς το παρην χρησιμοποιείται κυρως για τέχη προστασίας βασισμένα σε κεντρικό υπολογιστή.>#201#;

Τα ακόλουθα είναι κάποια παραδεγμάτα για το πως να χρησιμοποιήσετε το *ufw*:

- Πρτον, το *ufw* χρειζεται να ενεργοποιηθεί. Από ένα τερματικό εντολν εισγτε:

```
sudo ufw enable
```

- Για να ανοξτε μια θρα (*ssh* σε αυτό το παρδειγμα):

```
sudo ufw allow 22
```

- Καννές μπορον επσης να προστεθον χρησιμοποιντας τη μορφή *numbered*:

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

- Ομοως, για να κλεσετε μια ανοιχτή θρα:

```
sudo ufw deny 22
```

- Για να αφαιρέσετε έναν κανόνα, χρησιμοποιήστε `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 χεί 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, πληκτρολογήστε:

```
sudo ufw status
```

- Και για περισσότερες πληροφορίες κατ'επιστάσης πληκτρολογείτε:

```
sudo ufw status verbose
```

- Για να δείτε τη μορφή *numbered*:

```
sudo ufw status numbered
```



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

Αυτό είναι μια γρήγορη εισαγωγή για το πώς να χρησιμοποιήσετε το *ufw*. Παρακαλώ αναφερθείτε στη σελίδα *ufw* για περισσότερες πληροφορίες.

### 3.2.1. ##### μ ## μ ## 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
```

- Μοιά με το να επιτρέψετε κίνηση σε μια θύρα, το να χρησιμοποιήσετε ένα προφίλ εφαρμογής γνέται 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 ##### για την εφαρμογή, επειδή αυτό η πληροφορία είναι λεπτομερής στο προφίλ. Επίσης, σημειώστε ότι το όνομα ##### αντικαθιστά το νούμερο της #####.

- Για να δείτε λεπτομέρειες για το ποιες θύρες, πρωτοκόλλα, 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. ##### IP

Ο σκοπός της Μεταμόρφωσης IP είναι να επιτρέπει σε μηχανές με ιδιωτικές, μη δρομολογούμενες διευθύνσεις IP του δικτύου σας να έχουν πρόσβαση στο διαδίκτυο μέσω μιας μηχανής που κάνει τη μεταμόρφωση. Η κίνηση από τα ιδιωτικά σας δίκτυα που προορίζεται για το Διαδίκτυο, πρέπει να χειραγωγηθεί ώστε να είναι οι απαντήσεις δρομολογούμενες μέσω στην μηχανή που κάνει την ατήση. Για να το κάνετε αυτό, ο πυρήνας πρέπει να τροποποιήσει την ##### διεθύνση IP για κάθε πακέτο ώστε οι απαντήσεις να δρομολογούνται μέσω σε αυτό, και όχι στην ιδιωτική διεθύνση IP η οποία έκανε το ατύχημα, κάτι αδύνατο μέσω του Διαδικτύου. Το Linux χρησιμοποιεί #####μ# ##### (conntrack) για να ελέγχει ποιες συνδέσεις ανήκουν σε ποιες μηχανές και να αναδρομολογεί κάθε πακέτο επιστροφής ανήλογα. Η κίνηση που αφήνει το ιδιωτικό σας δίκτυο είναι για αυτό μεταμφιεσμένη σαν να προήλθε από μηχανή που λέγεται Ubuntu. Αυτό η διαδικασία αναφέρεται στις βοηθητικές οδηγίες της Microsoft σαν Διαμοίρασμα Σύνδεσης.

#### 3.3.1. ##### ufw

Η Μεταμόρφωση IP μπορεί να επιτευχθεί χρησιμοποιώντας προσαρμοσμένους κανόνες ufw. Αυτό είναι πιθανό επειδή το τμήμα προγράμματος υποστήριξης για το ufw είναι iptables-restore με τους κανόνες του αρχείου να βρίσκονται στο `/etc/ufw/*.rules`. Αυτό τα αρχεία είναι ένα τέλειο μέρος για να προσθέσετε παλιούς κανόνες πινάκων IP που χρησιμοποιούνται χωρίς ufw, και κανόνες που είναι περισσότερο συναφείς με πολλές δικτύους γέφυρες.

Οι κανόνες χωρίζονται σε δύο διαφορετικές 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 προθήκη πακέτου πρέπει να ενεργοποιηθεί στο ufw. Δοσμένο αρχείο διαμόρφωσης θα πρέπει να προσαρμοστούν, στο `/etc/default/ufw` αλλάξτε το `DEFAULT_FORWARD_POLICY` σε `&#x201C;ACCEPT&#x201D;`:

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

Μετά επεξεργαστείτε το `/etc/ufw/sysctl.conf` αποσχολίστε το:

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

Ομοίως, για την προθήκη IPv6 αποσχολίστε το:

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

- τ#ρα θα προσθ#σουμε καν#νες στο αρχε#ο `/etc/ufw/before.rules`. Οι προεπιλεγμ#νοι καν#νες διαμορφ#νουν μ#νο τον π#νακά `#####`, και για να ενεργοποι#σουμε τη μεταμφ#ση του π#νακά `nat` θα πρ#πει να διαμορφωθε#. Προσθ#στε τα ακ#λουθα στην κορυφ# του αρχε#ου μετ# τα σχ#λια κεφαλ#δας:

```
# ##### nat
*nat
:POSTROUTING ACCEPT [0:0]
```

```
# ##### eth1 μ### eth0.
-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE
```

```
# μ## ##### ## μμ# 'COMMIT' # ##### ## ##### nat ## μ#####
COMMIT
```

Τα σχ#λια δεν ε#ναι αυστηρ#ς αναγκα#, αλλ# θεωρε#ται καλ# #σκηση να καταγρ#φετε τη διαμ#ρφωσ# σας. Επ#σης, #ταν διαμορφ#νετε οποιοδ#ποτε απ# τα αρχε#α `#####` στο `/etc/ufw`, σιγουρευτε#τε #τι αυτ#ς οι γραμμ#ς ε#ναι οι τελευτα#ες γραμμ#ς για κ#θε π#νακά που διαμορφ#νετε.

```
# μ# ##### ## μμ# 'COMMIT' ##### ## ##### ## μ#####
COMMIT
```

Για κ#θε `#####` μια αντ#στοιχη δ#λωση `COMMIT` απαιτε#ται. Σε αυτ# τα παραδε#γματα εμφαν#ζονται οι π#νακες `nat` και `#####`, αλλ# μπορε#τε επ#σης να προσθ#σετε καν#νες για τους π#νακες `raw` και `mangle`.



Στο παραπ#νω παρ#δειγμα αντικαταστ#στε τα `eth0`, `eth1`, και `192.168.0.0/24` με την κατ#λληλη διεπαφ# και εμβ#λεια IP για το δ#κτυ# σας.

- Τ#λος, απενεργοποι#στε και επαναενεργοποι#στε το `ufw` για να ισχ#σουν οι αλλαγ#ς:

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

Η Μεταμφ#ση IP πρ#πει τ#ρα να #χει ενεργοποιηθε#. Μπορε#τε επ#σης να εισ#γετε #ποιους επιπλ#ον καν#νες ΠΡΟΩΘΗΣΗΣ στο `/etc/ufw/before.rules`. Συστ#νεται #τι αυτο# οι επιπρ#σθετοι καν#νες μπορο#ν να προστεθο#ν στην αλυσ#δα `ufw-before-forward`.

### 3.3.2. ##### IP

iptables can also be used to enable Masquerading.

- Ομο#ως με το `ufw`, το πρ#το β#μα ε#ναι να ενεργοποι#σετε την προ#θηση πακ#του IPv4 κ#νοντας επεξεργασ#α στο `/etc/sysctl.conf` και αποσχολι#ζοντας την ακ#λουθη γραμμ#

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

Εν επιθυμείτε να ενεργοποιήσετε την προέγερση IPv6 επείσης αποσχολήστε το:

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

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

```
sudo sysctl -p
```

- Η Μεταμόρφωση IP μπορεί τώρα να επιτευχθεί με έναν απλόν κανόνά IP, ο οποίος μπορεί να διαφείρει λόγο ανλόγα 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 χείρος των ιδιωτικών σας διευθύνσεων είναι 192.168.0.0/16 και ότι η συσκευή αντιμετπίσης Διαδικτύου είναι PPP0. Η σνταξη αναλείται πώς ακολοθως:

- `-t nat` -- ο κανόνας πρέπει να πεί στον πνόνά `nat`
- `-A POSTROUTING` -- ο κανόνας πρέπει να προσαρτηθεί στην αλυσίδα (-A) POSTROUTING
- `-s 192.168.0.0/16` -- ο κανόνας εφαρμζεται στην κνήση που παργεται απ τον προσαρμοσμένο χείρο διευθύνσεων
- `-o ppp0` -- ο κανόνας εφαρμζεται σε κνήση σχεδιασμένη να δρομολογηθεί μέσω της συσκευής δικτύου
- `-j MASQUERADE` -- η κνήση που ταιριζει σε αυτν τον κανόνα πρέπει να μεταπηδσει# (-j) στο στχο MASQUERADE για να χειραγωγηθεί πώς αναφρείται παραπάνω
- Επείσης, κθε αλυσίδα τον πνόνά φίλτρου (ο προεπιλεγμένος πνόνας, και εκε που γνεται το περισσέτερο # #λο το φίλτρρίσμα πακτών) #χει μια προεπιλεγμένη ##### ΑΠΟΔΟΧΗΣ, άλλ# εν δημιουργετε να τεχός προστασας εκτς απ μια μηχαν# πύλνα, #σως #χετε ορσει τις πολιτικς ΡΗΞΗ # ΑΠΟΡΡΙΨΗ, στην οποα περπτωση η μεταμφιεσμένη κνήση πρέπει να επιτρίτετε μέσω της αλυσίδας ΠΡΟΩΘΗΣΗΣ για να δουλψει 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 εντολς θα επιτρίψουν #λες τις συνδσεις απ το τοπικ# σας δκτυο στο Διαδκτυο και #λη την κνήση που σχετζεται με εκενες τις συνδσεις να επιστρίψει στην μηχαν# που τις επτρεψε.

- Εάν θέλετε να ενεργοποιηθεί η μεταμόρφωση κατά την εκκίνηση, κάτι που μάλλον θέλετε, επεξεργαστείτε το `/etc/rc.local` και προσθέστε οποιοδήποτε σχήλο 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. #####

Τα ιστορικά του Τεχνούς Προστασίας είναι σημαντικά για αναγνώριση επιθέσεων, επήλυση προβλημάτων των κανόνων του τεχνούς προστασίας, και για παρατήρηση ασυνήθιστης δραστηριότητας στο δίκτυό σας. Πρέπει να περιλάβετε κανόνες δημιουργίας ιστορικού στο τεχνούς προστασίας για να παραχθούν, όμως, οι κανόνες δημιουργίας ιστορικού πρέπει να ρθουν πριν απ' κάθε εφαρμοσμένο κανόνα τερματισμού (ήνας κανόνας με στόχο που αποφασίζει την τήξη του πακέτου, όπως ΑΠΟΔΟΧΗ, ΡΗΞΗ, ΑΠΟΡΡΙΨΗ).

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

```
sudo ufw logging on
```

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

Εάν χρησιμοποιείτε πλάκες 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=00:00:00:00:00:00:00:00:00:00:00:00:08:00
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. #####

Υπάρχουν πολλή διαθεσίμα εργαλεία για να σας βοηθήσουν να κατασκευάσετε ένα πλήρες τεχνούς προστασίας χωρίς οικεία γνώση πινάκων IP. Για την GUI-κλήση:

- Το *fwbuilder*<sup>1</sup> είναι πολύ ισχυρό και θα φανεί γρήγορο σε έναν διαχειριστή ο οποίος χειρίζεται μια λειτουργία εμπορικού τείχους προστασίας όπως το Checkpoint Firewall-1.

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

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

### 3.6. #####

- The *Ubuntu Firewall*<sup>3</sup> 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*<sup>4</sup> για περισσότερες πληροφορίες για τη χρήση πινάκων IP.
- Το *nat-HOWTO*<sup>5</sup> περιέχει επιπλέον λεπτομέρειες για τη μεταμόρφωση.
- The *IPTables HowTo*<sup>6</sup> in the Ubuntu wiki is a great resource.

---

<sup>1</sup> <http://www.fwbuilder.org/>

<sup>2</sup> <http://www.shorewall.net/>

<sup>3</sup> <https://wiki.ubuntu.com/UncomplicatedFirewall>

<sup>4</sup> <http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html>

<sup>5</sup> <http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO.html>

<sup>6</sup> <https://help.ubuntu.com/community/IptablesHowTo>



## 4. AppArmor

Το AppArmor είναι μια εκτέλεση Υπομονδας Ασφάλειας Linux υποχρεωτικn ελγχνων πρσβαση βασισμνης σε ονματα. Το AppArmor περιορζει μεμονωμνα προγρμματα σε να σνολο απ αριθμημνων αρχεων και προσχδιδων ικανοττων posix 1003.1e

Το AppArmor εγκαθιστται και φορτνεται απ προεπιλογ#. Χρησιμοποιε# μίας εφαρμογς για να διαπιστσει τι αρχεα και διακαιμματα απαιτε# η εφαρμογ#. Μερικ# πακτα θα εγκαταστσουν τα δικ# του προφλ, και επιπρσθετα προφλ μπορο#ν βρεθο#ν στο πακτο apparmor-profiles.

Για να εγκαταστσετε το πακτο apparmor-profiles απ# να τερματικ# εντολ#ν:

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

Τα προφλ του AppArmor #χουν δo καταστσεις εκτλεσης:

- Complaining/Learning: οι παραβσεις προφλ επιτρπονται και καταγρφονται. Χρσιμο για #λεγχο και ανπτυξη νων προφλ.
- Enforced/Confined: ενισχ#ει την πολιτικ# προφλ καθς και την καταγραφ# παραβσεων.

### 4.1. ##### AppArmor

Το πακτο apparmor-utils περιχει λειτουργες γραμμς εντολ#ν τις οποες μπορετε να χρησιμοποιε#τε #στε να αλλ#ξετε την κατσταση εκτλεσης του AppArmor, να βρε#τε την κατσταση ενς προφλ, να δημιουργε#τε να προφλ, κλπ.

- Το apparmor\_status χρησιμοποιε#ται για να προβληθε# η τρ#χουσα κατσταση των προφλ του AppArmor.

```
sudo apparmor_status
```

- Το aa-complain βζει να προφλ σε κατσταση *complain*

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

- Το aa-enforce τοποθετε# να προφλ σε κατσταση *enforce*.

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

- Ο κατλογος `/etc/apparmor.d` ε#ναι εκε# #που βρ#σκονται τα προφλ του AppArmor. Μπορε# να χρησιμοποιηθε# για να χειραγωγηθε# η ##### #λων των προφλ.

Πληκτρολογε#στε τα ακλουθα για να τοποθετ#σετε #λα τα προφλ σε κατσταση complain:

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

Για να τοποθετήσετε #λα τα προφίλ σε κατάσταση `enforce`:

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

- Το `apparmor_parser` χρησιμοποιείται για να φορτίσετε #να προφίλ στον πυρήνα. Μπορείτε επίσης να χρησιμοποιηθείτε για να επαναφορτίσετε #να #δη φορτωμένο προφίλ χρησιμοποιώντας την επιλογή `-r`. Για να φορτίσετε #να προφίλ:

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

Για να επαναφορτίσετε #να 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 ##### #να προφίλ.

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

Για να ##### #να απενεργοποιημένο προφίλ αφαιρέστε τον συμβολικό σήνδεσμο του προφίλ στο `/etc/apparmor.d/disable/`. #στερα φορτίστε 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 υπομονή πυρήνα να αποφορτωθεί πλήρως τα ακόλουθα:

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

- Για να επανεργοποιήσετε το `AppArmor` πληκτρολογήστε:

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



Αντικαταστήστε το `profile.name` με το #νομα του προφίλ το οποίο θέλετε να παραπο#στεί. Επίσης, αντικαταστήστε το `/path/to/bin/` με το πραγματικό μονοπ#τι εκτελ#σιμου αρχέου. Για παρ#δειγμα για την εντολ# `ping` χρησιμοποιήστε το `/bin/ping`

## 4.2. #####

Τα προφίλ του AppArmor είναι απλές αρχές κειμένου που βρίσκονται στο AppArmor. Τα αρχεία παρνούν το νόμο τους από το πλές μονοπτι του εκτελσιμου αντικαθιστντας το "/" με ".". Για παρδειγμα το `/etc/apparmor.d/bin.ping` είναι το προφίλ AppArmor για την εντολή `/bin/ping`.

Υπάρχουν δύο κριρι τποι καννών που χρησιμοποιο#νται στα προφίλ:

- ##### μ#####: που δ#νουν λεπτομ#ρειες για το σε ποια αρχε#α στο σ#στημα αρχε#ων μπορε# να #χει πρ#σβαση μια εφαρμογ#
- ##### #: καθορ#ζουν τι δικαι#ματα επιτρ#πεται να χρησιμοποιε# μια περιορισμ#νη διαδικασ#α.

Σαν παρδειγμα κοιτ#ξετε 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>`: περ#ληψη δηλ#σεων απ# #λλα αρχε#α. Αυτ# επιτρ#πει σε δηλ#σεις που αφορο#ν πολλ#ς εφαρμογ#ς να τοποθετηθο#ν σε #να κοιν# αρχε#ο.
- `/bin/ping flags=(complain)`: μονοπτι στο πρ#γραμμα του προφίλ, επ#σης θ#τει την κατ#σταση σε *complain*.
- `capability net_raw`: επιτρ#πει στην εφαρμογ# πρ#σβαση στο CAP\_NET\_RAW Posix.1e capability.
- `/bin/ping mixr`: επιτρ#πει στην εφαρμογ# πρ#σβαση αν#γνωσης και εκτ#λεσης στο αρχε#ο.



Αφο# επεξεργαστε#τε #να αρχε#ο προφίλ το προφίλ θα πρ#πει να επαναφορτωθε#. Δε#τε το #μ#μ# 4.1, &#x201C;##### AppArmor&#x201D; [171] για λεπτομ#ρειες.

### 4.2.1. ##μ##### #####

- ##### #: Προσπαθ#στε να σκεφτε#τε πως η εφαρμογ# θα πρ#πει να ασκε#τε. Το σχ#διο ελ#γχου θα πρ#πει να διαχωριστε# σε πολλ#ς υποθ#σεις ελ#γχου. Κ#θε υπ#θεση ελ#γχου θα πρ#πει να #χει μια μικρ# περιγραφ# και να καταγρ#φει τα β#ματα που ακολουθο#ν.

Κποιες πρ#τυπες υποθ#σεις ελ#γχου ε#ναι:

- Εκκ#νηση του προγρ#μματος.
- Τερματισμ#ς του προγρ#μματος.
- Επαναφ#ρτωση του προγρ#μματος.
- #λεγχος #λων των εντολ#ν που υποστηρ#ζονται απ# το σεν#ριο `init`.
- ##### #: Χρησιμοποιε#στε το `aa-genprof` για να παρ#γετε #να καινο#ριο προφ#λ. Απ# #να τερματικ#:

**aa-genprof**

Για παρ#δειγμα:

**sudo aa-genprof slapd**

- Για να συμπεριλ#βετε το καινο#ριο σας προφ#λ στο πακ#το `apparmor-profiles`, υποβ#λετε #να σφ#λμα στο *Launchpad* εναντ#ον του πακ#του *AppArmor*<sup>7</sup>:
- Συμπεριλ#βετε το σχ#διο ελ#γχου και τις υποθ#σεις ελ#γχου.
- Επισυν#ψτε το καινο#ριο προφ#λ στο σφ#λμα.

#### 4.2.2. #####

#ταν #να πρ#γραμμα συμπεριφ#ρεται #σημα, μην#ματα ελ#γχου αποστ#λνονται στα αρχε#α ιστορικο#. Το πρ#γραμμα `aa-logprof` μπορε# να χρησιμοποιηθε# για να σαρ#σετε τα αρχε#α ιστορικο# για μην#ματα ελ#γχου *AppArmor*, να τα αναθεωρ#σετε και να ενημερ#σετε τα προφ#λ. Απ# #να τερματικ#:

**sudo aa-logprof**

### 4.3. #####

- Δε#τε το *AppArmor Administration Guide*<sup>8</sup> για προηγμ#νες επιλογ#ς διαμ#ρφωσης.
- Για πληροφορ#ες για το πως να χρησιμοποι#σετε το *AppArmor* με #λλες κυκλοφορ#ες *Ubuntu* δε#τε τη σελ#δα *AppArmor Community Wiki*<sup>9</sup>.
- The *OpenSUSE AppArmor*<sup>10</sup> page is another introduction to *AppArmor*.
- #να τ#λειο μ#ρος για να ζητ#σετε βο#θεια για το *AppArmor*, και να λ#βετε μ#ρος στην κοιν#τητα Διακομιστ# *Ubuntu*, ε#ναι το καν#λι *IRC #ubuntu-server* στο *freenode*<sup>11</sup>.

<sup>7</sup> <https://bugs.launchpad.net/ubuntu/+source/apparmor/+filebug>

<sup>8</sup> [http://www.novell.com/documentation/apparmor/apparmor201\\_sp10\\_admin/index.html?page=/documentation/apparmor/apparmor201\\_sp10\\_admin/data/book\\_apparmor\\_admin.html](http://www.novell.com/documentation/apparmor/apparmor201_sp10_admin/index.html?page=/documentation/apparmor/apparmor201_sp10_admin/data/book_apparmor_admin.html)

<sup>9</sup> <https://help.ubuntu.com/community/AppArmor>

<sup>10</sup> [http://en.opensuse.org/SDB:AppArmor\\_geeks](http://en.opensuse.org/SDB:AppArmor_geeks)

<sup>11</sup> <http://freenode.net>

## 5. #####

Μια απ# τις πιο κοιν#ς μορφ#ς κρυπτογραφ#ας σ#μερα ε#ναι η κρυπτογραφ#α #####-#####. Η κρυπτογραφ#α δημοσ#ου κλειδιο# χρησιμοποιε# #να ##### και #να #####. Το σ#στημα λειτουργε# ##### πληροφορ#ες με τη χρ#ση του δημ#σιου κλειδιο#. Οι πληροφορ#ες μπορο#ν να ##### μ#νο με τη χρ#ση του ιδιωτικο# κλειδιο#.

Μια κοιν# χρ#σης της κρυπτογραφ#ας δημ#σιου κλειδιο# ε#ναι η κρυπτογρ#φηση κ#νησης εφαρμογ#ν χρησιμοποι#ντας σ#νδεση Στρ#ματος Ασφαλο#ς Υποδοχ#α ( Secure Socket Layer (SSL)) # Μεταφορ#ς Στρ#ματος Ασφ#λειας (Transport Layer Security (TLS)). Για παρ#δειγμα, η διαμ#ρφωση του Apache #στε να παρ#χει HTTPS, το πρωτ#κόλλο HTTP π#νω απ# SSL. Αυτ# επιτρ#πει #ναν τρ#πο να κρυπτογραφ#σετε κ#νηση χρησιμοποι#ντας #να πρωτ#κόλλο το οπο#ο δεν παρ#χει κρυπτογρ#φηση απ# μ#νο του.

Το *Certificate* ε#ναι μια μ#θοδος που χρησιμοποιε#ται για να διαν#μει #να ##### και #λλες πληροφορ#ες για #ναν διακομιστ# και τον οργανισμ# ο οπο#ος ε#ναι υπε#θυνος για αυτ#. Τα πιστοποιητικ# μπορε# να ε#ναι ψηφιακ# υπογεγραμμ#να απ# μια ##### # ΑΠ. Η ΑΠ ε#ναι #νας αξι#πιστος τρ#τος που #χει επιβεβαι#σει #τι οι πληροφορ#ες που περι#χονται στο πιστοποιητικ# ε#ναι ακριβε#ς.

### 5.1. #####

Για να στ#σετε #ναν ασφαλ# διακομιστ# χρησιμοποι#ντας κρυπτογρ#φηση δημ#σιου κλειδιο#, στις περισσ#τερες περιπτ#σεις, στ#λνετε το α#τημα πιστοποιητικο# (συμπεριλαμβανομ#νου και του δημ#σιου κλειδιο# σας), απ#δειξη την ταυτ#τητας της εταιρ#ας σας, και πληρωμ# σε μια ΑΠ. Η ΑΠ επαληθε#ει το α#τημα πιστοποιητικο# και την ταυτ#τητ# σας, και μετ# σας στ#λνει #να πιστοποιητικ# για τον ασφαλ# διακομιστ# σας. Εναλλακτικ#, μπορε#τε να δημιουργ#σετε το δικ# σας #####μ### ### ##### πιστοποιητικ#.



Σημει#στε, #τι πιστοποιητικ# υπογεγραμμ#να απ# εσ#ς δε θα πρ#πει να χρησιμοποιο#νται στα περισσ#τερα περιβ#λλοντα παραγωγ#ς.

Συνεχ#ζοντας το παρ#δειγμα HTTPS, #να πιστοποιητικ# υπογεγραμμ#νο απ# ΑΠ παρ#χει δ#ο σημαντικ#ς δυνατ#τητες που #να πιστοποιητικ# υπογεγραμμ#νο απ# εσ#ς δεν παρ#χει:

- Οι φυλλομετρητ#ς (συν#θως) αναγνωρ#ζουν αυτ#ματα το πιστοποιητικ# και επιτρ#πουν μια ασφαλ# σ#νδεση να δημιουργηθε# χωρ#ς να προτρ#ψει το χρ#στη.
- #ταν μια ΑΠ εκδ#δει #να υπογεγραμμ#νο πιστοποιητικ#, εγγυ#ται την ταυτ#τητα του οργανισμο# ο οπο#ος παρ#χει τη σελ#δα ιστο# στο φυλλομετρητ#.

Οι περισσ#τεροι φυλλομετρητ#ς Ιστο#, και υπολογιστ#ς, οι οπο#οι υποστηρ#ζουν SSL #χουν λ#στα ΑΠ των οπο#ων τα πιστοποιητικ# αποδ#χονται αυτ#ματα. Ε#ν #νας φυλλομετρητ#ς αντιμετωπ#σει #να πιστοποιητικ# του οπο#ου η εξουσιοδοτημ#νη ΑΠ δεν ε#ναι στη λ#στα,

ο φύλλομετρητής ζητεί απ' τον χρήστη να δεχθεί # να απορρ#ψει την σ#νδεση. Επ#σης, #λλες εφαρμογ#ς μπορο#ν να παρ#γουν #να μ#νυμα σφ#λματος #ταν χρησιμοποιο#ν #να πιστοποιητικ# υπογεγραμμ#νο απ# εσ#ς.

Η διαδικασ#α του να π#ρετε #να πιστοποιητικ# απ# μια ΑΠ ε#ναι σχετικ# ε#κολο. Μια γρ#γορη επισκ#ψηση ε#ναι #πως ακολο#θως:

1. Δημιουργ#στε #να ζευγ#ρι ιδιωτικ# και δημ#σιου κλειδιο# κρυπτογρ#φησης.
2. Δημιουργ#στε #να α#τημα πιστοποιητικο# βασισμ#νο στο δημ#σιο κλειδ#. Το α#τημα πιστοποιητικο# περι#χει πληροφορ#ες για το διακομιστ# σας και την εταιρ#α που τον στεγ#ζει.
3. Στε#λτε το α#τημα πιστοποιητικο#, μαζ# με αρχε#α που αποδεικν#ουν την ταυτ#τητ# σας, σε μια ΑΠ. Δεν μπορο#με να σας πο#με πια αρχ# πιστοπο#ησης να διαλ#ξετε. Η απ#φασ# σας μπορε# να βασ#ζεται σε παλαι#τερη εμπειρ#α, # σε εμπειρ#ες των φ#λων # συναδ#λφων σας, # αμγ#ς σε οικονομικο#ς παρ#γοντες.

#ταν #χετε αποφασ#σει σε μια ΑΠ, πρ#πει να ακολουθ#σετε τις οδηγ#ες που παρ#χουν για το πως να αποκτ#σετε #να πιστοποιητικ# απ# αυτο#ς.

4. #ταν η ΑΠ #χει βεβαιωθε# #τι ε#στε αυτ#ς που ισχυρ#ζεστε, σας στ#λνουν #να ψηφιακ# πιστοποιητικ#.
5. Εγκαταστ#στε το πιστοποιητικ# σας στον ασφαλ# διακομιστ# σας, και διαμορφ#στε τις κατ#λληλες εφαρμογ#ς για να χρησιμοποι#σετε το πιστοποιητικ#.

## 5.2. ##### μ##### (###)

Ε#τε π#ρετε #να πιστοποιητικ# απ# μια ΑΠ ε#τε παρ#γετε το δικ# σας υπογεγραμμ#νο απ# εσ#ς, το πρ#το β#μα ε#ναι η παραγωγ# κλειδιο#.

Ε#ν το πιστοποιητικ# θα χρησιμοποιηθε# σε δα#μονες υπηρεσι#ν, #πως τα Apache, Postfix, Dovecot, κλπ, #να κλειδ# χωρ#ς κωδικ# φρ#ση ε#ναι συν#θως κατ#λληλο. Η μη χρησιμοπο#ηση κωδικ#ς φρ#σης επιτρ#πει στις υπηρεσ#ες να εκκιν#ν χωρ#ς χειροκ#νητη παρ#μβαση, συν#θως ο προτιμ#μενος τρ#πος να ξεκιν#σει #νας δα#μονας.

Αυτ# η εν#τητα θα καλ#ψει την παραγωγ# κλειδιο# με κωδικ# φρ#ση, και εν#ς χωρ#ς. Το κλειδ# χωρ#ς κωδικ# φρ#ση θα χρησιμοποιηθε# #στερα για την παραγωγ# εν#ς πιστοποιητικο# το οπο#ο μπορε# να χρησιμοποιηθε# σε ποικ#λους δα#μονες υπηρεσι#ν.



Το να εκτελε#τε την ασφαλ# υπηρεσ#α σας χωρ#ς κωδικ# φρ#ση ε#ναι βολικ# επειδ# δεν χρει#ζεται να εισ#γετε την κωδικ# φρ#ση κ#θε φορ# που εκκινε#τε την ασφαλ# υπηρεσ#α σας. Αλλ# δεν ε#ναι ασφαλ#ς και η #κθεση κλειδιο# σημα#νει την #κθεση του διακομιστ# επ#σης.

Για να παρ#γετε #να ##### για το Α#τημα Υπογραφ#ς Πιστοποιητικο# (ΑΥΠ) εκτελ#στε την ακ#λουθη εντολ# απ# #να τερματικ# εντολ#ν:

```
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 εισήγετε την κωδική φράση. Για μεγαλύτερη ασφάλεια, πρέπει να περιχαιτούλχιστον οχτχ χαρακτήρες. Το ελχιστο μγεθος #ταν προσδιορζετε -des3 ε#ναι τ#σσερις χαρακτήρες. Θα πρ#πει να περιλαμβ#νει αριθμο#ς και/σ σημεα στ#ξης και #χι να ε#ναι μια λ#ξη σε #να λεξικ#. Επ#σης θυμηθε#τε #τι η κωδικ# σας φρ#ση ε#ναι ευα#σθητη στα κεφαλαα#αμικρ# γρ#μματα.

Επαναπληκτρολογε#στε την κωδικ# φρ#ση για να την επαληθε#σετε. #ταν την #χετε επαναπληκτρολογ#σει σωστ#, το κλειδ# διακομιστ# παρ#γεται και αποθηκε#εται στο αρχε#ο server.key.

Τώρα δημιουργ#στε το μη ασφαλ#ς κλειδ#, αυτ# χωρ#ς κωδικ# φρ#ση, και ανακατ#ψτε τα ον#ματα κλειδι#ν:

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

```
mv server.key server.key.secure
```

```
mv server.key.insecure server.key
```

Το μη ασφαλ#ς κλειδ# #χει τ#ρα #νομα server.key, και μπορε#τε να χρησιμοποι#σετε αυτ# το αρχε#ο για να παρ#γετε #να ΑΥΠ χωρ#ς κωδικ# φρ#ση.

Για να δημιουργ#σετε #να ΑΥΠ, εκτελ#στε την ακ#λουθη εντολ# σε #να τερματικ# εντολ#ν:

```
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.

Μπορε#τε τ#ρα να υποβ#λετε αυτ# το αρχε#ο ΑΥΠ σε μια ΑΠ για διεργασα. Η ΑΠ θα χρησιμοποι#σει αυτ# ΑΥΠ αρχε#ο κα θα εκδ#σει #να πιστοποιητικ#. Αφ# ετ#ρου, μπορε#τε να δημιουργ#σετε #να πιστοποιητικ# υπογεγραμμ#νο απ# εσ#ς με αυτ# το ΑΥΠ.

### 5.3. ##### μ#####μ#####

Για να δημιουργ#σετε #να πιστοποιητικ# υπογεγραμμ#νο απ# εσ#ς, εκτελ#στε την ακ#λουθη εντολ# σε #να τερματικ# εντολ#ν:

```
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. #####

Μπορείτε να εγκαταστήσετε το αρχείο κλειδί `server.key` και το αρχείο πιστοποιητικό `server.crt`, στο αρχείο πιστοποιητικό που έχει παραχθεί από την ΑΠ, εκτελώντας τις ακόλουθες εντολές σε ένα τερματικό εντολήν:

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

Τώρα απλώς διαμορφώστε τις εφαρμογές, με την ικανότητα χρήσης κρυπτογράφησης δημιουργίας κλειδίου, για να χρησιμοποιούν τα αρχεία ##### και #####. Για παράδειγμα, ο Apache μπορεί να παρήχει HTTPS, το Dovecot μπορεί να παρήχει IMAPS και POP3S, κ.λ.π.

#### 5.5. #####

Εάν οι υπηρεσίες του δικτύου σας απαιτούν παραπάνω από μερικά πιστοποιητικά υπογεγραμμένα από εσάς, σάς αξίζει τον κόπο να στήσετε μια εσωτερική ##### (###). Χρησιμοποιώντας πιστοποιητικά υπογεγραμμένα από τη δική σας ΑΠ, επιτρέπει τις διάφορες υπηρεσίες που χρησιμοποιούν τα πιστοποιητικά να εμπιστευτούνται εύκολα άλλες υπηρεσίες που χρησιμοποιούν πιστοποιητικά που έχουν παραχθεί από την ίδια ΑΠ>

1. Πρώτον, δημιουργήστε τους καταλόγους που θα κρατούν 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 τρ#το αρχε#ο ε#ναι #να αρχε#ο διαμ#ρφωσης της ΑΠ. Παρ#λο που δεν ε#ναι αυστηρ#ς αναγκα#ο, ε#ναι πολ# βολικ# #ταν εκδ#δονται πολλαπλ# πιστοποιητικ#. Επεξεργαστε#τε το /etc/ssl/openssl.cnf, και το [ CA\_default ] αλλ#ξτε τα:

```
dir          = /etc/ssl/          # #####
database     = $dir/CA/index.txt  # #####
certificate   = $dir/certs/cacert.pem # ##
serial       = $dir/CA/serial      # #
private_key   = $dir/private/cakey.pem # ##
```

4. Μετ#, δημιουργ#στε το υπογεγραμμ#νο απ# εσ#ς πιστοποιητικ# β#σης:

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
```

#στερα θα σας ζητηθε# να εισ#γετε λεπτομ#ρειες σχετικ#ς με το πιστοποιητικ#.

5. Τ#ρα εγκαταστ#στε το πιστοποιητικ# και το κλειδ# β#σης:

```
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
```

6. Ε#στε τ#ρα #τοιμοι να αρχ#σετε να υπογρ#φετε πιστοποιητικ#. Το πρ#το αντικε#μενο που χρει#ζεστε ε#ναι #να Α#τημα Υπογραφ#ς Πιστοποιητικο# (ΑΥΠ), δε#τε #μ#μ# 5.2, &#x201C;##### μ##### (###)&#x201D; [176] για λεπτομ#ρειες. #ταν #χετε #να ΑΥΠ, εισ#γετε τα ακ#λουθα για να παρ#γετε #να πιστοποιητικ# υπογεγραμμ#νο απ# την ΑΠ:

```
sudo openssl ca -in server.csr -config /etc/ssl/openssl.cnf
```

Αφο# εισ#γετε τον κωδικ# για το κλειδ# ΑΠ, θα σας ζητηθε# να υπογρ#ψετε το πιστοποιητικ#, και ξαν# να παραδ#σετε το ν#ο πιστοποιητικ#. #στερα θα πρ#πει να δε#τε #να σχετικ# μεγ#λο #γκο εξ#δου σχετικ# με τη δημιουργ#α του πιστοποιητικο#.

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.

Μεταγεν#στερα πιστοποιητικ# θα ονομαστον 02.pem, 03.pem, κλπ.



Αντικαταστ#στε το mail.example.com.crt με το δικ# σας περιγραφικ# #νομα.

8. Τ#λος, αντιγρ#ψτε το καινο#ριο πιστοποιητικ# στον κεντρικ# υπολογιστ# που το χρει#ζεται, και διαμορφ#στε τις κατ#λληλες εφαρμογ#ς για να το χρησιμοποι#σουν. Η εξορισμο# τοποθεσ#α για να εγκαταστ#σετε πιστοποιητικ# ε#ναι η /etc/ssl/certs.

Αυτό επιτρέπει σε πολλαπλές υπηρεσίες να χρησιμοποιούν τα ίδια πιστοποιητικά χωρίς ιδιαίτερα περιπλοκές δεικτών 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. #####

- Για πιο λεπτομερείς οδηγίες για τη χρήση κρυπτογράφησης δείτε το *SSL Certificates HOWTO*<sup>12</sup> από το `tldp.org`
- Η σελίδα της Wikipedia *HTTPS*<sup>13</sup> περιχει περισσότερες πληροφορίες σχετικές με το HTTPS.
- Για περισσότερες πληροφορίες για το *OpenSSL* δείτε την *##### OpenSSL*<sup>14</sup>.
- Επίσης, το *Network Security with OpenSSL*<sup>15</sup> του O'Reilly είναι μια καλή σε βιβλίο αναφοράς.

---

<sup>12</sup> <http://tldp.org/HOWTO/SSL-Certificates-HOWTO/index.html>

<sup>13</sup> <http://en.wikipedia.org/wiki/Https>

<sup>14</sup> <http://www.openssl.org/>

<sup>15</sup> <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 απ' το στρώμα του συστήματος αρχείων το *eCryptfs* προστατεύει αρχεία χωρίς να χειριστεί το υποκείμενο σύστημα αρχείων, ο τσος διαμερισματος, κλπ.

Κατ' τη διάρκεια της εγκατάστασης υπάρχει μια επιλογή να κρυπτογραφηθεί το `/home` διαμερίσμα. Αυτ' θα διαμορφώσει αυτόματα τι χρειάζεται για να κρυπτογραφηθεί και να φορτωθεί το διαμερίσμα.

As an example, this section will cover configuring `/srv` to be encrypted using *eCryptfs*.

### 6.1. ##### eCryptfs.

Πρ'τον, εγκαταστήστε τα απαραίτητα πακέτα. Απ' να τερματικό εντολ'ν πληκτρολογήστε:

```
sudo apt-get install ecryptfs-utils
```

Τ'ρα φορτώστε να διαμερίσμα να κρυπτογραφηθεί:

```
sudo mount -t ecryptfs /srv /srv
```

στερα θα σας ζητηθ'ν κποιες λεπτομρείες για το πως το *ecryptfs* να κρυπτογραφηθεί τα δεδομ'να.

Για να ελ'γξετε αν τα αρχεία που τοποθετήθηκαν στο `/srv` ντως αποκρυπτογραφθηκαν αντιγρψτε το φκελο `/etc/default` στο `/srv`:

```
sudo cp -r /etc/default /srv
```

Τ'ρα, αποφορτώστε το `/srv`, και προσπαθώστε να δε#τε το αρχείο:

```
sudo umount /srv
cat /srv/default/cron
```

Φορτώνοντας ξαν# το `/srv` χρησιμοποιώντας το *ecryptfs* θα κνει τα δεδομ'να να προβληθ'ν ξαν#.

### 6.2. #####μ#####μ#####μ#####μ#####μ#####

Υπάρχουν κποιι τρποι να φορτώνετε αυτόματα να κρυπτογραφημ'νο *ecryptfs* σύστημα αρχείων κατ' την εκκ'νηση. Αυτ' το παρ#δειγμα θα χρησιμοποιήσει να αρχείο `/root/.ecryptfsrc` το οπο# περιχει επιλογ'ς φρτωσης, μαζ# με να αρχείο κωδικ'ς φρσης που βρ#σκεται σε να κλειδ# USB.

Πρ#τον, δημιουργ#στε το `/root/.ecryptfs` που περι#χει:

```
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
```



Προσαρμ#στε το `ecryptfs_sig` στην υπογραφ# στο `/root/.ecryptfs/sig-cache.txt`.

Μετ#, δημιουργ#στε #να αρχε#ο κωδικ#ς φρ#σης `/mnt/usb/passwd_file.txt`:

```
passphrase_passwd=[secrets]
```

Τ#ρα προσθ#στε τις απαρα#τητες γραμμ#ς στο `/etc/fstab`:

```
/dev/sdb1      /mnt/usb      ext3    ro      0 0
/srv /srv encryptfs defaults 0 0
```

Βεβαιωθε#τε #τι ο οδηγ#ς USB ε#ναι φορτωμ#νος πριν απ# το κρυπτογραφημ#νο διαμ#ρισμα.

Finally, reboot and the `/srv` should be mounted using *eCryptfs*.

### 6.3. #####

Το πακ#το `ecryptfs-utils` περιλαμβάνει πολλ#ς #λλες χρ#σιμες λειτουργ#ες:

- *ecryptfs-setup-private*: δημιουργε# #ναν `~/Private` για να περι#χει κρυπτογραφημ#νες πληροφορ#ες. Αυτ# η λειτουργ#α μπορε# να εκτελεστε# απ# χρ#στες χωρ#ς δικαι#ματα για να διατηρηθο#ν τα δεδομ#να ιδιωτικ# απ# #λλους χρ#στες στο σ#στημα.
- *ecryptfs-mount-private* and *ecryptfs-umount-private*: θα φορτ#σει και αποφορτ#σει αντ#στοιχα, #ναν `~/Private` κατ#λογο χρ#στη.
- *ecryptfs-add-passphrase*: προσθ#τει μια καινο#ρια κωδικ# φρ#ση στην κλειδοθ#κη του πυρ#να.
- *ecryptfs-manager*: διαχειρ#ζεται αντικε#μενα *eCryptfs* #πως κλειδι#.
- *ecryptfs-stat*: σας επιτρ#πει να προβ#λετε τις *ecryptfs meta* πληροφορ#ες για #να αρχε#ο.

### 6.4. #####

- For more information on *eCryptfs* see the *Launchpad project page*<sup>16</sup>.
- There is also a *Linux Journal*<sup>17</sup> article covering *eCryptfs*.

<sup>16</sup> <https://launchpad.net/ecryptfs>

<sup>17</sup> <http://www.linuxjournal.com/article/9400>

- Also, for more `ecryptfs` options see the *ecryptfs man page*<sup>18</sup>.
- The *eCryptfs Ubuntu Wiki*<sup>19</sup> page also has more details.

---

<sup>18</sup> <http://manpages.ubuntu.com/manpages/raring/en/man7/ecryptfs.7.html>

<sup>19</sup> <https://help.ubuntu.com/community/eCryptfs>

---

## Κεφάλαιο 10. Παρακολο#θηση

## 1. #####

Η παρακολο#θηση των εξυπηρετητ#ν και υπηρεσι#ν ζωτικ#ς σημασ#ας αποτελε# σημαντικ# συστατικ# της διαχε#ρισης συστημ#των. Οι περισσ#τερες υπηρεσ#ες δικτ#ου παρακολουθο#νται και ελ#γχονται #σον αφορ# την απ#δοση #/ και τη διαθεσιμ#τητ# τους. Αυτ# η εν#τητα θα καλ#ψει την εγκατ#σταση και ρ#θμιση του Nagios για την παρακολο#θηση της διαθεσιμ#τητας και του Munin για την παρακολο#θηση της απ#δοσης.

Στα παραδε#γματα αυτ#ς της εν#τητας θα χρησιμοποιηθο#ν δ#ο εξυπηρετητ#ς με ον#ματα *server01* και *server02*. Στον *Server01* θα γ#νει ρ#θμιση του Nagios για την παρακολο#θηση των υπηρεσι#ν στον #διο και στον *server02*. Στον *Server01* θα εγκατασταθε# και το πακ#το *munin* για τη συλλογ# πληροφορι#ν απ# το δ#κτυο. Χρησιμοποι#ντας το πακ#το *munin-node*, ο *server02* θα ρυθμιστε# #τσι #στε να αποστ#λλει πληροφορ#ες στον *server01*.

Ελπ#ζουμε #τι αυτ# τα απλ# παραδε#γματα θα σας επιτρ#ψουν να παρακολουθε#τε δι#φορους εξυπηρετητ#ς και υπηρεσ#ες στο δ#κτυ# σας.

## 2. Nagios

### 2.1. #####

Καταρχής, εγκαταστήστε το πακέτο `nagios` στον `server01`. Εισήγείτε σε τερματικό:

```
sudo apt-get install nagios3 nagios-nrpe-plugin
```

Θα σας ζητηθεί να εισήγείτε κωδικό για τον χρήστη `nagiosadmin`. Τα στοιχεία του χρήστη αποθηκεύονται στο `/etc/nagios3/htpasswd.users`. Για να αλλάξετε τον κωδικό του `nagiosadmin` για να προσθέσετε νέους χρήστες στα σενάρια Nagios CGI, χρησιμοποιήστε το `htpasswd` απ# το πακέτο `apache2-utils`.

Π.χ., για να αλλάξετε τον κωδικό του χρήστη `nagiosadmin` εισήγείτε:

```
sudo htpasswd /etc/nagios3/htpasswd.users nagiosadmin
```

Για να προσθέσετε χρήστη εισήγείτε:

```
sudo htpasswd /etc/nagios3/htpasswd.users steve
```

Στη συνέχεια, εγκαταστήστε το πακέτο `nagios-nrpe-server` στον `server02`. Απ# τον `server02` εισήγείτε σε τερματικό:

```
sudo apt-get install nagios-nrpe-server
```



Το NRPE σας επιτρέπει να εκτελέσετε τοπικούς ελέγχους σε απομακρυσμένους host. Αυτά μπορείτε να τα κ#νετε και μ#σω #λλων προσθ#των του Nagios # χρησιμοποι#ντας #λλους ελέγχους.

### 2.2. ##### μ#####

Τα αρχεία ρυθμίσεων και ελέγχου του Nagios περι#χονται σε ορισμένους καταλόγους.

- `/etc/nagios3`: περι#χει αρχεία ρυθμίσεων για τη λειτουργία της υπηρεσίας, των αρχέων CGI, των host nagios, κτλ.
- `/etc/nagios-plugins`: περι#χει αρχεία ρυθμίσεων για τους ελέγχους υπηρεσι#ν.
- `/etc/nagios`: περι#χει τα αρχεία ρυθμίσεων του `nagios-nrpe-server` στον απομακρυσμένο host.
- `/usr/lib/nagios/plugins/`: εδ# αποθηκεύονται τα εκτελ#σιμα αρχεία των ελέγχων. Για να ενημερωθείτε για τις επιλογ#ς εν#ς ελέγχου χρησιμοποιήστε την επιλογ# `-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 διαθεσιμότητα στο δίκτυο, το DNS και μια 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 `1, &#x201C;HTTPD - Apache2 #####&#x201D; [194]` για λεπτομέρειες σχετικά με τη ρύθμιση του Apache, το `##### 8, #####&#x201D; (DNS) [141]` για το DNS και το `##### 1, &#x201C;MySQL&#x201D; [216]` για τη MySQL.

Επιπλέον, υπάρχουν κάποιοι ρόλοι των οποίων η κατανάλωση θα πρέπει να διευκολύνει τη ρύθμιση του Nagios:

- **Host:** εξυπηρετητής, σταθμός εργασίας, συσκευή δικτύου, κτλ. που παρακολουθείται.
- **##### host:** μια ομάδα παρεμφερών host. Π.χ. μια ομάδα που θα περιλαμβάνει όλους τους εξυπηρετητές ιστού, τους εξυπηρετητές αρχείων, κτλ.
- **#####:** η παρακολουθούμενη υπηρεσία στον host. Π.χ. HTTP, DNS, NFS, κτλ.
- **#####:** σας επιτρέπει να ομαδοποιείτε πολλαπλές υπηρεσίες. Χρησιμοποιεί π.χ. στην ομαδοποίηση πολλαπλών HTTP.
- **#####:** τομο που λαμβάνει κοινοποίηση ήταν συμβαίνει κάτι. Το Nagios μπορεί να ρυθμιστεί έτσι ώστε να αποστέλλει email, μηνύματα SMS, κτλ.

Απρόεπιλογη το Nagios ελέγχει το HTTP, το χρο στο δίκτυο, το SSH, και τους τρέχοντες χροστές, διεργασίες, και φάσμα του `##### host`. Επίσης, το Nagios εκτελεί έλεγχο ping της `##### (gateway)`.

Η ρύθμιση μεγάλων εγκαταστάσεων Nagios μπορεί να αποβεί αρκετά πολύπλοκη. Συνθώς, είναι καλύτερο να ξεκινάτε με έναν δίο υπολογιστή, να τους ρυθμίζετε πώς επιθυμείτε, και στη συνέχεια να επεκτενεστε περαιτέρω.

## 2.3. #####

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. Επανεκκιν#στε την υπηρεσι#α *nagios* για να ενεργοποι#σετε τις ν#ες ρυθμ#σεις:

```
sudo service nagios3 restart
```

- 1. Τ#ρα, προσθ#στε #ναν ορισμ# υπηρεσι#ας για τον #λεγχο MySQL, προσθ#τοντας τα ακ#λουθα 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 #λεγχος του *Nagios* θα πρ#πει να πιστοποιηθε# στην MySQL. Για να προσθ#σετε #ναν χρ#στη *nagios* στην MySQL εισ#γετε:

```
mysql -u root -p -e "create user nagios identified by 'secret';"
```



Ο χρ#στης *nagios* θα προστεθε# σε #λους τους host της ομ#δας *mysql-servers*.

4. Επανεκκιν#στε το *nagios* για να αρχ#σετε να ελ#γχετε τους εξυπηρετητ#ς MySQL.

```
sudo service nagios3 restart
```

- 1. Τ#λος, ρυθμ#στε το NRPE #τσι #στε να ελ#γχει το χ#ρο στο δ#σκο του *server02*.

Στον *server01* προσθ#στε τον #λεγχο υπηρεσ#ας 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_larg!check_all_disks!172.18.100.101
}
```

- 2. Τ#ρα, στον *server02*, τροποποι#στε το `/etc/nagios/nrpe.cfg` κ#νοντας τις παρακ#τω αλλαγ#ς:

```
allowed_hosts=172.18.100.100
```

Και απ# κ#τω, στην περιοχ# ορισμ#ν εντολ#ν, προσθ#στε:

```
command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -e
```

- 3. Τ#λος, επανεκκιν#στε το `nagios-nrpe-server`:

```
sudo service nagios-nrpe-server restart
```

- 4. Επ#σης, στον *server01*, επανεκκιν#στε το `nagios`:

```
sudo service nagios3 restart
```

Τ#ρα θα πρ#πει να μπορε#τε να βλ#πετε τους ελ#γχους *host* και υπηρεσι#ν στα αρχε#α Nagios CGI. Για να αποκτ#σετε πρ#σβαση, πηγα#νετε στη σελ#δα <http://server01/nagios3> απ# τον περιηγητ# σας. Θα σας ζητηθε# το #νομα και ο κωδικ#ς χρ#στη του *nagiosadmin*.

## 2.4. #####

Αυτ# η εντ#τητα δεν #γγιξε παρ# μ#νο επιφανειακ# τα δι#φορα χαρακτηριστικ# του Nagios. Τα πακ#τα `nagios-plugins-extra` και `nagios-snmp-plugins` περι#χουν πολλο#ς περισσ#τερους ελ#γχους υπηρεσι#ν.

- Για περισσ#τερες πληροφορ#ες ανατρ#ξτε στον ιστ#τοπο του *Nagios*<sup>1</sup>.
- Και συγκεκριμ#να, στον ιστ#τοπο *Online #####*<sup>2</sup>.
- Επ#σης, υπ#ρχει #νας κατ#λογος με #####<sup>3</sup> για το Nagios και την παρακολο#θηση δικτ#ου:

<sup>1</sup> <http://www.nagios.org/>

<sup>2</sup> [http://nagios.sourceforge.net/docs/3\\_0/](http://nagios.sourceforge.net/docs/3_0/)

<sup>3</sup> <http://www.nagios.org/propaganda/books/>

- The *Nagios Ubuntu Wiki*<sup>4</sup> page also has more details.

---

<sup>4</sup> <https://help.ubuntu.com/community/Nagios>

## 3. Munin

### 3.1. #####

Πριν εγκαταστ#σετε το Munin στον *server01*, θα πρ#πει να εγκαταστ#σετε το *apache2*. Οι προεπιλεγμ#νες ρυθμ#σεις επαρκο#ν για τη λειτουργη#α εν#ς εξυπηρετητ# *munin*. Για περισσ#τερες πληροφορ#ες δε#τε το *#μ#μ# 1, &#x201C;HTTPD - Apache2 #####μ#####&#x201D; [194]*.

Καταρχ#ς, εγκαταστ#στε το πακ#το *munin* στον *server01*. Εισ#γετε σε τερματικ#:

```
sudo apt-get install munin
```

Τ#ρα, στον *server02* εγκαταστ#στε το πακ#το *munin-node*:

```
sudo apt-get install munin-node
```

### 3.2. #####

Στον *server01* τροποποι#στε το */etc/munin/munin.conf*, προσθ#τοντας τη διε#θυνση IP του *server02*:

```
## First our "normal" host.
[server02]
    address 172.18.100.101
```



Αντικαταστ#στε τα *server02* και *172.18.100.101* με το #νομα και τη διε#θυνση IP του δικο# σας εξυπηρετητ#.

Στη συν#χεια, ρυθμ#στε το *munin-node* στον *server02*. Τροποποι#στε το */etc/munin/munin-node.conf* για να επιτρ#ψετε την πρ#σβαση του *server01*:

```
allow ^172\.18\.100\.100$
```



Αντικαταστ#στε το *^172\.18\.100\.100\$* με τη διε#θυνση IP του δικο# σας εξυπηρετητ# *munin*.

Τ#ρα, επανεκκιν#στε το *munin-node* στον *server02* για να ενεργοποι#σετε τις αλλαγ#ς:

```
sudo service munin-node restart
```

Τ#λος, απ# τον περιηγητ# σας πηγα#νετε στο *http://server01/munin*. Θα πρ#πει να μπορε#τε να δε#τε συνδ#σμους προς κομψ# γραφ#ματα με πληροφορ#ες των βασικ#ν ##### ## *munin* για το δ#σκο, το δ#κτυο, τις διεργασ#ες και το σ#στημα.



Εφ#σον πρ#κειται για ν#α εγκατ#σταση, #σως χρειαστε# λ#γος χρ#νος μ#χρι να εμφανιστο#ν κ#ποιες χρ#σιμες πληροφορ#ες στα γραφ#ματα.

### 3.3. #####

Το πακ#το `munin-plugins-extra` περιλαμβ#νει ελ#γχους απ#δοσης για επιπλ#ον υπηρεσ#ες. Π.χ., DNS, DHCP, Samba, κτλ. Για να εγκαταστ#σετε το πακ#το, εισ#γετε απ# το τερματικ#:

```
sudo apt-get install munin-plugins-extra
```

Θυμηθε#τε να εγκαταστ#σετε το πακ#το τ#σο στον εξυπηρετητ# #σο και στα κομβικ# μηχαν#ματα (node).

### 3.4. #####

- Δε#τε τον ιστ#τοπο του *Munin*<sup>5</sup> για περισσ#τερες λεπτομ#ρειες.
- Συγκεκριμ#να, η σελ#δα με την *##### Munin*<sup>6</sup> περιλαμβ#νει πληροφορ#ες σχετικ# με επιπλ#ον πρ#σθετα, τη συγγραφ# προσθ#των, κτλ.
- Επ#σης, κυκλοφορε# #να βιβλ#ο της Open Source Press στα Γερμανικ#: *Munin Graphisches Netzwerk- und System-Monitoring*<sup>7</sup>.
- Another resource is the *Munin Ubuntu Wiki*<sup>8</sup> page.

<sup>5</sup> <http://munin.projects.linpro.no/>

<sup>6</sup> <http://munin.projects.linpro.no/wiki/Documentation>

<sup>7</sup> [https://www.opensourcepress.de/index.php?26&backPID=178&tt\\_products=152](https://www.opensourcepress.de/index.php?26&backPID=178&tt_products=152)

<sup>8</sup> <https://help.ubuntu.com/community/Munin>

---

## Κεφάλαιο 11. Διακομιστές Ιστο

Ένας Διακομιστής Ιστο είναι το λογισμικό που είναι υπεύθυνο για την αποδοχή αιτημάτων HTTP από πελάτες, γνωστό και ως φυλλομετρητής Ιστο, και να στέλνουν απαντήσεις HTTP μαζί με προαιρετικό περιεχόμενο δεδομένων, τα οποία συνήθως είναι Ιστοσελίδες όπως αρχεία HTML και συνδεδεμένα αντικείμενα (εικόνες, κλπ.).

## 1. HTTPD - Apache2 #####μ#####

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*<sup>1</sup> a user will enter only the FQDN:

`www.ubuntu.com`

To view the *community*<sup>2</sup> 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 πηγαίνουν από το Στρώμα Ασφαλών Υποδοχών (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 σενάρου Προεπεξεργαστή Υπερκειμένου (PHP), και άλλες δημοφιλείς γλώσσες σενάρου όπως οι Python και Perl. Αυτή η σύνθεση ονομάζεται LAMP (Linux, Apache, MySQL and Perl/Python/PHP) και σχηματίζει μια ισχυρή και αυτοδυναμική πλατφόρμα για την ανάπτυξη εφαρμογών βασισμένων στον Ιστό.

### 1.1. #####

Ο διακομιστής ιστού Apache2 είναι διαθέσιμος για Ubuntu Linux. Για να εγκαταστήσετε τον Apache2:

- Σε ένα τερματικό εντολές πληκτρολογήστε την ακόλουθη εντολή:

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

### 1.2. #####μ#####

Ο Apache2 ρυθμίζετε τοποθετώντας ##### σε απλά αρχεία κειμένου διαμόρφωσης. Αυτές οι ##### χωρίζονται μεταξύ των ακόλουθων φακέλων και καταλόγων:

- *apache2.conf*: το κύριο αρχείο διαμόρφωσης. Περιέχει ρυθμίσεις οι οποίες είναι ##### για το Apache2.

---

<sup>1</sup> <http://www.ubuntu.com>

<sup>2</sup> <http://www.ubuntu.com/community>



- *conf.d*: περιέχει αρχεία διαμόρφωσης τα οποία εφαρμόζονται ##### στο Apache2. #λλά πακέτα που χρησιμοποιούν τον Apache2 για να εξυπηρετούν περιεχόμενο μπορεί να προσθέσουν αρχεία, # συνδύσους, σε αυτόν τον κατάλογο.
- *envvars*: αρχείο στο οποίο ορίζονται η μεταβλητές ##### 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 φορτίνει ##### και να τις τροποποιεί. Δεν θα έχουν #λες οι επιλογές συγκεκριμένα αρχεία διαμόρφωσης, #μως.
- *mods-enabled*: κρατεί ##### στα αρχεία του /etc/apache2/mods-available. #ταν #να αρχείο διαμόρφωσης επιλογής συνδέεται θα ενεργοποιηθεί την επόμενη φορά που θα επανεκκινηθεί ο apache2.
- *ports.conf*: στεγάζει τις οδηγίες που προσδιορίζουν ποιες θ#ρες ακούει ο Apache2.
- *sites-available*: αυτός ο κατάλογος #χει αρχεία διαμόρφωσης για τους Εικονικούς Κ#μβους του Apache2. Οι Εικονικοί Κ#μβοί επιτ#πουν στον Apache2 να διαμορφώνεται για πολλαπλούς δικτυακούς τ#πους που #χουν διαφορετικές ρυθμίσεις.
- *sites-enabled*: #πως το mods-enabled, το sites-enabled περιέχει συνδύσους στον κατάλογο /etc/apache2/sites-available. #μοια, #ταν #να αρχείο διαμόρφωσης στο sites-available συνδέεται, ο δικτυακός τ#πος που ρυθμίζετε απ# αυτό θα ενεργοποιηθεί #ταν ο Apache2 επανεκκινηθεί.

Επιπλέον, #λλά αρχεία διαμόρφωσης μπορεί να προστεθούν χρησιμοποιώντας τον κ#δικά παραπομπής *Include*, και μπάλαντ#ρ μπορεί να χρησιμοποιηθούν για να προστεθούν πολλ# αρχεία διαμόρφωσης. Οποιοσδήποτε κ#δικός παραπομπής μπορεί να χρησιμοποιηθεί σε οποιοδήποτε απ# αυτό τα αρχεία διαμόρφωσης. Οι αλλαγές στο κ#ριο αρχείο διαμόρφωσης αναγνωρίζονται απ# τον Apache2 #ταν ενεργοποιείται # επανεκκιν#τε.

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. #####

Αυτό η ενότητα εξηγεί τις ουσίες παραμέτρους ρ#θμισης του διακομιστή Apache2.

Αναφερθείτε στο *Apache2 Documentation*<sup>3</sup> για περισσότερες λεπτομ#ρείες.

- Ο Apache2 αποστ#λλεται με μ#α προεπιλεγμένη εικονική φιλική προς τον υπολογιστή ρ#θμιση. #χει ρυθμιστεί με #να προεπιλεγμένο εικονικό κεντρικό υπολογιστή (χρησιμοποιώντας τον κ#δικά παραπομπής *VirtualHost*) ο οποίος μπορεί να τροποποιηθεί # να χρησιμοποιηθεί #πως ε#ναι ε#ν #χετε #να μ#νο δικτυακό τ#πο, # να χρησιμοποιηθεί

<sup>3</sup> <http://httpd.apache.org/docs/2.2/>

ως πρότυπο για επιπλέον εικονικούς κεντρικούς υπολογιστές εάν έχετε πολλαπλούς δικτυακούς τήπους. Εάν αφεθεί μόνος, ο προεπιλεγμένος κεντρικός υπολογιστής θα λειτουργήσει ως ο προεπιλεγμένος δικτυακός τήπος σας, # ο δικτυακός τήπος που θα βλ#πουν οι χρήστες εάν το URL που εισ#γουν δεν ταιρι#ζει με τον κ#δικά παραπομπ#ς *ServerName* κανεν#ς απ# τους δικτυακούς σας τήπους. Για να τροποποι#σετε τον προεπιλεγμ#νο εικονικ# κεντρικ# υπολογιστ#, επεξεργαστε#τε το αρχε#ο `/etc/apache2/sites-available/default`.



Οι κ#δικές παραπομπ#ς που ορ#ζονται για #ναν εικονικ# κεντρικ# υπολογιστ# απευθ#νονται μ#νο στον συγκεκριμ#νο εικονικ# κεντρικ# υπολογιστ#. Εάν #νας κ#δικας παραπομπ#ς #χει οριστε# ως *server-wide* και δεν #χει οριστε# στα πλα#σια των ρυθμ#σεων του εικονικο# κεντρικο# υπολογιστ#, χρησιμοποιε#τε η προεπιλεγμ#νη ρ#θμιση. Για παρ#δειγμα, μπορε#τε να ορ#σετε μια διε#θυνση ηλεκτρονικο# ταχυδρομε#ου *Webmaster* και να μην ορ#σετε ατομικ#ς διευθ#νσεις για κ#θε εικονικ# κεντρικ# υπολογιστ#.

Εάν επιθυμ#τε να ρυθμ#σετε #ναν καινο#ριο εικονικ# κεντρικ# υπολογιστ# # δικτυακ# τήπο, αντιγρ#ψτε αυτ# το αρχε#ο στον #διο κατ#λ#γο με #νομα που θα επιλ#ξετε. Για παρ#δειγμα:

```
sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/mynewsite
```

Επεξεργαστε#τε το καινο#ριο αρχε#ο για να ρυθμ#σετε τον καινο#ριο δικτυακ# τήπο χρησιμοποι#ντας κ#ποιους απ# τους κ#δικές παραπομπ#ς που περιγρ#φονται παρακ#τω.

- Ο κ#δικας παραπομπ#ς *ServerAdmin* προσδιορ#ζει τη διε#θυνση ηλεκτρονικο# ταχυδρομε#ου του διαχειριστ# του διακομιστ#. Η προεπιλεγμ#νη τιμ# ε#ναι `webmaster@localhost`. Αυτ# θα πρ#πει να αλλαχτε# σε μια ηλεκτρονικ# διε#θυνση ταχυδρομε#ου που θα παραδοθε# σε εσ#ς (ε#ν ε#στε ο διαχειριστ#ς του διακομιστ#). Εάν η ιστοσελ#δα σας #χει πρ#βλημα, ο *Apache2* θα εμφαν#σει #να μ#νυμα σφ#λματος το οπο#ο θα περιλαμβ#νει τη συγκεκριμ#νη διε#θυνση στην οπο#α θα αναφ#ρετε το πρ#βλημα. Βρε#τε το συγκεκριμ#νο κ#δικά παραπομπ#ς στο αρχε#ο ρ#θμισης της ιστοσελ#δας σας στο `/etc/apache2/sites-available`.
- Ο κ#δικας παραπομπ#ς *Listen* ορ#ζει τη θ#ρα, και προαιρετικ# τη διε#θυνση IP, που θα πρ#πει να ακο#ει ο *Apache2*. Εάν η διε#θυνση IP δεν #χει οριστε#, ο *Apache2* θα ακο#ει #λες τις IP διευθ#νσεις που #χουν εκχωρηθε# στη μηχαν# στην οπο#α τρ#χει. Η προεπιλεγμ#νη τιμ# για τον κ#δικά παραπομπ#ς *Listen* ε#ναι <sup>80</sup>. Αλλ#ζτε το σε `127.0.0.1:80` #στε ο *Apache2* να ακο#ει μ#νο τη διεπαφ# *loopback* #στε να μην ε#ναι διαθ#σιμος το Διαδ#κτυο, στο (για παρ#δειγμα) <sup>81</sup> για να μην αλλ#ζει τη θ#ρα την οπο#α ακο#ει, # να την αφ#σει #πως ε#ναι για κανονικ# λειτουργ#α. Αυτ#ς ο κ#δικας παραπομπ#ς μπορε# να βρεθε# και να αλλαχτε# στο δικ# του αρχε#ου, `/etc/apache2/ports.conf`
- Ο κ#δικας παραπομπ#ς *ServerName* ε#ναι προαιρετικ#ς και ορ#ζει σε τι FQDN θα απαντ#ει η ιστοσελ#δα σας. Ο προεπιλεγμ#νος εικονικ#ς κεντρικ#ς υπολογιστ#ς δεν #χει

κάποιον `ServerName` κδικά παραπομπής ορισμένο, #τσι θα ανταποκριθε# σε #λες τις αιτήσεις που δεν ταιριάζουν με κάποιο κδικά παραπομπής `ServerName` #λλου εικονικού κεντρικού υπολογιστή. Εάν #χετε μ#λεις αποκτ#σει το #νομα τομ#α `ubunturocks.com` και επιθυμείτε να το φιλοξεν#σετε στον διακομιστή `Ubuntu` σας, η τιμ# του κδικά παραπομπής `ServerName` στο αρχείο ρ#θμίσης του εικονικού κεντρικού υπολογιστή πρ#πει να είναι `ubunturocks.com`. Προσθ#στε αυτ#ν τον κδικά παραπομπής στο καινούριο αρχείο εικονικού κεντρικού υπολογιστή που δημιουργ#σατε προηγουμένως (`/etc/apache2/sites-available/mynewsite`).

Μπορε# επ#σης να θ#λετε ο δικτυακ#ς σας τ#πος να ανταποκρ#νεται στο `www.ubunturocks.com`, καθ#ς πολλο# χρ#στες θα θεωρ#σουν #τι το πρ#θεμα `www` είναι απαραίτητο. Χρησιμοποιε#στε τον κδικά παραπομπής `ServerAlias` για αυτ#. Μπορε#τε επ#σης να χρησιμοποι#σετε μπαλαντ#ρ στον κδικά παραπομπής `ServerAlias`.

Για παρ#δειγμα, η ακ#λουθη ρ#θμίση θα προκαλ#σει τον δικτυακ# σας τ#πο να ανταποκρ#νεται σε κ#θε α#τημα τομ#α που τελεινει 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!

Ενεργοποι#στε το *VirtualHost* χρησιμοποι#ντας τη λειτουργη# `a2ensite` και επανεκκιν#στε τον Apache2:

```
sudo a2ensite mynewsite
sudo service apache2 restart
```



Φροντ#στε να αντικαταστ#σετε το `mynewsite` με #να πιο περιγραφικ# #νομα για τον Εικονικ# Κεντρικ# Υπολογιστή. Μια μ#θοδος είναι να το ονομ#σετε το αρχείο π#ως ο κδικάς παραπομπής `ServerName` του Εικονικού Κεντρικού Υπολογιστή.

Ομο#ως, χρησιμοποι#στε τη λειτουργη# `a2dissite` για να απενεργοποι#σετε δικτυακ#ς τ#πους. Αυτ# μπορε# να είναι χρ#σιμο #ταν λ#νετε προβλ#ματα ρ#θμίσης με πολλ#ς Εικονικ#ς Κεντρικ#ς Υπολογιστ#ς:

```
sudo a2dissite mynewsite
sudo service apache2 restart
```

### 1.2.2. ##### μ#####

Αυτ# η εν#τητα εξηγ# τη ρ#θμίση των αρχικ#ν ρυθμ#σεων του Apache2. Για παρ#δειγμα, εάν προσθ#σετε #ναν εικονικ# κεντρικ# υπολογιστή, οι ρυθμ#σεις που επεξεργ#ζεστε για

τον εικονικό κεντρικό υπολογιστή υπερισχούν για εκείνο τον εικονικό υπολογιστή. Για να κδικά παραπομπές 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 ζητεί το ευρετήριο ενός καταλόγου προσδιορίζοντας μια κθετο (/) στο τέλος του ονόματος του καταλόγου.

Για παράδειγμα, όταν ένας χρήστης ζητεί τη σελίδα [http://www.example.com/this\\_directory/](http://www.example.com/this_directory/), αυτός 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 δειά Απορρ#φθηκε εάν τποτα από τα δύο δεν αληθεύει. Ο διακομιστής θα προσπαθήσει να βρει ένα από τα αρχεία που βρίσκονται στη λίστα του κδικά 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 παρήγει 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"`. #τσι, 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 από κατάλογο αντί από διακομιστή. Ο *Options* είναι ένας από εκείνους τους κδικές παραπομπές. Μια στροφή καταλόγου περιλαμβάνεται σε ετικέτες στυλ XML, #πως:

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

Ο κδικάς παραπομπής *Options* μέσα σε μια στροφή Καταλόγου δ#χεται μέσα # περισσότερες από τις ακόλουθες τιμές (μεταξύ #λλων), χωρισμένες από κεν#:

- **ExecCGI** - Επιτρέπει εκτέλεση σεναρίων CGI. Τα σενάρια CGI δεν εκτελούνται εάν αυτό 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 ξεχωριστό από και έξω από το `DocumentRoot`, και μόνο σε αυτόν τον κατάλογο πρέπει να οριστεί η επιλογή `ExecCGI`. Αυτό είναι η προεπιλογή, και η προεπιλεγμένη τοποθέτηση 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)*<sup>4</sup> for more information.
- **IncludesNOEXEC** - Επιτρέπει περιλήψεις διακομιστή, αλλά απενεργοποιεί τις εντολές `#exec` και `#include` σε σενάρια CGI.
- **Indexes** - Προβλέπει 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 αυτό την επιλογή προσεκτικά αν κατάλογο μόνο εάν έχετε σίγουροι ότι θέλετε οι χρήστες να βλέπουν όλα τα περιεχόμενα του καταλόγου.

- **Multiview** - Υποστηρίζει πολλαπλές προβολές διαπραγματεύσιμου περιεχομένου, αυτό η επιλογή είναι απενεργοποιημένη από προεπιλογή για λόγους ασφαλείας. Δείτε το *Apache2 documentation on this option*<sup>5</sup>.
- **SymLinksIfOwnerMatch** - Ακολουθείστε μόνο συμβολικούς συνδέσμους εάν το αρχείο # ο κατάλογος στόχος έχει τον ίδιο ιδιοκτήτη με το σύνδεσμο.

### 1.2.3. ##### httpd

Αυτό η ενότητα εξηγεί κάποιες βασικές ρυθμίσεις διαμόρφωσης του δαμονά `httpd`.

**LockFile** - Ο κδικας παραπομπής `LockFile` ορίζει το μονοπάτι του `lockfile`

που χρησιμοποιείται όταν ο διακομιστής καταρτίζεται είτε με το `USE_FCNTL_SERIALIZED_ACCEPT` με το `USE_FLOCK_SERIALIZED_AC`. Πρέπει να είναι αποθηκευμένο στον τοπικό δίσκο. Πρέπει να μενεί στις προεπιλεγμένες τιμές εκτός εάν ο κατάλογος του ιστορικού βρσκεται σε ένα διαμοιρασμένο `NFS`. Σε αυτό την περίπτωση, η προεπιλεγμένη τιμή πρέπει να αλλάξει σε μια τοποθέτηση του τοπικού δίσκου και σε έναν κατάλογο που είναι αναγνώσιμος μόνο από τη βση.

**PidFile** - Ο κδικας παραπομπής `PidFile` ορίζει το αρχείο στο οποίο ο διακομιστής καταγράφει την πρδο `ID (pid)`. Αυτό το αρχείο θα πρέπει να είναι αναγνώσιμο από τη βση. Στις περισσότερες περιπτώσεις, θα πρέπει να αφεθεί στις αρχικές τιμές.

<sup>4</sup> <https://help.ubuntu.com/community/ServerSideIncludes>

<sup>5</sup> [http://httpd.apache.org/docs/2.2/mod/mod\\_negotiation.html#multiviews](http://httpd.apache.org/docs/2.2/mod/mod_negotiation.html#multiviews)

**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 κωδικά παραπομπής User στη βήση. Χρησιμοποιώντας τη βήση ως User θα δημιουργήσει μεγάλες τρέπες 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. ##### Apache2

Ο Apache2 είναι ένας σπονδυλωτός διακομιστής. Αυτός σημαίνει ότι μόνο η πιο βασική λειτουργικότητα περιλαμβάνεται στον πυρήνα του διακομιστή. Επιπρόσθετα χαρακτηριστικά είναι διαθέσιμα μέσω υπομονών οι οποίες μπορούν να φορτωθούν στον Apache2. Από προεπιλογή, ένα βασικό σύνολο υπομονών περιλαμβάνεται στο διακομιστή κατά την σύνταξη. Εάν ο διακομιστής έχει συνταχθεί ώστε να χρησιμοποιεί υπομονές φορτωμένες δυναμικά, τότε οι υπομονές μπορούν να συνταχθούν ξεχωριστά, και να προστεθούν οποιαδήποτε στιγμή χρησιμοποιώντας τον κωδικά παραπομπής LoadModule. Αλλιώς, ο Apache2 πρέπει να ανασυνταχθεί ώστε να προσθθεί να αφαιρεθεί υπομονές.

Το Ubuntu συντρέπει τον Apache2 ώστε να επιτρέπει τη δυναμική φόρτωση υπομονών. Οι κωδικές παραπομπές διαμόρφωσης μπορούν να περιληφθούν υπέρ ή κάτω την παρουσία μιας συγκεκριμένης υπομονής περικλειόντες τους σε ένα μπλοκ *<IfModule>*.

Μπορείτε να εγκαταστήσετε επιπρόσθετες υπομονές του Apache2 και να τις χρησιμοποιήσετε με τον διακομιστή Ιστού σας. Για παράδειγμα, τρέξτε την ακόλουθη εντολή απευθείας τερματικό εντολή για να εγκαταστήσετε την υπομονή MySQL Authentication:

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

Δείτε τον κατάλογο `/etc/apache2/mods-available` για επιπλέον υπομονές.

Χρησιμοποιήστε τη λειτουργία `a2enmod` για να ενεργοποιήσετε μια υπομονή:

```
a2enmod
sudo service apache2 restart
```

Ομοίως, `a2dismod` θα απενεργοποιήσει μια υπομονή:

```
sudo a2dismod auth_mysql
sudo service apache2 restart
```

### 1.3. ##### HTTPS

Η υπομονδα `mod_ssl` προσθ#τει #να σημαντικ# χαρακτηριστικ# στο διακομιστ# Apache2 - την ικαν#τητα να κρυπτογραφε# επικοινων#ες. #τσι, #ταν ο φυλλομετρητ#ς σας επικοινωνε# χρησιμοποι#ντας SSL, το πρ#θεμα `https://` χρησιμοποιε#ται στην αρχ# του URL στην μπ#ρα πλο#γησης του φυλλομετρητ#.

Η υπομονδα `mod_ssl` ε#ναι διαθ#σιμη στο πακ#το `apache2-common`. Εκτελ#στε την ακ#λουθη εντολ# απ# #να τερματικ# εντολ#ν για να ενεργοποι#σετε την υπομονδα `mod_ssl`:

```
sudo a2enmod ssl
```

Υπ#ρχει #να προεπιλεγμ#νο αρχε#ο διαμ#ρφωσης HTTPS στο `/etc/apache2/sites-available/default-ssl`. Για να παρ#χει ο Apache2 HTTPS, χρει#ζονται επ#σης #να ##### και #να αρχε#ο #####. Η προεπιλεγμ#νη διαμ#ρφωση HTTPS θα χρησιμοποι#σει #να πιστοποιητικ# και #να κλειδ# που θα παραχθo#ν απ# το πακ#το `ssl-cert`. Ε#ναι καλ# για δοκιμ#, αλλ# το πιστοποιητικ# και το κλειδ# που παρ#χθηκαν αυτ#ματα πρ#πει να αντικατασταθo#ν απ# #να πιστοποιητικ# συγκεκριμ#νο για τον δικτυακ# τ#πο # το διακομιστ#. Για πληροφοριες στο πως να παρ#γετε #να κλειδ# και να αποκτ#σετε #να πιστοποιητικ# δ#τε #μ#μ# 5, &#x201C;#####&#x201D; [175]

Για να διαμορφ#σετε τον Apache2 για HTTPS, πληκτρολογ#στε το ακ#λουθο:

```
sudo a2ensite default-ssl
```



Οι κατ#λογοι `/etc/ssl/certs` και `/etc/ssl/private` ε#ναι οι προεπιλεγμ#νες τοποθεσιες. Ε#ν εγκαταστ#σετε το πιστοποιητικ# και το κλειδ# σε #λλο κατ#λογο βεβαιωθε#τε να αλλ#ξετε τα `SSLCertificateFile` και `SSLCertificateKeyFile` κατ#λληλα.

Με τον Apache2 τ#ρα διαμορφωμ#νο για HTTPS, επανεκκιν#στε την υπηρεσι# για να ενεργοποιηθo#ν οι ρυθμ#σεις:

```
sudo service apache2 restart
```



Αν#λογα με τον πως αποκτ#σατε το πιστοποιητικ# σας #σως χρειαστε# να εισ#γετε #να συνθηματικ# #ταν εκκινήθε# ο Apache2.

Μπορε#τε να εισ#λθετε στις ασφαλε#ς σελ#δες του διακομιστ# πληκτρολογ#ντας `https://your_hostname/url/` στην μπ#ρα διε#θυνσης του φυλλομετρητ# 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=rw "}" \;
```



If access must be granted to more than one group per directory, enable Access Control Lists (ACLs).

## 1.5. #####

- Το *Apache2 Documentation*<sup>6</sup> περιχει πληροφορίες σε βθος για τους κδικες παραπομπς διαμρφωσης του Apache2. Επσης, δετε το πακτο apache2-doc για τα επσημα αρχεα του Apache2.
- Δετε την ιστοσελδα *Mod SSL Documentation*<sup>7</sup> για περισστερες πληροφορίες σχετικς με SSL.
- Το *Apache Cookbook*<sup>8</sup> του O'Reilly ενα καλ# μσο για να πετχετε συγκεκριμνες διαμορφσεις για το Apache2.
- Για συγκεκριμνες ερωτσεις για τον Apache2 για Ubuntu, ρωτστε στο κανλι IRC *#ubuntu-server* στο *freenode.net*<sup>9</sup>.
- Συνθως ενσωματωμνη με την PHP και τη MySQL η σελδα *Apache MySQL PHP Ubuntu Wiki*<sup>10</sup> ενα καλ# πηγ#.

---

<sup>6</sup> <http://httpd.apache.org/docs/2.2/>

<sup>7</sup> <http://www.modssl.org/docs/>

<sup>8</sup> <http://oreilly.com/catalog/9780596001919/>

<sup>9</sup> <http://freenode.net/>

<sup>10</sup> <https://help.ubuntu.com/community/ApacheMySQLPHP>



## 2. PHP5 - #####

Η PHP είναι μια γλώσσα σενάρου γενικού σκοπού κατάλληλη για ανάπτυξη Ιστό#. Το σενάριο PHP μπορεί να ενσωματωθεί στην HTML. Αυτή η ενότητα εξηγεί πώς 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 Ιστό# Apache2 και τον Διακομιστή Βάσεως δεδομένων MySQL. Μπορείτε να αναφερθείτε στα τμήματα Apache2 και MySQL σε αυτή το αρχείο για να εγκαταστήσετε και να διαμορφώσετε τον Apache2 και το MySQL αντίστοιχα.

### 2.1. #####

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 εντολ#ν:

```
sudo apt-get install php5 libapache2-mod-php5
```

Μπορείτε να εκτελέσετε PHP5 σενάρια απ# τη γραμμή εντολ#ν. Για να εκτελέσετε σενάρια PHP5 από τη γραμμή εντολ#ν πρέπει να εγκαταστήσετε το πακέτο php5-cli. Για να το εγκαταστήσετε το php5-cli μπορείτε να πληκτρολογήσετε την ακόλουθη εντολή στο τερματικό εντολ#ν:

```
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 εντολ#ν 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 εντολ#ν:

```
sudo apt-get install php5-mysql
```

Ομο#ως, για να χρησιμοποι#σετε PostgreSQL με PHP5 πρ#πει να εγκαταστ#σετε το πακ#το php5-pgsql. Για να εγκαταστ#σετε το php5-pgsql μπορείτε να πληκτρολογ#σετε την ακ#λουθη εντολ# στο τερματικ# εντολ#ν:

```
sudo apt-get install php5-pgsql
```

## 2.2. #####

Αφο# εγκαταστ#σετε την PHP5, μπορείτε να εκτελ#σετε σεν#ρια PHP5 απ# τον φυλλομετρητ# ιστο# σας. Ε#ν #χετε εγκαταστ#σει το πακ#το php5-cli, μπορείτε να εκτελ#σετε σεν#ρια PHP5 απ# τη γραμμ# εντολ#ν.

Απ# προεπιλογ#, ο διακομιστ#ς Ιστο# Apache2 ε#ναι διαμορφωμ#νος να εκτελε# σεν#ρια PHP5. Με #λλα λ#για, η υπομον#δα PHP5 ενεργοποιε#τε στον διακομιστ# Ιστο# Apache2 αυτ#ματα #ταν εγκαθιστ#τε την υπομον#δα. Παρακαλ# επαληθε#στε ε#ν τα αρχε#α /etc/apache2/mods-enabled/php5.conf και /etc/apache2/mods-enabled/php5.load υπ#ρχουν. Ε#ν δεν υπ#ρχουν, μπορείτε να ενεργοποι#σετε την υπομον#δα χρησιμοποι#ντας την εντολ# **a2enmod**.

Μ#λις εγκαταστ#σετε τα πακ#τα που σχετ#ζονται με PHP5 και ενεργοποι#σετε την εν#τητα PHP5 Apache 2, θα πρ#πει να επανεκκιν#σετε το διακομιστ# διαδικτ#ου Apache2 για να τρ#ξει τα σεν#ρια PHP5. Μπορείτε να εκτελ#σετε την ακ#λουθη εντολ# σε #να τερματικ# εντολ#ν για να κ#νετε επανεκκ#νηση το διακομιστ# διαδικτ#ου σας:

```
sudo service apache2 restart
```

## 2.3. #####

για να επαληθε#σετε την εγκατ#στασ# σας, μπορείτε να εκτελ#σετε το ακ#λουθο σεν#ριο PHP5 phpinfo:

```
<?php
    phpinfo();
?>
```

Μπορείτε να αποθηκε#σετε το περιεχ#μενο σε #να αρχε#ο `phpinfo.php` και να το τοποθετ#σετε κ#τω απ# τον κατ#λογο **DocumentRoot** του διακομιστ# Ιστο# Apache2. #ταν υποδε#ξετε στον φυλλομετρητ# σας το `http://hostname/phpinfo.php`, θα εμφαν#σει τιμ#ς διαφ#ρων παραμ#τρων διαμ#ρφωσης PHP5.

## 2.4. #####

- Για περισσ#τερες πληροφορι#ς σε β#θος δε#τε τις βοηθητικ#ς οδηγ#ες *php.net*<sup>11</sup>.

<sup>11</sup> <http://www.php.net/docs.php>

- Υπ#ρχει μια πληθ#ρα βιβλ#ων για την PHP. Δ#ο καλ# βιβλ#α απ# τον O'Reilly ε#ναι τα *Learning PHP 5*<sup>12</sup> και *PHP Cook Book*<sup>13</sup>.
- Επ#σης, δε#τε τη σελ#δα του wiki για *Apache MySQL PHP ### Ubuntu*<sup>14</sup> για περισσ#τερες πληροφορίες.

---

<sup>12</sup> <http://oreilly.com/catalog/9780596005603/>

<sup>13</sup> <http://oreilly.com/catalog/9781565926813/>

<sup>14</sup> <https://help.ubuntu.com/community/ApacheMySQLPHP>

### 3. Squid - ##### μ#####

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. #####

Σε #να τερματικ# εντολ#ν, πληκτρολογ#στε την ακ#λουθη εντολ# για να εγκαταστ#σετε το διακομιστ# Squid:

```
sudo apt-get install squid3
```

#### 3.2. #####

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 ορ#σετε τον διακομιστ# Squid να ακο#ει τη θ#ρα TCP 8888 αντ# για την προεπιλεγμ#νη θ#ρα TCP 3128, αλλ#ξτε τον κ#δικα παραπομπ#ς `http_port`:

```
http_port 8888
```

- Αλλ#ξτε τον κ#δικα παραπομπ#ς `visible_hostname` #στε να δ#σετε στον διακομιστ# Squid #να συγκεκριμ#νο #νομα. Αυτ# το #νομα κεντρικο# υπολογιστ# δεν πρ#πει να ε#ναι

απαρ#τητα το #νομα του κεντρικο# υπολογιστ#. Σε αυτ# το παρ#δειγμα ορ#ζεται σε *weezie*

```
visible_hostname weezie
```

- Χρησιμοποι#ντας τον #λεγχο πρ#σβασης Squid, μπορε#τε να διαμορφ#σετε υπηρεσ#ες Διαδικτ#ου που #χουν διαμεσολαβητ# το Squid #στε να ε#ναι διαθ#σιμες μ#νο σε χρ#στες με συγκεκριμ#νες IP διευθ#νσεις. Για παρ#δειγμα, θα επεξηγ#σουμε την πρ#σβαση απ# χρ#στες του υποδικτ#ου 192.168.42.0/24 μ#νο:

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. #####

##### Squid<sup>15</sup>

<sup>15</sup> <http://www.squid-cache.org/>

Σελ#δα *Ubuntu Wiki Squid*<sup>16</sup>.

---

<sup>16</sup> <https://help.ubuntu.com/community/Squid>

## 4. Ruby on Rails

Το Ruby on Rails είναι ένα πλαίσιο ιστο ανοιχτού κώδικα για την ανάπτυξη εφαρμογών ιστο με βάση δεδομένων. Είναι βελτιστοποιημένο για την ανεκτίμηση παραγωγικότητας του προγραμματιστή καθώς επιτρέπει στον προγραμματιστή να γράψει κώδικα ευνοώντας τη συνθημία αντί την διαμρφώση.

### 4.1. #####

Πριν εγκαταστήσετε το Rails θα πρέπει να εγκαταστήσετε τα Apache και MySQL. Για να εγκαταστήσετε το πακέτο Apache, παρακαλώ αναφερθείτε στο [μικροβιβλίο 1, &#x201C;HTTPD - Apache2 #####&#x201D; \[194\]](#). Για οδηγίες για το πώς να εγκαταστήσετε το MySQL αναφερθείτε στο [μικροβιβλίο 1, &#x201C;MySQL&#x201D; \[216\]](#).

Αφού έχετε εγκαταστήσει τα #####Apache και MySQL, έχετε #τοιμοί 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 εντολίν:

```
sudo apt-get install rails
```

### 4.2. #####

τροποποιήστε το αρχείο διαμρφώσης `/etc/apache2/sites-available/default` για να εγκαταστήσετε τον τομ#α.

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 υπομονή `mod_rewrite` για τον Apache. Για να ενεργοποιήσετε την υπομονή `mod_rewrite`, παρακαλώ πληκτρολογήστε την ακόλουθη εντολή σε ένα τερματικό εντολίν:

```
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 εκτελέσει 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. #####

- Δείτε την ιστοσελίδα *Ruby on Rails*<sup>17</sup> για περισσότερες πληροφορίες.
- Επσης το *Agile Development with Rails*<sup>18</sup> είναι μια καλή πηγή.
- Άλλη τοποθεσία για περισσότερες πληροφορίες είναι η σελίδα *Ruby on Rails Ubuntu Wiki*<sup>19</sup>.

---

<sup>17</sup> <http://rubyonrails.org/>

<sup>18</sup> <http://pragprog.com/titles/rails3/agile-web-development-with-rails-third-edition>

<sup>19</sup> <https://help.ubuntu.com/community/RubyOnRails>



## 5. Apache Tomcat

Το Apache Tomcat είναι ένα δοχείο ιστο# που σας επιτρέπει να εξυπηρετείται εφαρμογ#ς ιστο# 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. ##### μ#

Για να εγκαταστήσετε το διακομιστή Tomcat, μπορείτε να εισ#γετε την ακ#λουθη εντολ# στο τερματικ# εντολ#ν:

```
sudo apt-get install tomcat6
```

Αυτ# θα εγκαταστήσει το διακομιστή Tomcat με μ#νο μια εφαρμογ# ιστο# ROOT που προβ#λει μια απλ# σελ#δα #λειτουργε## απ# προεπιλογ#.

### 5.2. #####

Τα αρχε#α διαμ#ρφωσης του Tomcat μπορο#ν να βρεθο#ν στο /etc/tomcat6. Μ#νο λ#γες κοιν#ς αλλαγ#ς διαμ#ρφωσης θα περιγραφο#ν εδ#, παρακαλ# δε#τε το Tomcat 6.0 *documentation*<sup>20</sup> για περισσ#τερα.

#### 5.2.1. #####

Απ# προεπιλογ# το Tomcat 6.0 τρ#χει #ναν συζευκτ#ρα HTTP στη θ#ρα 8080 και #ναν συζευκτ#ρα AJP στη θ#ρα 8009. #σως θ#λετε να αλλ#ξετε τις προεπιλεμ#νες θ#ρες για να αποφ#γετε σ#γκρουση με #ναν #λλο διακομιστ# του συστ#ματος. Αυτ# γ#νεται αλλ#ζοντας τις ακ#λουθες γραμμ#ς 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. #####

Απ# προεπιλογ# το Tomcat θα τρ#ξει κατ# προτ#μηση με το OpenJDK-6, μετ# θα δοκιμ#σει το Sun's JVM, μετ# θα δοκιμ#σει κ#ποια #λλα JVMs. Ε#ν #χετε πολλαπλ# JVMs εγκατεστημ#να,

<sup>20</sup> <http://tomcat.apache.org/tomcat-6.0-doc/index.html>

μπορείτε να ορίσετε ποια θύλη να χρησιμοποιηθούν ορίζοντας το `JAVA_HOME` στο `/etc/default/tomcat6`:

```
JAVA_HOME=/usr/lib/jvm/java-6-sun
```

### 5.2.3. #####

Ονόματα χρηστών, κωδικός 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. ##### Tomcat

Το Tomcat αποστέλλεται με εφαρμογές ιστο που μπορείτε να εγκαταστήσετε για σκοπούς τεκμηρίωσης, διαχείρισης δοκιμαστικών.

### 5.3.1. ##### Tomcat

Το πακέτο `tomcat6-docs` περιέχει τις βοηθητικές οδηγίες του Tomcat 6.0, δομημένες σαν εφαρμογή ιστο στην οποία μπορείτε να έχετε πρόσβαση απ' προεπιλογή στο `http://yourserver:8080/docs`. Μπορείτε να το εγκαταστήσετε πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολ:

```
sudo apt-get install tomcat6-docs
```

### 5.3.2. ##### Tomcat

Το πακέτο `tomcat6-admin` περιέχει δύο εφαρμογές ιστο 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 εντολ:

```
sudo apt-get install tomcat6-admin
```

Το πρώτο είναι η εφαρμογή ιστο *manager*, την οποία μπορείτε να βρείτε απ' προεπιλογή στο `http://yourserver:8080/manager/html`. Πρωτστώς χρησιμοποιείται για τη λήψη κατάστασης διακομιστή και για την επανεκκίνηση εφαρμογών ιστο.



Η πρόσβαση στην εφαρμογή *manager* προστατεύεται απ' 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 ιστο *host-manager*, την οποία μπορείτε να βρείτε απ' 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 μπορείτε 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 ιστο `admin` (ανπτυξη εφαρμογής, δημιουργία εικονικού υπολογιστή) χρειάζονται δειά 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. ##### Tomcat

Το πακέτο `tomcat6-examples` περιλαμβάνει δύο εφαρμογές ιστο που μπορούν να χρησιμοποιηθούν για να ελεγχθούν να επιδεξούν 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 εντολ:

```
sudo apt-get install tomcat6-examples
```

### 5.4. #####

Το Tomcat χρησιμοποιείται πολύ στην ανάπτυξη και τον έλεγχο σεναρίων που η χρησιμοποίηση ενός στιγμιτύπου για το στήμα δεν πληροί τις απαιτήσεις πολλών χρηστών σε ένα μόνο στήμα. Τα πακέτα του Tomcat 6.0 στο Ubuntu έχουν εργαλεία για να σας βοηθήσουν να αναπτύξετε τα δική σας στιγμιτυπα προσανατολισμένα στο χρήστη, επιτρέποντας σε κάθε χρήστη του συστήματος (χωρίς δικαιώματα βήσης) να εκτελούν ξεχωριστά ιδιωτικά στιγμιτυπα ενώ χρησιμοποιούν ακόμα τις βιβλιοθήκες συστήματος.



Είναι δυνατό να εκτελέσετε το στιγμιτυπο για λο το στήμα παράλληλα με ιδιωτικά στιγμιτυπα, εφόσον δε χρησιμοποιούν τις διες TCP πλες.

#### 5.4.1. #####

Μπορείτε να εγκαταστήσετε οτιδήποτε απαραίτητο για να εκτελέσετε ιδιωτικά σεναρία πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολ:

```
sudo apt-get install tomcat6-user
```

#### 5.4.2. #####

Μπορείτε να δημιουργήσετε έναν κατάλογο ιδιωτικών στιγμιτυπων πληκτρολογώντας την ακόλουθη εντολή στο τερματικό εντολ:

**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 κοινότητες βιβλιοθηκών σας στον υποκατάλογο `lib/` και να αναπτύξετε τις εφαρμογές ιστο στον υποκατάλογο `webapps/`. Κάθε εφαρμογή ιστο δεν αναπτύσσεται απ' προεπιλογή.

#### 5.4.3. #####

Θα βρείτε τα κλασικά αρχεία διαμόρφωσης του Tomcat για τα ιδιωτικά στιγμιότυπά σας στον υποκατάλογο `conf/`. Θα πρέπει για παράδειγμα σ'αυτά να επεξεργαστείτε το αρχείο `conf/server.xml` για να αλλάξετε τις προεπιλεγμένες θύρες που χρησιμοποιούνται απ' το ιδιωτικό στιγμιότυπο Tomcat για να αποφύγετε σύγκρουση με άλλα στιγμιότυπα που μπορεί να εκτελούνται.

#### 5.4.4. #####

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**



Συστηνεται 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. #####

- Δείτε την ιστοσελίδα *Apache Tomcat*<sup>21</sup> για περισσότερες πληροφορίες.
- το *Tomcat: The Definitive Guide*<sup>22</sup> είναι ένας καλός πηρος για τη δημιουργία εφαρμογών ιστο με το Tomcat.
- Για επιπλέον βιβλία δείτε λίστα στη σελίδα *Tomcat Books*<sup>23</sup>.
- Επίσης, δείτε τη σελίδα *Ubuntu Wiki Apache Tomcat*<sup>24</sup>.

<sup>21</sup> <http://tomcat.apache.org/>

<sup>22</sup> <http://oreilly.com/catalog/9780596003180/>

<sup>23</sup> <http://wiki.apache.org/tomcat/Tomcat/Books>

<sup>24</sup> <https://help.ubuntu.com/community/ApacheTomcat5>

---

## Κεφάλαιο 12. Βάσεις δεδομένων

Το Ubuntu παρ#χει δ#ο δημοφιλε#ς εξυπηρετητ#ς β#σεων δεδομ#νων. Ε#ναι οι:

- MySQL™
- PostgreSQL

Ε#ναι διαθ#σιμοι στο κ#ριο αποθετ#ριο. Αυτ# η εν#τητα εξηγ# π#ς να εγκαταστ#σετε και να ρυθμ#σετε αυτο#ς τους εξυπηρετητ#ς β#σεων δεδομ#νων.

# 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. #####

Για να εγκαταστ#σετε το MySQL, εκτελ#στε την ακ#λουθη εντολ# σε #να τερματικ#:

```
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.

Μ#λις η εγκατ#σταση ολοκληρωθε#, ο εξυπηρετητ#ς MySQL θα πρ#πει να εκκινηθε# αυτ#ματα. Μπορε#τε να εκτελ#σετε την παρακ#τω εντολ# σε #να τερματικ# για να ελ#γξετε ε#ν ο εξυπηρετητ#ς MySQL #####:.....

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

#ταν εκτελε#τε αυτ# την εντολ#, θα πρ#πει να δε#τε τις ακ#λουθες γραμμ#ς # κ#τι παρ#μοιο:

```
tcp          0      0 localhost:mysql    *:*                LISTEN        2556/mysqld
```

Αν ο εξυπηρετητ#ς δεν εκτελε#ται σωστ#, μπορε#τε να πληκτρολογ#σετε την παρακ#τω εντολ# για να τον εκκιν#σετε:

```
sudo service mysql restart
```

## 1.2. #####

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
```



Αντικαταστ#στε το 192.168.0.5 με την κατ#λληλη διε#θυνση.

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*<sup>1</sup>.
- InnoDB is a more modern database engine, designed to be *ACID compliant*<sup>2</sup> which guarantees database transactions are processed reliably. Write locking can occur on a row level basis within a table. That means multiple updates can occur on a single table simultaneously. Data caching is also handled in memory within the database engine, allowing caching on a more efficient row level basis rather than file block. To meet ACID compliance all transactions are journaled independently of the main tables. This allows for much more reliable data recovery as data consistency can be checked.

---

<sup>1</sup> <http://www.mysqlperformanceblog.com/2006/06/17/using-mysam-in-production/>

<sup>2</sup> <http://en.wikipedia.org/wiki/ACID>

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*<sup>3</sup> 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:

```
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

---

<sup>3</sup> <http://tools.percona.com/members/wizard>



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. #####

- Δε#τε την ##### MySQL<sup>4</sup> για περισ#τερες πληροφορ#ες.
- Full documentation is available in both online and offline formats from the *MySQL Developers portal*<sup>5</sup>
- For general SQL information see *Using SQL Special Edition*<sup>6</sup> by Rafe Colburn.
- The *Apache MySQL PHP Ubuntu Wiki*<sup>7</sup> page also has useful information.

---

<sup>4</sup> <http://www.mysql.com/>

<sup>5</sup> <http://dev.mysql.com/doc/>

<sup>6</sup> <http://www.informit.com/store/product.aspx?isbn=0768664128>

<sup>7</sup> <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. #####

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. #####

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*<sup>8</sup> 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`

Εντοπ#στε τη γραμμ# `#listen_addresses = 'localhost'` και αλλ#ξτε 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.

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:

---

<sup>8</sup> <http://www.postgresql.org/docs/9.1/static/admin.html>

```
sudo -u postgres psql template1
```

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

```
ALTER USER postgres with encrypted password '#_#####_###';
```

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
```

Τ#λος, θα πρ#πει να επανεκκιν#σετε την υπηρεσ#α PostgreSQL για να αρχικοποιηθο#ν οι ν#ες ρυθμ#σεις. Σε #να τερματικ# πληκτρολογ#στε το παρακ#τω για να επανεκκιν#σετε την PostgreSQL:

```
sudo service postgresql restart
```



The above configuration is not complete by any means. Please refer *the PostgreSQL Administrator's Guide*<sup>9</sup> 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. #####

PostgreSQL databases should be backed up regularly. Refer to the *the PostgreSQL Administrator's Guide*<sup>10</sup> for different approaches.

## 2.4. #####

- As mentioned above the *the PostgreSQL Administrator's Guide*<sup>11</sup> 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:

<sup>9</sup> <http://www.postgresql.org/docs/9.1/static/admin.html>

<sup>10</sup> <http://www.postgresql.org/docs/9.1/static/backup.html>

<sup>11</sup> <http://www.postgresql.org/docs/9.1/static/admin.html>

```
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 γενικ#ς πληροφορι#ς σχετικ# με την SQL δε#τε το *Using SQL Special Edition*<sup>12</sup> απ# τον Rafe Colburn.
- Also, see the *PostgreSQL Ubuntu Wiki*<sup>13</sup> page for more information.

---

<sup>12</sup> <http://www.informit.com/store/product.aspx?isbn=0768664128>

<sup>13</sup> <https://help.ubuntu.com/community/PostgreSQL>

---

## Κεφάλαιο 13. Εφαρμογές LAMP

## 1. #####

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 #να τερματικ# εντολ#ν πληκτρολογ#στε την ακ#λουθη εντολ#:

```
sudo tasksel install lamp-server
```

After installing it you'll be able to install most *LAMP* applications in this way:

- Λ#ψη εν#ς αρχε#ου που περι#χει τα πηγ#α αρχε#α της εφαρμογ#ς.
- Αποσυμπ#εση του αρχε#ο, συν#θως σε #ναν κατ#λογο προσβ#σιμο απ# κ#ποιον εξυπηρετητ# ιστο#.
- Depending on where the source was extracted, configure a web server to serve the files.
- Ρ#θμιση της εφαρμογ#ς για να συνδεθε# με τη β#ση δεδομ#νων.
- Εκτ#λεση κ#ποιου σεναρ#ου εντολ#ν, # περι#γηση σε κ#ποια σελ#δα της εφαρμογ#ς, για την εγκατ#σταση της β#σης δεδομ#νων που χρει#ζεται η εφαρμογ#.
- Μ#λεις τα παραπ#νω β#ματα, # παρ#μοια β#ματα, ολοκληρωθ#ν, θα ε#στε #τοιμοι να ξεκιν#σετε να χρησιμοποιε#τε την εφαρμογ#.

#να μειον#κτημα αυτ#ς της προσγγισης ε#ναι πως τα αρχε#α της εφαρμογ#ς δεν τοποθετ#νται στο σ#στημα αρχε#ων με κ#ποιον τυπικ# τρ#πο, πρ#γμα που μπορε# να προκαλ#σει σ#γχυση ως προς το πο# #χει εγκατασταθε# η εφαρμογ#. #να ακμ#η μεγαλ#τερο μειον#κτημα ε#ναι η αναβ#θμιση της εφαρμογ#. #ταν μια ν#α #κδοση κυκλοφορ#σει, η #δια διαδικασ#α που χρησιμοποι#θηκε για την εγκατ#σταση της εφαρμογ#ς θα χρειαστε# για να εφαρμοστο#ν οι ενημερ#σεις.

Ευτυχ#ς, μια σειρ# εφαρμογ#ν *LAMP* ε#ναι #δη σε πακ#τα για το Ubuntu και ε#ναι διαθ#σιμες για εγκατ#σταση με τον #διο τρ#πο #πως οι μ#-LAMP εφαρμογ#ς. Ωστ#σο, αν#λογα την εφαρμογ#, κ#ποια επιπλ#ον β#ματα ρ#θμισης και εγκατ#στασης μπορε# να χρειαστο#ν.

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 υπέρ την δειά GNU GPL.

### 2.1. #####

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 ιστοτού apache2. Για να εγκαταστήσετε τον εξυπηρετητή ιστοτού apache2, παρακαλούμε αναφερθείτε στην υποενότητα [#μ#μ# 1.1, &#x201C;#####&#x201D; \[194\]](#) της ενότητας [#μ#μ# 1, &#x201C;HTTPD - Apache2 #####μ#####&#x201D; \[194\]](#).

### 2.2. ##μ#####

Για να ρυθμίσετε την πρώτη σας εφαρμογή Wiki, παρακαλούμε εκτελέστε το ακόλουθο σενάριο 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 εντοπίζει το νούμερό 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 #χετε ονομ#σει το Wiki σας ως *my\_wiki\_name* θα πρ#πει να προσθ#σετε μια γραμμ# `&#x201C;("my_wiki_name", r".*")&#x201D;` στο αρχε#ο `/etc/moin/farmconfig.py` μετ# απ# τη γραμμ# `&#x201C;("mywiki", r".*")&#x201D;`.

Μ#λιν ρυθμ#σετε το MoinMoin για να εντοπ#σει την πρ#τη σας εφαρμογ# Wiki *mywiki*, θα πρ#πει να ρυθμ#σετε το `apache2` και να το ετοιμ#σετε για την εφαρμογ# σας Wiki.

Θα πρ#πει να προσθ#σετε τις ακ#λουθες γραμμ#ς στο αρχε#ο `/etc/apache2/sites-available/default` μ#σα στην κατηγορ#α `&#x201C;<VirtualHost *>&#x201D;`:

```
### 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
```

Μ#λιν ρυθμ#σετε τον εξυπηρετητ# ιστο# `apache2` και τον κ#νετε διαθ#σιμο για την εφαρμογ# σας Wiki, θα πρ#πει να τον επανεκκιν#σετε. Μπορε#τε να εκτελ#σετε την ακ#λουθη εντολ# για να επανεκκιν#σετε τον εξυπηρετητ# ιστο# `apache2`:

```
sudo service apache2 restart
```

## 2.3. #####

Μπορε#τε να ελ#γξετε την εφαρμογ# Wiki και να δε#τε αν λειτουργε# πηγα#νοντας με το πρ#γραμμα περι#γησ#ς σας στο παρακ#τω URL:

```
http://localhost/mywiki
```

Για περισσ#τερες πληροφορ#ες παρακαλο#με επισκεφθε#τε τον ιστ#τοπο του *MoinMoin*<sup>1</sup>.

## 2.4. #####

- Για περισσ#τερες πληροφορ#ες δε#τε το Wiki `### moinmoin`<sup>2</sup>.
- Also, see the *Ubuntu Wiki MoinMoin*<sup>3</sup> page.

<sup>1</sup> <http://moinmo.in/>

<sup>2</sup> <http://moinmo.in/>

<sup>3</sup> <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. #####

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 δέστε το πακέτο mediawiki-extensions.

#### 3.2. #####

Το αρχείο ρθμίσης του Apache για το MediaWiki είναι εγκατεστημένο στον κατάλογο `/etc/apache2/conf.d/`. Θα πρέπει να αποσχολίσετε την ακόλουθη γραμμή σε αυτό το αρχείο για να αποκτήσετε πρόσβαση στην εφαρμογή MediaWiki.

```
# Alias /mediawiki /var/lib/mediawiki
```

Αφού αποσχολίσετε 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 `&#x201C;Checking environment...&#x201D;` σε αυτή τη σελίδα. Θα μπορείτε να διορθώσετε 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. #####

Οι επεκτάσεις προσθ#τουν νέες λειτουργ#ες και βελτι#σεις στην εφαρμογ# MediaWiki. Οι επεκτάσεις δ#νουν στους διαχειριστ#ς και στους τελικο#ς χρ#στες τη δυνατ#τητα να προσαρμ#σουν το MediaWiki στις απαιτ#σεις τους.

Μπορε#τε να κ#νετε λ#ψη επεκτ#σεων του MediaWiki ως συμπιεσμ#νο αρχε#ο # απ# το αποθετ#ριο Subversion. Θα πρ#πει να τις αντιγρ#ψετε στον κατ#λογο `/var/lib/mediawiki/extensions`. Επ#σης, θα πρ#πει να προσθ#σετε την ακ#λουθη γραμμ# στο τ#λος του αρχε#ου `/etc/mediawiki/LocalSettings.php`.

```
require_once "$IP/extensions/#####/#####.php";
```

### 3.4. #####

- Για περισσ#τερες πληροφορ#ες, παρακαλο#με αναφερθε#τε στον ιστ#τοπο του *MediaWiki*<sup>4</sup>
- Ο ##### *MediaWiki* #####<sup>5</sup> περι#χει πλ#θος πληροφορι#ν για ν#ους διαχειριστ#ς MediaWiki.
- Also, the *Ubuntu Wiki MediaWiki*<sup>6</sup> page is a good resource.

---

<sup>4</sup> <http://www.mediawiki.org>

<sup>5</sup> <http://www.packtpub.com/Mediawiki/book>

<sup>6</sup> <https://help.ubuntu.com/community/MediaWiki>

## 4. phpMyAdmin

Το phpMyAdmin είναι μια εφαρμογή LAMP γραμμένη ειδικά για τη διαχείριση εξυπηρετητή MySQL. Γραμμένο σε PHP και προσβάσιμο μέσω ενός περιηγητή ιστοσελίδων, το phpMyAdmin προσφέρει ένα γραφικό περιβάλλον για εργασίες διαχείρισης βάσεων δεδομένων.

### 4.1. #####

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 εδφ: [\[1\]](#), [\[2\]](#), [\[3\]](#), [\[4\]](#), [\[5\]](#), [\[6\]](#), [\[7\]](#), [\[8\]](#), [\[9\]](#), [\[10\]](#), [\[11\]](#), [\[12\]](#), [\[13\]](#), [\[14\]](#), [\[15\]](#), [\[16\]](#). Σε ένα τερματικό πληκτρολογήστε:

```
sudo apt-get install phpmyadmin
```

Στο τερματικό επιλέξτε ποιος εξυπηρετητής ιστοθ θα ρυθμίσετε για το phpMyAdmin. Το υπόλοιπο αυτς της εντητας θα χρησιμοποιεθ το Apache2 για εξυπηρετηθ ιστοθ.

Σε έναν περιηγηθ πηγαίνετε στο [http://###μ#\\_#####/phpmyadmin](http://###μ#_#####/phpmyadmin), αντικαθιστώντας το [###μ#\\_#####](#) με το πραγματικό #νομα του εξυπηρετηθ. Στη σελδα εισδου, πληκτρολογήστε root για [###μ#\\_#####](#), ή κποιον #λλο χρσθ MySQL, αν #χετε κνει κποια ρθμιση, και πληκτρολογήστε τον κωδικ# πρσβασης MySQL του χρσθ.

Μ#λις συνδεθε#τε, μπορε#τε να επαναφ#ρετε τον κωδικ# του root, αν χρειζεται, να δημιουργ#σετε χρστες, να δημιουργ#σετε/διαγρ#ψετε β#σεις δεδομ#νων και π#νακες, κτλ.

### 4.2. ###μ#####

Τα αρχε#α ρθμισης του phpMyAdmin βρ#σκονται στο `/etc/phpmyadmin`. Το κ#ριο αρχε#ο ρυθμ#σεων ε#ναι το `/etc/phpmyadmin/config.inc.php`. Αυτ# το αρχε#ο περι#χει ρυθμ#σεις που ισχ#ουν για ολ#κληρο το phpMyAdmin.

Για να χρησιμοποι#σετε το phpMyAdmin για να διαχειριστε#τε μια β#ση δεδομ#νων MySQL που φιλοξενε#ται σε #ναν #λλον εξυπηρετηθ, ρυθμ#στε τα ακ#λουθα στο `/etc/phpmyadmin/config.inc.php`:

```
$cfg['Servers'][$i]['host'] = 'db_server';
```



Αντικαταστ#στε το `db_server` με το πραγματικό #νομα # τη διεθ#νση IP του απομακρυσμ#νου εξυπηρετηθ β#σεων δεδομ#νων. Επ#σης, σιγουρευτε#τε πω# ο υπολογιστς που ε#ναι εγκατεστημ#νο το phpMyAdmin #χει δικαι#ματα πρσβασης στην απομακρυσμ#νη β#ση δεδομ#νων.

Μέλις 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 υποσλιδίου 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 παρχει το site του phpMyAdmin. Το αρχείο περιχει οδηγίες για την φέρωση της PHP, για δικαιώματα καταλόγων, κτλ. Για περισσότερες πληροφορίες σχετικά με τη ρύθμιση του Apache2 δείτε εδ: [#1, &#x201C;HTTPD - Apache2 #####&#x201D; \[194\]](#).

#### 4.3. #####

- Η τεκμηρίωση του phpMyAdmin εγκαθίσταται μαζί με το πακέτο και μπορεί να βρεθεί από τον σύνδεσμο [##### phpMyAdmin](#) (ένα ερωτηματικό με ένα πλάσιο γράμμα του), κάτω από το λογότυπο του phpMyAdmin. Η επσημη τεκμηρίωση μπορεί επίσης να βρεθεί στον ιστότοπο του *phpMyAdmin*<sup>7</sup>.
- Επίσης, το *Mastering phpMyAdmin*<sup>8</sup> είναι μια πολύ καλή πηγή.
- A third resource is the *phpMyAdmin Ubuntu Wiki*<sup>9</sup> page.

---

<sup>7</sup> [http://www.phpmyadmin.net/home\\_page/docs.php](http://www.phpmyadmin.net/home_page/docs.php)

<sup>8</sup> <http://www.packtpub.com/phpmyadmin-3rd-edition/book>

<sup>9</sup> <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. #####

To install WordPress, run the following comand 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 [μ#μ# 1.1, &#x201C;#####&#x201D; \[194\]](#) sub-section in [μ#μ# 1, &#x201C;HTTPD - Apache2 #####&#x201D; \[194\]](#) section. For installing mysql server, please refer to [μ#μ# 1.1, &#x201C;#####&#x201D; \[216\]](#) sub-section in [μ#μ# 1, &#x201C;MySQL&#x201D; \[216\]](#) section.

### 5.2. #####

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](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. #####

- *WordPress.org Codex*<sup>10</sup>
- *Ubuntu Wiki WordPress*<sup>11</sup>

---

<sup>10</sup> <https://codex.wordpress.org/>

<sup>11</sup> <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, κάλπτουμε την εγκατάσταση και τη ρύθμιση για FTP, NFS και CUPS.

## 1. ##### 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 ##### 6, #####μ#####μ#### [82] 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 - ##### 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. #####μ####μ## 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 κ#νετε την αλλαγή, επανεκκιν#στε 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. ##### FTP μ# #####

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
```

Τ#ρα επανεκκιν#στε το vsftpd:

```
sudo restart vsftpd
```

Τ#ρα, #ταν οι χρ#στες του συστ#ματος συνδ#ονται στο FTP, θα ξεκιν#ν στους #####  
##### τους, #που μπορ#ν να κ#νουν λ#ψη, αποστολ#, δημιουργ#α καταλ#γων, 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 αν#νυμης αποστολ#ς FTP μπορε# να ε#ναι ακρα#ος κ#νδυνος ασφαλε#ας. Ε#ναι καλ#τερα να μην ενεργοποι#σετε την αν#νυμη αποστολ# σε εξυπηρετητ#ς στους οπο#ους ε#ναι δυνατ# η πρ#σβαση απευθε#ας απ# το διαδ#κτυο.

Το αρχε#ο ρυθμ#σεων αποτελε#ται απ# πολλ#ς παραμ#τρους ρ#θμισης. Οι πληροφορι#ες για κ#θε παρ#μετρο ε#ναι διαθ#σιμες στο αρχε#ο ρυθμ#σεων. Εναλλακτικ#, μπορε#τε να αναφερθε#τε στη σελ#δα `man - man 5 vsftpd.conf` - για λεπτομ#ρειες για κ#θε παρ#μετρο.

### 1.4. ##### FTP

Υπ#ρχουν επιλογ#ς στο /etc/vsftpd.conf που βοηθ#νε στο να κ#νετε το vsftpd πιο ασφαλ#. Για παρ#δειγμα οι χρ#στες μπορ#ν να περιοριστ#ν στους αρχικο#ς τους καταλ#γους αν αποσχολι#σετε 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 αποσχολισετε τις παραπάνω επιλογές, δημιουργήστε ένα αρχείο `/etc/vsftpd.chroot_list` που περιχει 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 #### η πρόσβαση FTP. Η προεπιλεγμένη λίστα περιχει τους χρήστες `root`, `daemon`, `nobody`, κτλ. Για να απενεργοποιήσετε την πρόσβαση FTP σε επιπλέον χρήστες, απλώς 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 σχετικές 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 [μ#μ# 5, &#x201C;#####&#x201D; \[175\]](#).

Τώρα επανεκκινήστε το `vsftpd`, και οι μ#-άνωνυμοι 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: #####  
/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, απ# προεπιλογ# το vsftpd χρησιμοποιε# το PAM για πιστοπο#ηση και το αρχε#ο ρυθμ#σεων /etc/pam.d/vsftpd περι#χει το παρακ#τω:

```
auth    required    pam_shells.so
```

Το #ρθρωμα PAM *shells* περιορ#ζει την πρ#σβαση στα κελ#φη που υπ#ρχουν στο αρχε#ο /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. #####

- Δε#τε τον ##### ## vsftpd<sup>1</sup> για περισσ#τερες πληροφορ#ες.
- For detailed /etc/vsftpd.conf options see the *vsftpd.conf man page*<sup>2</sup>.

---

<sup>1</sup> [http://vsftpd.beasts.org/vsftpd\\_conf.html](http://vsftpd.beasts.org/vsftpd_conf.html)

<sup>2</sup> <http://manpages.ubuntu.com/manpages/raring/en/man5/vsftpd.conf.5.html>

## 2. ##### (NFS)

Το NFS επιτρέπει σε ένα σύστημα να μοιραστεί καταλόγους και αρχεία με άλλα μ#σω εν#ς δικτ#ου. Με τη χρ#ση του NFS, οι χρ#στες και τα προγρ#μματα μπορο#ν να #χουν πρ#σβαση σε αρχεία που βρ#σκονται σε απομακρυσμ#να συστ#ματα σχεδ#ν σα να #ταν τοπικ# αρχεία.

Κ#ποια απ# τα πιο αξιοσημ#ωτα πλεονεκτ#ματα που προσφ#ρει το NFS ε#ναι:

- Οι τοπικ# σταθμο# εργασ#ας χρησιμοποιο#ν λιγ#τερο χ#ρο στο δ#σκο επειδ# τα δεδομ#να που χρησιμοποιο#νται συχν#, μπορο#ν να αποθηκευτο#ν σε #να μ#χ#νημα και να παραμεινουν ακμ#η προσβ#σιμα σε #λλους μ#σω του δικτ#ου.
- Δεν χρει#ζεται οι χρ#στες να #χουν ξεχωριστο#ς αρχικο#ς καταλόγους σε κ#θε μ#χ#νημα του δικτ#ου. Οι αρχικο# κατ#λόγοι μπορο#ν να τοποθετηθο#ν στον εξυπηρετητ# NFS και να ε#ναι διαθ#σιμοι μ#σω του δικτ#ου.
- Οι συσκευ#ς αποθ#κευσης #πως οι συσκευ#ς δισκ#τας, CDROM και USB μπορο#ν να χρησιμοποιηθο#ν απ# #λλα μ#χαν#ματα στο δ#κτυο. Αυτ# μπορε# να μεισει τον αριθμ# των αφαιρομ#νων συσκευ#ν που υπ#ρχουν στο δ#κτυο.

### 2.1. #####

Σε #να τερματικ# πληκτρολογ#στε την ακ#λουθη εντολ# για να εγκαταστ#σετε τον εξυπηρετητ# NFS:

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

### 2.2. #####

Μπορε#τε να ρυθμ#σετε τους καταλόγους που θα εξαχθο#ν προσθ#τοντ# τους στο αρχε#ο /etc/exports. Για παρ#δειγμα:

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

Μπορε#τε να αντικαταστ#σετε το \* με μια απ# τις μορφ#ς ον#ματος υπολογιστ#. Κ#ντε την καταχρ#ρηση του ον#ματος υπολογιστ# #σο πιο συγκεκριμ#νη γ#νεται #στε να μην ε#ναι δυνατ# η πρ#σβαση του π#ρου NFS απ# ανεπιθ#μητα συστ#ματα.

Για να εκκιν#σετε τον εξυπηρετητ# NFS, μπορε#τε να εκτελ#σετε την παρακ#τω εντολ# σε #να τερματικ#:

```
sudo service nfs-kernel-server start
```

## 2.3. ##### NFS

Χρησιμοποιήστε την εντολή `mount` για να προσάρтите έναν κοινόχρηστο κατάλογο NFS απ' 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`.

Ενας εναλλακτικός τρόπος για να προσάρтите έναν κοινόχρηστο κατάλογο απ' 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 εξηγείται 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. #####

*Linux NFS faq*<sup>3</sup>

*Ubuntu Wiki NFS Howto*<sup>4</sup>

---

<sup>3</sup> <http://nfs.sourceforge.net/>

<sup>4</sup> <https://help.ubuntu.com/community/NFSv4Howto>

### 3. A##### 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:s17b92030000520000-2
```



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. #####

*Open-iSCSI Website*<sup>5</sup>

*Debian Open-iSCSI page*<sup>6</sup>

---

<sup>5</sup> <http://www.open-iscsi.org/>

<sup>6</sup> <http://wiki.debian.org/SAN/iSCSI/open-iscsi>

## 4. CUPS - #####

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. #####

Για να εγκαταστήσετε το CUPS στον υπολογιστή σας, απλ# χρησιμοποι#στε το `sudo` με την εντολ# `apt-get` και δ#στε τα πακ#τα προς εγκατ#σταση ως πρ#τη παρ#μετρο. Μια ολοκληρωμ#νη εγκατ#σταση CUPS #χει πολλ#ς εξαρτ#σεις πακ#των, αλλ# μπορο#ν #λες να δοθο#ν στην #δια εντολ#. Πληκτρολογ#στε το παρακ#τω σε #να τερματικ# για να εγκαταστ#σετε το CUPS:

```
sudo apt-get install cups
```

Μ#λιν πιστοποιηθε#τε με τον κωδικ# πρ#σβασης του χρ#στη σας, τα πακ#τα θα πρ#πει να ληφθο#ν και να εγκατασταθο#ν χωρ#ς σφ#λματα. Μετ# το π#ρας της εγκατ#στασης, ο εξυπηρετητ#ς CUPS θα εκκινηθε# αυτ#ματα.

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. #####

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 επεξεργαστε#τε το αρχε#ο ρυθμ#σεων, θα πρ#πει να δημιουργ#σετε #να αντ#γραφο του αρχικο# αρχε#ου και να το προστατ#ψετε απ# εγγραφ#, #στε να #χετε τις αρχικ#ς ρυθμ#σεις ως αναφορ# και να τις επαναχρησιμοποιε#τε πω#ς χρει#ζεται.



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
```



#ποτέ κ#νετε αλλαγές στο αρχείο ρυθμίσεων `/etc/cups/cupsd.conf`, θα χρειάζεται να επανεκκινήτε τον εξυπηρετητή CUPS πληκτρολογώντας την ακόλουθη εντολή σε ένα τερματικό:

```
sudo service cups restart
```

#### 4.3. #####



Το CUPS μπορεί να ρυθμίζεται και να παρακολουθείται μέσω ενός περιβάλλοντος ιστο#, που απ# προεπιλογ# είναι διαθέσιμο στο `http://localhost:631/admin`. Το περιβάλλον ιστο# μπορεί να χρησιμοποιηθε# για να πραγματοποιούνται όλες οι εργασίες διαχείρισης του εκτυπωτή.

Για να πραγματοποιήσετε διαχειριστικές εργασίες μέσω του περιβάλλοντος ιστο#, θα πρέπει είτε να #χετε τον λογαριασμό `root` ενεργοποιημένο στον εξυπηρετητή σας, # να πιστοποιηθε#τε ως κ#ποιος χρ#στής της ομάδας `lpadmin`. Για λόγους ασφαλείας, το CUPS δεν θα πιστοποιήσει κ#ποιον χρ#στή που δεν #χει κωδικ# πρόσβασης.

Για να προσθ#σετε #ναν χρ#στή στην ομάδα `lpadmin`, εκτελ#στε στο τερματικό:

```
sudo usermod -aG lpadmin ##μ#_#####
```

Περαιτ#ρω τεκμηρ#ωση είναι διαθέσιμη στην καρτ#λα `##μ#####` του περιβάλλοντος ιστο#.

#### 4.4. #####

##### CUPS<sup>7</sup>

Debian Open-iSCSI page<sup>8</sup>

<sup>7</sup> <http://www.cups.org/>

<sup>8</sup> <http://wiki.debian.org/SAN/iSCSI/open-iscsi>

---

## Κεφάλαιο 15. Υπηρεσίες Ηλ. Αλληλογραφίας

Η διαδικασία διαβίβασης ενός email απ# να τομο σε #λλο μ#σω του Διαδικτ#ου # #λλου δικτ#ου απαιτε# τη συνεργασ#α πολλ#ν διαφορετικ#ν συστημ#των. Καθ#να απ# αυτ# τα συστ#ματα θα πρ#πει να #χει ρυθμιστε# κατ#λληλα προκειμ#νου να λειτουργ#σει σωστ# η διαδικασ#α. Ο αποστολ#ας χρησιμοποιε# #ναν *Mail User Agent* (Πρ#κτορα Χρ#στη Αλληλογραφ#ας - MUA), # πελ#τη email, για την αποστολ# του μην#ματος μ#σω εν#ς # περισσ#τερων *Mail Transfer Agents* (Πρακτ#ρων Μεταφορ#ς Αλληλογραφ#ας - MTA), ο τελευτα#ος των οπο#ων παραδ#δει το μ#νυμα στον *Mail Delivery Agent* (Πρ#κτορα Παρ#δοσης Αλληλογραφ#ας - MDA). Ο τελευτα#ος το παραδ#δει στην ταχυδρομικ# θυρ#δα του παραλ#πτη, απ# #που ανακτ#ται απ# τον πελ#τη email του παραλ#πτη, συν#θως μ#σω εξυπηρετητ# POP3 # IMAP.

## 1. Postfix

Το Postfix είναι ο προεπιλεγμένος Mail Transfer Agent (MTA) του Ubuntu. Φιλοδοξεί να είναι γρηγορός, ευδιαχέριστος και ασφαλής. Είναι συμβατός με τον MTA sendmail. Σε αυτή την ενότητα περιγράφεται η εγκατάσταση και ρύθμιση του postfix. Επσης, περιγράφεται η χρήση του ως εξυπηρετητής SMTP με χρήση ασφαλούς σύνδεσης (για την ασφαλής αποστολή email).



Αυτός ο οδηγός δεν καλύπτει την εγκατάσταση *Virtual Domains* για το Postfix. Για πληροφορίες σχετικές με τους εικονικούς τομείς και άλλες προχωρημένες δυνατότητες, δείτε το *μύθος 1.7.4, &#x201C;Virtual Domains&#x201D; [256]*.

### 1.1. Εγκατάσταση

Για να εγκαταστήσετε το postfix εκτελέστε την ακόλουθη εντολή:

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

Απλώς πατήστε *enter* όποτε εμφανίζονται ερωτήσεις. Στο επόμενο σκριν θα κνείτε λεπτομερύτερες ρυθμίσεις

### 1.2. Ρύθμιση

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
- χι
- 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 αποδίδετε email. Επσης, το 192.168.0.0/24 με το δίκτυο και το ερώς (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 θύρας (mailbox) που θα χρησιμοποιήσετε. Η προεπιλογή του Postfix είναι το **mbox**. Αντ να τροποποιήσετε απευθείας το αρχείο ρυθμίσεων, μπορείτε να χρησιμοποιήσετε την

εντολή **postconf** για να ρυθμίσετε όλες τις παραμέτρους του postfix. Οι παράμετροι βρ#σκονται αποθηκευμένες στο αρχείο `/etc/postfix/main.cf`. Αργότερα, αν επιθυμείτε να τροποποιήσετε μια συγκεκριμένη παράμετρο, μπορείτε είτε να τρ#ξετε την εντολή, είτε να κ#νετε την αλλαγ# απευθείας στο αρχείο.

Για να ρυθμίσετε τη μορφή της ταχυδρομικής θυράδας ως **Maildir** εκτελέστε:

```
sudo postconf -e 'home_mailbox = Maildir/'
```



#τσι, τα νέα μηνύματα θα τοποθετούνται στο `/home/###μ#####/Maildir`. Θα πρέπει να ρυθμίσετε το Mail Delivery Agent (MDA) #στε να χρησιμοποιεί την #δια διαδρομή.

### 1.3. ##### 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. Μετ# την πιστοποίηση, ο εξυπηρετητ#ς SMTP θα επιτρέπει στον πελάτη να διαβίβ#ζει email.

1. Ρυθμίστε το Postfix #στε 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 ούρων του Postfix.

2. Next, generate or obtain a digital certificate for TLS. See #μ#μ# 5, &#x201C;#####&#x201D; [175] for details. This example also uses a Certificate Authority (CA). For information on generating a CA certificate see #μ#μ# 5.5, &#x201C;#####&#x201D; [178].



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 #μ#μ# 5.3, &#x201C;#####&#x201D; #####&#x201D; [177] for more details.



3. Αφού αποκτούμε πιστοποιητικό, ρυθμίζουμε το Postfix έτσι ώστε να παρχει 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 [μικροβλ. 5](#),  
&#x201C;#####&#x201D; [175].



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
smtpd_tls_security_level = may
smtpd_tls_security_level = may
smtpd_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*<sup>1</sup>. It is based on *SASL*<sup>2</sup>. However it is still necessary to set up SASL authentication before you can use SMTP-AUTH.

#### 1.4. Η εγκατάσταση της 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. Απλοποιήστε το, δίνοντας:

```
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 =
        #group =
    }
}
```

---

<sup>1</sup> <http://www.ietf.org/rfc/rfc2554.txt>

<sup>2</sup> <http://www.ietf.org/rfc/rfc2222.txt>

```
# 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 απλώς τερματίζοντας, εισάγετε:

```
sudo apt-get install mail-stack-delivery
```

Θα πρέπει πλέον να διαθέτετε ένα λειτουργικό εξυπηρετητή email, αλλά υπάρχουν και κάποιες ακριβείς επιλογές που σίγουρα ενδιαφέρουν. Π.χ., το πακέτο χρησιμοποιεί το πιστοποιητικό και το κλειδί του πακέτου `ssl-cert`, και σε ένα περιβάλλον παραγωγής θα πρέπει να χρησιμοποιήσετε πιστοποιητικό και κλειδί που έχουν δημιουργηθεί για το συγκεκριμένο σύστημα. Δείτε το `#μ#μ# 5, &#x201C;#####&#x201D; [175]` 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, επανεκκινείτε το Postfix:

```
sudo service postfix restart
```

## 1.6. #####

Η ρύθμιση του SMTP-AUTH χει ολοκληρώθηκε. 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. #####

Σε αυτή την ενότητα περιγράφονται ορισμένοι κοινοί τρόποι εντοπισμού της αιτίας σε περίπτωση που προκύψουν προβλήματα.

### 1.7.1. ##### chroot

Το πακέτο postfix του Ubuntu εγκαθίσταται απροεπιλόγως 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. ##### (Log)

Το Postfix αποστέλλει όλα τα μηνύματα καταγραφών στο `/var/log/mail.log`. Ωστόσο, επειδή τα μηνύματα σφάλματων και προειδοποιήσεων είναι εύκολο να χαθούν ανάμεσα στα κανονικά μηνύματα, καταγράφονται και στα αρχεία `/var/log/mail.err` και `/var/log/mail.warn`, αντίστοιχως.

Για να παρακολουθείτε σε πραγματικό χρόνο τα μηνύματα των καταγραφών, μπορείτε να χρησιμοποιήσετε την εντολή `tail -f`:

```
tail -f /var/log/mail.err
```

Το επόμενο λεπτομέρεια 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 επόμενο 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 λήψης 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 αξίωση των πληροφοριών που θα αποθηκεύονται στα αρχεία καταγραφών. Θυμηθείτε να επιστρέψετε στα προηγούμενα επίπεδα καταγραφών αφού επιλέξετε το πρόβλημα. Και φυσικά, επανεκκινήστε την κατάλληλη υπηρεσία για να εφαρμοστούν οι αλλαγές στις ρυθμίσεις.

#### 1.7.4. #####

Η διαχείριση ενός εξυπηρετητή Postfix μπορεί να αποδειχθεί ιδιαίτερα πολύπλοκη διαδικασία. Σας χρειαστεί να απευθυνθείτε στην κοινότητα του Ubuntu για πιο εξειδικευμένη βοήθεια.

Να καλέσετε τον αριθμό βοήθειας για το Postfix και να ενταχθείτε στην κοινότητα του Ubuntu Server είναι το κανάλι IRC `#ubuntu-server` στο *freenode*<sup>3</sup>. Επίσης, μπορείτε να δημοσιεύσετε μήνυμα σε ένα από τα ##### μ<sup>4</sup>.

Για εις βάθος εξερεύνηση του Postfix οι ειδικοί του Ubuntu συνιστούν το: ##### Postfix<sup>5</sup>.

Τέλος, ο ιστότοπος του Postfix<sup>6</sup> περιέχει επίσης καλή τεκμηρίωση όλων των διαθέσιμων ρυθμίσεων.

Also, the *Ubuntu Wiki Postfix*<sup>7</sup> page has more information.

<sup>3</sup> <http://freenode.net>

<sup>4</sup> <http://www.ubuntu.com/support/community/webforums>

<sup>5</sup> <http://www.postfix-book.com/>

<sup>6</sup> <http://www.postfix.org/documentation.html>

<sup>7</sup> <https://help.ubuntu.com/community/Postfix>

## 2. Exim4

Το Exim4 είναι ένας ακριβής 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. #####

Για να εγκαταστήσετε το exim4, εκτελέστε την ακόλουθη εντολή:

```
sudo apt-get install exim4
```

### 2.2. #####

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 καταναεμημένες 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 #ποτε εκτελέστε την εντολή **update-exim4.conf**

Μπορείτε να εκτελέσετε την ακόλουθη εντολή για να ξεκινήσετε την υπηρεσία Exim4.

```
sudo service exim4 start
```

### 2.3. ##### SMTP

Αυτή η ενότητα περιγράφει τη ρύθμιση του Exim4 #στε 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::"
    # ## μ## ##### ## ##### ##### ## μ### μ# #####μ### #####
    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. ##### 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` χρειάζεται ρύθμιση για χρήση του SMTP-AUTH με πιστοποίηση TLS και SASL.

## 2.5. #####

- Ανατρέξτε στο *exim.org*<sup>8</sup> για περισσότερες λεπτομέρειες.
- Επίσης, διατίθεται και το *##### Exim4*<sup>9</sup>.
- Another resource is the *Exim4 Ubuntu Wiki*<sup>10</sup> page.

---

<sup>8</sup> <http://www.exim.org/>

<sup>9</sup> <http://www.uit.co.uk/content/exim-smtp-mail-server>

<sup>10</sup> <https://help.ubuntu.com/community/Exim4>

### 3. ##### Dovecot

Το Dovecot είναι Mail Delivery Agent, γραμμένος με πρώτο γνώμονα την ασφάλεια. Υποστηρίζει τις κυριότερες μορφές ταχυδρομικών θυρών: mbox και Maildir. Σε αυτή την ενότητα περιγράφεται η ρύθμιση του ως εξυπηρετητή imap # pop3.

#### 3.1. #####

Για να εγκαταστήσετε το dovecot, εισάγετε την ακόλουθη εντολή στο τερματικό:

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

#### 3.2. #####

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 βιβλία της Βικιπαίδειας για το POP3<sup>11</sup> και το IMAP<sup>12</sup>.

Τα IMAPS και POP3S είναι περισσότερο ασφαλή απ' 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*<sup>13</sup>.

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 # (### ## maildir)
#
mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u # (### ## mbox)
```



Αν ο τύπος ταχυδρομικών θυρών σας ήταν διαφορετικός, θα πρέπει να ρυθμίσετε τον Mail Transport Agent (MTA) για να μεταφέρει την εισερχόμενη αλληλογραφία στον νέο τύπο.

<sup>11</sup> <http://en.wikipedia.org/wiki/POP3>

<sup>12</sup> [http://en.wikipedia.org/wiki/Internet\\_Message\\_Access\\_Protocol](http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol)

<sup>13</sup> <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 ενεργοποιήσει το `imap`, το `pop3`, μπορείτε να προσπαθήσετε να κνέτε εσοδο με τις εντολές **`telnet localhost pop3`** # **`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. ##### 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 [5, &#x201C;#####&#x201D; \[175\]](#) 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. #####

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. #####

- Ανατρέξτε στον [##### Dovecot<sup>14</sup>](#) για περισσότερες πληροφορίες.
- Also, the *Dovecot Ubuntu Wiki*<sup>15</sup> page has more details.

<sup>14</sup> <http://www.dovecot.org/>

<sup>15</sup> <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 λιστές ηλ. ταχυδρομείου ανοιχτού κώδικα (συμπεριλαμβανομένων και των [Ubuntu<sup>16</sup>](#)) χρησιμοποιούν το Mailman. Πρόκειται για ισχυρό λογισμικό, εφικό στην εγκατάσταση και τη συντήρηση.

### 4.1. #####

Το Mailman παρείχει μια διεπαφή Ιστού για τους διαχειριστές και τους χρήστες, και χρησιμοποιεί εξωτερικό εξυπηρετητή για την αποστολή και λήψη email. Συνεργάζεται ψογα 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 επιθυμούμε να εγκαταστήσουμε το Mailman χρησιμοποιώντας διαφορετικό εξυπηρετητή email, παρακαλούμε ανατρέξτε στην ενότητα Αναφορές.



Θα πρέπει να εγκαταστήσετε μνο έναν εξυπηρετητή email, και το Postfix είναι ο προεπιλεγμένος Mail Transfer Agent του Ubuntu.

#### 4.1.1. Apache2

To install apache2 you refer to [μνο 1.1, &#x201C;#####&#x201D; \[194\]](#) for details.

#### 4.1.2. Postfix

Για οδηγίες σχετικές με την εγκατάσταση και ρύθμιση του Postfix δείτε το [μνο 1, &#x201C;Postfix&#x201D; \[249\]](#)

#### 4.1.3. Exim4

Για την εγκατάσταση του Exim4 δείτε το [μνο 2, &#x201C;Exim4&#x201D; \[257\]](#).

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:

<sup>16</sup> <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 χρονοδιάγραμμα `linux list`. Δημιουργεί την ομάδα `linux list`. Η διεργασία του `mailman` ανήκει σε αυτήν το χρονοδιάγραμμα.

### 4.2. #####

Σε αυτή την ενότητα υποθέτουμε ότι έχετε ήδη εγκαταστήσει επιτυχώς τα `mailman`, `apache2` και το `postfix` ή το `exim4`. Θα μπορούσαμε να μην είχαμε ρυθμίσει τους.

#### 4.2.1. Apache2

Το Mailman συμπεριλαμβάνει ένα αρχείο υποδείγματος ρύθμισης του Apache, το `/etc/mailman/apache.conf`. Για να μπορεί 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
```

Τότε, δημιουργείται ένα νέο ##### (VirtualHost) Apache για τον ιστότοπο διαχείρισης του Mailman. Θα μπορούσαμε να ενεργοποιήσουμε τις νέες ρυθμίσεις και να επανεκκινήσουμε 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`. Ή, 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 τι διαθίκετε τον ακόλουθο μεταφορέα (transport):

```
mailman    unix    -    n    n    -    -    pipe
    flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
    ${nexthop} ${user}
```

Κάλεστε 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 χρήτη μεταφορέα (transport map). Τροποποιήστε το αρχείο `/etc/postfix/transport`:

```
lists.example.com    mailman:
```

Τώρα, ζητήστε από το Postfix να δημιουργήσει το χρήτη μεταφορέα, 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. Πώς αναφέρθηκε προηγουμένως, η προεπιλογή του Exim4 είναι να χρησιμοποιεί πολλαπλά αρχεία ρυθμίσεων διαφορετικών τμημάτων. Για περισσότερες λεπτομέρειες, δείτε τον ιστότοπο του Exim<sup>17</sup>. Για το mailman, θα πρέπει να προσθούμε ένα νέο αρχείο ρυθμίσεων στους ακόλουθους τμήματα ρυθμίσεων:

- Main (Κρίσιμος)
- Transport (Μεταφορέας)
- Router (Δρομολογητής)

Το Exim δημιουργεί ένα κεντρικό αρχείο ρυθμίσεων, ταξινομώντας όλα αυτά τα επιμέρους αρχεία ρυθμίσεων. Πρά, η σειρά αυτών των αρχείων παίζει καθοριστικό ρόλο.

<sup>17</sup> <http://www.exim.org>

265

```
user = MM_UID
group = MM_GID
```

#### 4.2.6. Router (###μ#####)

#λα τα αρχε#α ρυθμ#σεων που αν#κουν στον τ#πο `router` αποθηκε#ονται στον κατ#λογο `/etc/exim4/conf.d/router/`. Μπορε#τε να προσθ#σετε τα παρακ#τω σε #να ν#ο αρχε#ο, με #νομα `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 αρχε#α ρυθμ#σεων `main` και `transport` μπορο#ν να τοποθετηθο#ν με οποιαδ#ποτε σειρ#. Ωστ#σο, η σειρ# των αρχε#ων ρυθμ#σεων `router` πρ#πει να ε#ναι η #δια. Το αρχε#ο αυτ# πρ#πει να βρ#σκεται πριν απ# το αρχε#ο `200_exim4-config_primary`. Αυτ# τα δ#ο αρχε#α ρυθμ#σεων περι#χουν τον #διο τ#πο πληροφορι#. Το πρ#το αρχε#ο υπερισχ#ει. Για περισσ#τερες λεπτομ#ρειες, δε#τε την εν#τητα Αναφορ#ς.

#### 4.2.7. Mailman

Αφο# εγκατασταθε# το `mailman`, μπορε#τε να το εκτελ#σετε με την ακ#λουθη εντολ#:

```
sudo service mailman start
```

Αφο# εγκατασταθε# το `mailman`, θα πρ#πει να δημιουργ#σετε την προεπιλεγμ#νη λ#στα ταχυδρομε#ου. Εκτελ#στε την ακ#λουθη εντολ#:

```
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:
```

```
## ##### #####μ##### 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...

#

#χουμε ρυθμ#σει το Postfix # το Exim4 #στε να αναγνωρ#ζουν #λα τα email του mailman. #ρα, δεν ε#ναι υποχρεωτικ# να προσθ#σουμε ν#ες εγγραφ#ς στο /etc/aliases. Αν #χετε κ#νει αλλαγ#ς στα αρχε#α ρυθμ#σεων, φροντ#στε να επανεκκιν#σετε τις αντ#στοιχες υπηρεσιες πριν προχωρ#σετε στην επ#μενη εν#τητα.



Το Exim4 δεν χρησιμοποιε# τα παραπ#νω ψευδ#νυμα (alias) για την προ#θηση email στο Mailman, γιατ# χρησιμοποιε# τη μ#θοδο ##### (discover). Για να απενεργοποι#σετε τα ψευδ#νυμα κατ# τη δημιουργ#α της λ#στας, μπορε#τε να προσθ#σετε τη γραμμ# *MTA=None* στο αρχε#ο ρυθμ#σεων του Mailman, /etc/mailman/mm\_cfg.py.

#### 4.3. #####

Υποθ#τουμε #τι η εγκατ#στασ# σας διαθ#τει τις προεπιλεγμ#νες ρυθμ#σεις. Τα σεν#ρια cgi του mailman βρ#σκονται στον κατ#λογο /usr/lib/cgi-bin/mailman/. Το Mailman παρ#χει #να εργαλε#ο διαχε#ρισης μ#σω Ιστο#. Για να αποκτ#σετε πρ#σβαση στη σελ#δα, εισ#γετε την ακ#λουθη διε#θυνση στον περιηγητ# σας:

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

Η προεπιλεγμ#νη λ#στα ταχυδρομε#ου, η *mailman*, εμφαν#ζεται στην οθ#νη. Αν κ#νετε κλικ στο #νομ# της, θα σας ζητηθε# ο κωδικ#ς πιστοποιησ#ς σας. Αν εισ#γετε το σωστ# κωδικ#, θα σας δοθε# η δυνατ#τητα να αλλ#ξετε τις ρυθμ#σεις διαχε#ρισης αυτ#ς της λ#στας. Μπορε#τε να δημιουργ#σετε ν#α λ#στα ταχυδρομε#ου χρησιμοποι#ντας το εργαλε#ο της γραμμ#ς εντολ#ν(/usr/sbin/newlist). Εναλλακτικ#, μπορε#τε να δημιουργ#σετε ν#α λ#στα ταχυδρομε#ου χρησιμοποι#ντας τη διεπαφ# Ιστο#.

#### 4.4. #####

Το Mailman παρ#χει μ#α διεπαφ# ιστο# για τους χρ#στες. Για να αποκτ#σετε πρ#σβαση στη σελ#δα, εισ#γετε την ακ#λουθη διε#θυνση στον περιηγητ# σας:

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

Η προεπιλεγμ#νη λ#στα ταχυδρομε#ου, η *mailman*, εμφαν#ζεται στην οθ#νη. Αν κ#νετε κλικ στο #νομ# της, θα εμφανιστε# η φ#ρμα εγγραφ#ς συνδρομητ#. Μπορε#τε να εισ#γετε τη διε#θυνση email σας, το #νομ# σας (προαιρετικ#) και τον κωδικ# σας για να εγγραφ#τε

συνδρομητής. Στη συνέχεια, θα σας σταλέι μια πρόσκληση μέσω email. Μπορείτε να ακολουθήσετε τις οδηγίες στην πρόσκληση για να ολοκληρώσετε την εγγραφή σας.

#### 4.5. #####

*GNU Mailman - #####*<sup>18</sup>

*HOWTO - #####μ## Exim 4 ### Mailman 2.1*<sup>19</sup>

Also, see the *Mailman Ubuntu Wiki*<sup>20</sup> page.

---

<sup>18</sup> <http://www.list.org/mailman-install/index.html>

<sup>19</sup> <http://www.exim.org/howto/mailman21.html>

<sup>20</sup> <https://help.ubuntu.com/community/Mailman>



```
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 απ τα σπαμ:

```
sudo apt-get install pyzor razor
```

Πρά απ τις κριες εφαρμογς φίλτραρσματος, για ορισμένα συνημμένα απαιτούνται και εργαλέα συμπέσης:

```
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. μ#####

Τρα, κντε τις απαρατητες ρυθμσεις για να επιτρψετε τη συνεργασα λων των εργαλεων στο φίλτρρισμα του email.

### 5.2.1. ClamAV

Η προεπιλεγμνη συμπεριφορ του ClamAV καλπτει τις ανγκες μας. Για περισστερες επιλογς ρθμισης του ClamAV, ανατρζτε στα αρχεα ρυθμσεων στο `/etc/clamav`.

Προσθστε το χρστη *clamav* στην ομδα *amavis*, #τσι #στε το Amavisd-new να διαθτει πρσβαση για τη σρωση αρχεων:

```
sudo adduser clamav amavis
sudo adduser amavis clamav
```

### 5.2.2. Spamassassin

Το Spamassassin εντοπζει αυτματα και χρησιμοποιε# τα διφορα προαιρετικ# εργαλεα. #ρα, δεν απαιτε#ται ρθμιση των pyzor και razor.

Τροποποι#στε το `/etc/default/spamassassin` για να ενεργοποι#σετε την υπηρεσα Spamassassin. Αλλ#ζτε το `ENABLED=0` σε:

```
ENABLED=1
```

Τρα, εκκιν#στε την υπηρεσα:

```
sudo service spamassassin start
```

### 5.2.3. Amavisd-new

Καταρχής, ενεργοποιήστε τον εντοπισμό σπαμ και ι#ν του Amavisd-new, τροποποιώντας το αρχείο `/etc/amavis/conf.d/15-content_filter_mode:`

```
use strict;

# #####  ## #####  ## #####  ## #####  ## #####  ## #####
# ##  ##  μ## spamassassin, #####  ##  ##  #####μ# ##.

#
# #####μ##  #####  #####  #####
# #####  ##  #####  ##  ##  ##  #####  #####μ##  ##  ##  ##  #####
#

@bypass_virus_checks_maps = (
    \%bypass_virus_checks, \%bypass_virus_checks_acl, \%bypass_virus_checks_re);

#
# #####μ##  #####  #####  ##  ##μ
# #####  ##  #####  ##  ##  ##  #####  #####μ##  ##  ##  ##  #####
#

@bypass_spam_checks_maps = (
    \%bypass_spam_checks, \%bypass_spam_checks_acl, \%bypass_spam_checks_re);

1;  # #####  #####μ#####
```

Η επιστροφή των μηνυμάτων σπαμ στον αποστολέα μπορεί να αποδειχθεί κακή ιδέα, καθώς η διεθυσση 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` (διαγραφά) αντ# για `D_BOUNCE` (επιστροφή), ως εξής:

```
$final_spam_destiny = D_DISCARD;
```

Επιπροσθ#τως, μπορείτε να προσαρμ#σετε τις ακολουθες επιλογ#ς, #στε να σημει#νονται περισσ#τερα μην#ματα ως σπαμ:

```
$sa_tag_level_deflt = -999; # #####  #####  #####  #####μ  ##  ##  ##  #####  ##  ##
$sa_tag2_level_deflt = 6.0; # #####  #####  'spam detected' (#####  #####μ) ##  ##  ##  #####
$sa_kill_level_deflt = 21.0; # #####  #####  #####  #####μ
$sa_dsn_cutoff_level = 4; # #####  #####μ  #####  ##  ##  #####  ##  #####  ##### DSN
```

Αν το ##### του εξυπηρετη# είναι διαφορετικ# απ# την εγγραφ# MX του τομ#α, #σως χρειαστε# να ορίσετε χειροκ#νητα την επιλογ# `$myhostname`. Επιπλ#ον, αν ο εξυπηρετη#

λαμβάνει email για πολλαπλούς τομείς, θα πρέπει να προσαρμόσετε 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. ##### DKIM

Το Amavisd-new μπορεί να ρυθμιστεί έτσι ώστε να προσθεται αυτματα στη ##### τις διευθ#νσεις που προ#ρχονται απ# τομείς με #γκυρά κλειδι# τομ#α (domain keys). Το αρχείο /etc/amavis/conf.d/40-policy\_banks περι#χει ορισμ#νους προκαθορισμ#νους τομείς.

Υπ#ρχουν δι#φοροι τρ#ποι ρ#θμισης της λευκ#ς λ#στας για #να τομ#α:

- 'example.com' => 'WHITELIST': προσθ#τει στη λευκ# λ#στα #λες τις διευθ#νσεις του τομ#α "example.com".
- '.example.com' => 'WHITELIST': προσθ#τει στη λευκ# λ#στα #λες τις διευθ#νσεις των #####μ### του "example.com" που διαθ#τουν #γκυρή υπογραφή.
- '.example.com/@example.com' => 'WHITELIST': προσθ#τει στη λευκ# λ#στα τους υποτομείς του "example.com" που χρησιμοποιο#ν την υπογραφή του γονικο# τομ#α 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 αυτ#ς τις περιπτ#σεις, απ# τη στιγμ# που #νας τομ#ας προσθ#θεται στη λευκ# λ#στα, τα μην#ματ# του δεν φιλτρ#ρονται καθ#λου για σπαμ #ιο#ς. Εσείς αποφασ#ζετε αν αυτ# ε#ναι η συμπεριφορ# που επιθυμ#τε για τον τομ#α.

#### 5.2.4. Postfix

Για το συνδυασμ# με το Postfix, εισ#γ#τε τα ακ#λουθα στο τερματικ#:

```
sudo postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'
```

Τ#ρα, τροποποι#στε το /etc/postfix/master.cf και προσθ#στε τα ακ#λουθα στο τ#λος του αρχ#ου:

```
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
```

Επ#σης, προσθ#στε τις ακ#λουθες δ#ο γραμμ#ς αμ#σως μετ# την υπηρεσ#α μεταφορ#ς "pickup":

```
-o content_filter=
-o receive_override_options=no_header_body_checks
```

#τσι, τα μην#ματα που δημιουργο#νται για την υποβολ# αναφορ#ν για σπαμ δε θα χαρακτηρ#ζονται ως σπαμ.

Τ#ρα επανεκκιν#στε το Postfix:

```
sudo service postfix restart
```

Θα ενεργοποιηθε# το φίλτρ#ρισμα του περιεχομ#νου για τον εντοπισμ# 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. #####

Καταρχής, ελγξτε τι το SMTP του Amavisd-new αφουγκρζεται:

```
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 κεφάλδα των μηνυμάτων που χχουν περσει απ το φλτρο περιεχομνου θα πρπει να εμφανζονται 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 δικ# σας #ξοδος μπορε# να διαφρει, αλλ# το σημαντικ# ε#ναι να υπρχουν οι εγγραφ#ς `X-Virus-Scanned` και `X-Spam-Status`.

### 5.4. #####

Ο καλ#τερος τρ#πος να καταλ#βετε γιατ# κ#τι δεν π#ει καλ# σε περ#πτωση προβλ#ματος ε#ναι να ελγξτε τα αρχε#α καταγραφ#ν.

- Για πληροφορ#ες σχετικ# με τις καταγραφ#ς του Postfix δε#τε την εν#τητα `#μ#μ# 1.7, &#x201C;#####μ#####&#x201D; [254]`.
- Το Amavisd-new χρησημοποιε# το Syslog για να αποστ#λλει μην#ματα στο `/var/log/mail.log`. Το επ#πεδο λεπτομ#ρει#ς τους μπορε# να αυξηθε# αν προστεθε# η επιλογ# `$log_level` στο `/etc/amavis/conf.d/50-user`, και οριστε# η τιμ# της μεταξ# 1 και 5.

```
$log_level = 2;
```



#ταν αυξ#νεται το επ#πεδο καταγραφ#ν του Amavisd-new, αυξ#νεται και το επ#πεδο καταγραφ#ν του Spamassassin.

- Το επ#πεδο καταγραφ#ν του ClamAV μπορε# να αυξηθε# αν τροποποιηθε# το `/etc/clamav/clamd.conf` με προσθ#κη της ακ#λουθης επιλογ#ς:



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 ενεργοποιησετε τις νέες ρυθμίσεις. Επίσης, ήταν επιπλέον το πρόβλημά σας, καλό θα ήταν να επαναφάρετε τις φυσιολογικές ρυθμίσεις των καταγραφών.

## 5.5. #####

Για περισσότερες πληροφορίες σχετικές με τη χρήση φίλτρων email δείτε τους ακόλουθους συνδέσμους:

- ##### *Amavisd-new*<sup>21</sup>
- *ClamAV Documentation*<sup>22</sup> and *ClamAV Wiki*<sup>23</sup>
- *Spamassassin Wiki*<sup>24</sup>
- ##### *Pyzor*<sup>25</sup>
- ##### *Razor*<sup>26</sup>
- *DKIM.org*<sup>27</sup>
- *Postfix Amavis New*<sup>28</sup>

Επίσης, ρωτήστε ελεύθερα στο κανάλι IRC `#ubuntu-server` στο *freenode*<sup>29</sup>.

<sup>21</sup> <http://www.ijs.si/software/amavisd/amavisd-new-docs.html>

<sup>22</sup> <http://www.clamav.net/doc/latest/html/>

<sup>23</sup> <http://wiki.clamav.net/Main/WebHome>

<sup>24</sup> <http://wiki.apache.org/spamassassin/>

<sup>25</sup> <http://sourceforge.net/apps/trac/pyzor/>

<sup>26</sup> <http://razor.sourceforge.net/>

<sup>27</sup> <http://dkim.org/>

<sup>28</sup> <https://help.ubuntu.com/community/PostfixAmavisNew>

<sup>29</sup> <http://freenode.net>

---

## Κεφάλαιο 16. Εφαρμογές συζήτησης

## **1. #####**

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 μέσης ανταλλαγής μηνυμάτων.

## 2. ##### IRC

Το αποθετήριο του Ubuntu #χει πολλούς εξυπηρετητές Internet Relay Chat. Αυτή η ενότητα εξηγεί πώς να εγκαταστήσετε και να ρυθμίσετε τον πρώτο εξυπηρετητή IRC, τον `ircd-irc2`.

### 2.1. #####

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 #γγραφα είναι διαθέσιμα στον κατάλογο `/usr/share/doc/ircd-irc2`.

### 2.2. #####

Οι ρυθμίσεις του IRC μπορούν να γίνουν στο αρχείο ρυθμίσεων `/etc/ircd/ircd.conf`. Σε αυτό το αρχείο μπορείτε να ορίσετε το #νομα τομέα του IRC τροποποιώντας την ακόλουθη γραμμή:

```
M:irc.localhost::Debian ircd default configuration::000A
```

Παρακαλούμε σιγουρευτείτε πως προσθήσατε ψευδ#νυμα (aliases) DNS για το #νομα τομέα του IRC. Για παρ#δειγμα, αν ορίσατε το `irc.livecipher.com` ως το #νομα τομέα του IRC, παρακαλούμε σιγουρευτείτε πως το `irc.livecipher.com` είναι επιλ#σιμο στον εξυπηρετητή ονομάτων τομέα (DNS) σας. Το #νομα τομέα του IRC δεν θα πρέπει να είναι το #διο με το #νομα 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 προσθήσετε συγκεκριμένες γραμμές για την ρ#θμιση της λ#στας των θυρών IRC στις οποίες θα αναμ#νονται συνδ#σεις, να ρυθμίσετε τα πιστοποιητικά των διαχειριστών, να ρυθμίσετε την πιστοπο#ηση πελατών, κτλ. Για λεπτομ#ρείες, παρακαλούμε αναφερθείτε στο παρ#δειγμα αρχείου ρυθμίσεων `/usr/share/doc/ircd-irc2/ircd.conf.example.gz`.

Το λογ#τυπο του IRC που θα εμφαν#ζεται στον πελ#τη IRC, #ταν ο χρ#στής συνδ#εται στον εξυπηρετητή, μπορεί να οριστεί στο αρχείο `/etc/ircd/ircd.motd`.

Αφ# κ#νετε τις απαραίτητες αλλαγές στο αρχείο ρυθμίσεων, μπορείτε να επανεκκιν#σετε τον εξυπηρετητή IRC χρησιμοποιώντας την ακόλουθη εντολή:

```
sudo service ircd-irc2 restart
```

## 2.3. #####

Μπορείτε 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 ### IRCD*<sup>1</sup> για περισσότερες λεπτομέρειες για τον εξυπηρετητή IRC.

---

<sup>1</sup> [http://www.irc.org/tech\\_docs/ircnet/faq.html](http://www.irc.org/tech_docs/ircnet/faq.html)

### 3. ##### μ##### μ##### Jabber

Το *Jabber*, ένα δημοφιλές πρωτόκολλο ανταλλαγής μεσών μηνυμάτων, βασίζεται στο XMPP, ένα ανοιχτό πρότυπο για ανταλλαγή μεσών μηνυμάτων και χρησιμοποιείται από πολλές δημοφιλείς εφαρμογές. Αυτό 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 χρονο σε όλο το διαδίκτυο.

#### 3.1. #####

Για να εγκαταστήσετε το *jabberd2*, πληκτρολογήστε σε ένα τερματικό:

```
sudo apt-get install jabberd2
```

#### 3.2. #####

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, κποιό 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 ρυθμίσετε, δεν χρειάζεται περαιτέρω συντήρηση. Αν χρειάζεστε περισσότερο έλεγχο στους λογαριασμούς και στα πιστοποιητικά των χρηστών, συνιστάται να χρησιμοποιήσετε κάποια άλλη μέθοδο πιστοποίησης.

### 3.3. #####

- Ο ##### *Jabberd2*<sup>2</sup> περιχει περισσότερες λεπτομέρειες για τη ρύθμιση του Jabberd2.
- For more authentication options see the *Jabberd2 Install Guide*<sup>3</sup>.
- Also, the *Setting Up Jabber Server Ubuntu Wiki*<sup>4</sup> page has more information.

---

<sup>2</sup> <http://codex.xiaoka.com/wiki/jabberd2:start>

<sup>3</sup> <http://www.jabberdoc.org/>

<sup>4</sup> <https://help.ubuntu.com/community/SettingUpJabberServer>

---

## Κεφάλαιο 17. Συστήμα Ελέγχου Κόδοσης

Ο έλεγχος κώδωσης είναι η τέχνη του να ελέγχετε αλλαγές στις πληροφορίες. Είναι εδικοί και καιρός να κρυσίμο εργαλειό για προγραμματιστές, που τυπικά περνούν το χρόνο τους κινώντας μικρές αλλαγές σε λογισμικό και μετά αναιρώντας τις την επόμενη μέρα. Αλλά η χρησιμότητα του λογισμικού ελέγχου εκδόσεως επεκτείνεται πέρα από τα όρια του κώδικου ανάπτυξης. που μπορείτε να βρείτε ανθρώπους που χρησιμοποιούν υπολογιστές για να διαχειρίζονται πληροφορίες που αλλάζουν συχνά, υπάρχει χώρος για το έλεγχο κώδωσης.



## 1. Bazaar

Το Bazaar είναι μια καινούρια κώδοση του συστήματος ελέγχου κώδοσης που χορηγείται από την Canonical, τη διαφημιστική εταιρεία πίσω από το Ubuntu. Σε αντίθεση με τα Subversion και CVS που υποστηρίζουν μόνο ένα κεντρικό μοντέλο αποθετηρίου, το Bazaar υποστηρίζει επίσης [αποκεντρωμένα μοντέλα αποθετηρίου](#), δίνοντας τη δυνατότητα πιο αποτελεσματικής διαδικασίας. Συγκεκριμένα, το Bazaar είναι σχεδιασμένο να μεγιστοποιεί το επίπεδο συμμετοχής στην κοινότητα σε ένα ανοιχτό κώδικα.

### 1.1. Εγκατάσταση

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

```
sudo apt-get install bazaar
```

### 1.2. Δημιουργία προφίλ

Για να συστήσετε τον εαυτό σας στο bazaar, χρησιμοποιήστε την εντολή `whoami` έτσι:

```
$ bazaar whoami 'Joe Doe <joe.doe@gmail.com>'
```

### 1.3. Βοήθεια

Το Bazaar [ρχεται με βοηθητικές οδηγίες εγκατεστημένων εξορισμών στο /usr/share/doc/bazaar/html](#). Το εγχειρίδιο οδηγούν είναι ένα καλό μέρος να ξεκινήσετε. Η εντολή `bazaar help` [ρχεται επίσης με ενσωματωμένη βοήθεια](#):

```
$ bazaar help
```

Για να μάθετε περισσότερα για την εντολή `foo`:

```
$ bazaar help foo
```

### 1.4. Ενσωμάτωση με το Launchpad

Εν είναι ιδιαίτερα χρήσιμο σαν ένα αυτόνομο σύστημα, το Bazaar [καλά, προαιρετικά ενσωμάτωση με το Launchpad](#)<sup>1</sup>, 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 πώς μπορεί το Bazaar να χρησιμοποιηθεί με το Launchpad για να συνεργαστούν σε ένα έργο ανοιχτού κώδικα, δείτε το <http://bazaar-vcs.org/LaunchpadIntegration><sup>2</sup>.

<sup>1</sup> <https://launchpad.net/>

<sup>2</sup> <http://bazaar-vcs.org/LaunchpadIntegration/>

## 2. Subversion

Το Subversion είναι μια κώδωση ανοιχτού κώδικα του συστήματος ελέγχου κώδους. Χρησιμοποιώντας το Subversion, μπορείτε να καταγράψετε το ιστορικό αρχείων πηγών και αρχείων. Διαχειρίζεται αρχεία και καταλόγους σε πρόοδο χρόνου. Ένα δέντρο αρχείων τοποθετείτε σε ένα κεντρικό αποθετήριο. Το αποθετήριο είναι σαν ένας κανονικός διακομιστής αρχείων, με τη διαφορά ότι θυμύεται κάθε αλλαγή που γινε σε αρχεία και καταλόγους.

### 2.1. #####

Για να έχετε πρόσβαση στο αποθετήριο του Subversion χρησιμοποιώντας πρωτόκολλο HTTP, πρέπει να εγκαταστήσετε και να διαμορφώσετε έναν διακομιστή ιστο. Ο Apache2 έχει αποδειχθεί ότι δουλεύει με το Subversion. Παρακαλώ αναφερθείτε στην υποενότητα 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 ιστο Apache 2. Παρακαλώ αναφερθείτε στην υποενότητα HTTPS στην ενότητα Apache2 για να εγκαταστήσετε και να διαμορφώσετε το ψηφιακό πιστοποιητικό.

Για να εγκαταστήσετε το Subversion, εκτελέστε την ακόλουθη εντολή απ' ένα τερματικό εντολίν:

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

### 2.2. #####

Αυτή το βήμα υποθέτει ότι έχετε εγκαταστήσει πακέτα που αναφέρθηκαν νωρίτερα στο σύστημά σας. Αυτή η ενότητα εξηγεί πώς να δημιουργήσετε ένα αποθετήριο Subversion και να έχετε πρόσβαση στο ήργο.

#### 2.2.1. ##### Subversion

Το αποθετήριο Subversion μπορεί να δημιουργηθεί χρησιμοποιώντας την ακόλουθη εντολή απ' ένα τερματικό εντολίν:

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

#### 2.2.2. #####

Αφού δημιουργήσετε ένα αποθετήριο μπορείτε να ##### αρχεία στο αποθετήριο. Για να εισήγετε έναν κατάλογο, εισήγετε τα ακόλουθα απ' ένα τερματικό εντολίν:

```
svn import /path/to/import/directory file:///path/to/repos/project
```

## 2.3. #####

Μπορείτε να έχετε πρόσβαση (ελέγξετε) τα αποθετήρια Subversion μέσω πολλών διαφορετικών μεθόδων -- στον τοπικό δίσκο, # μέσω διαφόρων πρωτοκόλλων δικτύου. Μια τοποθεσία αποθετηρίου, #μω, είναι πάντα ένα URL. Ο πίνακας εξηγεί πως διαφορετικές σχήμα URL αντιστοιχούν 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 Subversion-aware Apache2
https://	#μια με http://, αλλά με κρυπτογράφηση SSL
svn://	Πρόσβαση μέσω προσαρμοσμένου πρωτοκόλλου σε έναν διακομιστή svnserve
svn+ssh://	#μια με svn://, αλλά μέσω ενδεδειγμένης 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*<sup>3</sup>.

#### 2.3.1. ##### (file://)

Αυτή είναι η πιο απλή μέθοδος πρόσβασης. Δεν απαιτείται καμία διαδικασία διακομιστή Subversion να εκτελείται. Αυτή η μέθοδος πρόσβασης, αν πληκτρολογηθεί σε ένα τερματικό εντολόν, είναι #πως ακολουθεί:

```
svn co file:///path/to/repos/project
```

```
#
```

```
svn co file://localhost/path/to/repos/project
```



Εάν δεν προσδιορίσετε το όνομα κεντρικού υπολογιστή, υπάρχουν τρεις κθετοί (///) -- δό για το πρωτόκολλο (αρχείο, σε αυτή την περίπτωση) και η πρώτη κθετος στο μονοπάτι. Εάν προσδιορίσετε το όνομα κεντρικού υπολογιστή, πρέπει να χρησιμοποιήσετε δό καθ'τους (/).

Τα δικαιώματα του αποθετηρίου εξαρτώνται απ' τα δικαιώματα του συστήματος αρχείων. Εάν ο χρήστης έχει δικαιώματα ανήγνωσης/επεξεργασίας, μπορεί να ελέγξει και να παραδώσει στο αποθετήριο.

<sup>3</sup> <http://svnbook.red-bean.com/>

### 2.3.2. ##### 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 απίσπασμα διαμρφωσης υποθέτει ότι τα αποθέματα Subversion είναι δημιουργημένα στον κατάλογο `/home/svn/` χρησιμοποιώντας την εντολή **svnadmin**. Μπορούν να είναι προσβίσιμα χρησιμοποιώντας το url `http://hostname/svn/repos_name`.

Για να εισήγεται να παραδσσετε αρχεία στο αποθετήριο Subversion μέσω HTTP, το αποθετήριο θα πρέπει να ανήκει σε ένα χρηστή HTTP. Σε συστήματα Ubuntu, κανονικά ο χρηστής HTTP είναι **www-data**. Για να αλλάξετε την ιδιοκτησία των αρχείων του αποθετηρίου πληκτρολογήστε την ακόλουθη εντολή απ να τερματικό εντολν:

```
sudo chown -R www-data:www-data /path/to/repos
```



Αλλάζοντας την ιδιοκτησία του αποθετηρίου σαν **www-data** δε θα μπορείτε να εισήγεται και να παραδσντε αρχεία στο αποθετήριο εκτελντας την εντολή **svn import file:///** ως οποιοσδήποτε χρηστής του **www-data**.

Μετά, πρέπει να δημιουργήσετε ένα αρχείο `/etc/subversion/passwd` που θα περιχει λεπτομρείες ταυτοποίησης χρηστή. Για να δημιουργήσετε ένα αρχείο χρησιμοποιήστε την ακόλουθη εντολή σε ένα τερματικό εντολν (η οποα θα δημιουργήσει το αρχείο και θα προσθσει τον πρώτο χρηστή):

```
sudo htpasswd -c /etc/subversion/passwd user_name
```

Για να προσθσετε επιπλόν χρηστές παραλέψτε την επιλογή `"-c"` καθώς αυτ η επιλογή αντικαθιστ το παλιό αρχείο. Αυτ αυτς χρησιμοποιήστε αυτ τη μορφή:

```
sudo htpasswd /etc/subversion/passwd user_name
```

Αυτ η εντολ θα σας ζητήσει να εισήγεται τον κωδικ. Όταν εισήγεται τον κωδικ, ο χρηστής προσθθεται. Τώρα, για να ήγεται πρσβάση στο αποθετήριο μπορείτε να εκτελέσετε την ακόλουθη εντολ:

```
svn co http://servername/svn
```



Ο κωδικός μεταδίδεται σαν απλός κείμενο. Εάν ανησυχείτε για κατασκήπηση κωδικού, συνιστάται να χρησιμοποιήσετε κρυπτογράφηση SSL. Για λεπτομρείες, παρακαλώ αναφερθείτε στην επόμενη ενότητα.

### 2.3.3. ##### WebDAV με ##### 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 πώς να στήσετε τον Apache2 με SSL δείτε [#1.3, &#x201C;##### HTTPS&#x201D; \[201\]](#).

Μπορείτε να εγκαταστήσετε ψηφιακό πιστοποιητικό που έχουν εκδοθεί από μια αρχή υπογραφής. Εναλλακτικά, μπορείτε να εγκαταστήσετε τα δικά σας αυτό 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. ##### (svn://)

Όταν δημιουργήθει 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 σχήλια των ακόλουθων γραμμών στο αρχείο διαμόρφωσης:

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

Αφού διαγράψετε τα σχήλια στις παραπάνω γραμμές, μπορείτε να διατηρήσετε τη λίστα χρηστών στο αρχείο `passwd`. #τσι, επεξεργαστείτε το αρχείο `passwd` στον ίδιο κατάλογο και προσθέστε τον καινούριο χρήστη. Η σήνταξη είναι #πως ακολούθως:

```
username = password
```

Για περισσότερες λεπτομρείες, παρακαλώ αναφερθείτε στο αρχείο.

Τώρα, για πρόσβαση του Subversion μέσω του προσαρμοσμένου πρωτοκόλλου `svn://`, έχετε από την διαμηνχαν# από διαφορετικά, μπορείτε να εκτελέσετε το `svnserver` χρησιμοποιώντας την εντολή `svnserve`. Η σήνταξη είναι #πως ακολούθως:

```
$ svnserve -d --foreground -r /path/to/repos
# -d -- #####
# --foreground -- ##### (#####)
# -r -- #####
```

```
### #####, #####
$ svnserve --help
```

Το Subversion αρχίζει να ακούει στην προεπιλεγμένη θύρα (3690). Για να έχετε πρόσβαση στο αποθετήριο του #ργου, πρέπει να εκτελέσετε την ακόλουθη εντολή απ# να τερματίσετε την εντολή:

```
svn co svn://hostname/project project --username user_name
```

Βήμα της διαμόρφωσης του διακομιστή, ζητείται κωδικ#. Το πιστοποιήσετε την ταυτότητάς σας, ελέγχει τον κωδικά απ# το αποθετήριο Subversion. Για να συγχρονίσετε το αποθετήριο του #ργου με το τοπικό αντίγραφο, μπορείτε να εκτελέσετε την υποεντολή **update**. Η σήνταξη της εντολής, αν πληκτρολογήσετε σε ένα τερματικό, είναι όπως ακολούθε:

```
cd project_dir ; svn update
```

Για περισσότερες λεπτομέρειες για το πως να χρησιμοποιήσετε κάθε υποεντολή Subversion, μπορείτε να αναφερθείτε στο εγχειρίδιο. Για παράδειγμα, για να μ#θετε περισσότερα για την εντολή **co** (checkout) παρακαλώ εκτελέστε την ακόλουθη εντολή απ# να τερματίσετε την εντολή:

```
svn co help
```

### 2.3.5. ##### μ### ##### μ# ##### SSL (svn+ssh://)

Η διαμόρφωση και η διαδικασία διακομιστή είναι ίδιες με τη μέθοδο **svn://**. Για λεπτομέρειες, παρακαλώ αναφερθείτε στην παραπ#νω ενότητα. Αυτή το βήμα υποθέτει ότι έχετε ακολουθήσει τα παραπ#νω 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 #λά 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 μεταφορές είναι κρυπτογραφημένα χρησιμοποιώντας αυτή τη μέθοδο. Για να έχετε πρόσβαση στο αποθετήριο του #ργου (για παράδειγμα με **checkout**), πρέπει να χρησιμοποιήσετε τη σήνταξη 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.

Βση της διαμόρφωσης του διακομιστή, ζητείται κωδικός. Πρέπει να εισάγετε τον κωδικό που χρησιμοποιείτε για να εισέλθετε μέσω <sup>ssh</sup>. Μην πιστοποιήσετε την ταυτότητά σας, ελέγχει τον κώδικα από το αποθετήριο Subversion.

### 3. ##### CVS

Το CVS είναι ένα σύστημα ελέγχου έκδοσης. Μπορείτε να το χρησιμοποιείτε για να καταγράφετε το ιστορικό αρχείων πηγής.

#### 3.1. #####

Για να εγκαταστήσετε το CVS, εκτελέστε την ακόλουθη εντολή απ' το τερματικό εντολήν:

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

Αφ' εγκαταστήσετε το CVS, πρέπει να εγκαταστήσετε το xinetd για να εκκινείτε/τερματίζετε το διακομιστή CVS. Ήταν σας ζητηθεί, εισήγετε την ακόλουθη εντολή για να εγκαταστήσετε το xinetd:

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

#### 3.2. #####

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 τι 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 κτι 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 ανεξαρτήτως από την υποκειμενική εγκατάσταση λειτουργικού συστήματος. Πιθανόν ο πιο εύκολος τρόπος είναι να χρησιμοποιήσετε Χρήστες Linux για CVS, παρόλο που έχει πιθανά θύματα ασφαλείας. Παρακαλώ αναφερθείτε στο εγχειρίδιο CVS για λεπτομέρειες.

### 3.3. #####

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 βήσης CVS. Όταν έχετε της μεταβλητής περιβάλλοντος CVSROOT, μπορείτε να αποφεύγετε 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. #####**

##### *Bazaar*<sup>4</sup>

#####<sup>5</sup>

##### *Subversion*<sup>6</sup>

##### *Subversion*<sup>7</sup>

##### *CVS*<sup>8</sup>

*Easy Bazaar Ubuntu Wiki page*<sup>9</sup>

*Ubuntu Wiki Subversion page*<sup>10</sup>

---

<sup>4</sup> <http://bazaar.canonical.com/en/>

<sup>5</sup> <https://launchpad.net/>

<sup>6</sup> <http://subversion.tigris.org/>

<sup>7</sup> <http://svnbook.red-bean.com/>

<sup>8</sup> [http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs\\_toc.html](http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs_toc.html)

<sup>9</sup> <https://help.ubuntu.com/community/EasyBazaar>

<sup>10</sup> <https://help.ubuntu.com/community/Subversion>

---

## Κεφάλαιο 18. Samba

Τα δίκτυα υπολογιστών συχνά αποτελούνται από διαφορετικά συστήματα, και ενδέχεται να λειτουργικά δίκτυο που αποτελείται εξ ολοκλήρου από υπολογιστές desktop και server Ubuntu θα ήταν σίγουρα διασκεδαστικό, μερικά περιβλλοντας 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. #####

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 σχετικών με τους υπολογιστές και τους χρήστες που συμμετέχουν στο δίκτυο, και μπορούν να ταξινομηθούν σε τρεις μεγάλες κατηγορίες λειτουργιών:

- Υπηρεσία Διαμορφώσεως Αρχείου και Εκτυπωτή· Χρησιμοποίηση του πρωτοκόλλου Server Message Block (SMB) για τη διευκλίνηση της ανταλλαγής αρχείων, φακέλων, τμημάτων, καθώς και την απήκοοι των εκτυπωτών σε όλο το δίκτυο.
- Υπηρεσίες Κατάλογου· 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 του δικτύου και καθορισμός της πληροφορίας ο υπολογιστής ο χρήστης επιτρέπεται να έχει πρόσβαση χρησιμοποιώντας αρχές και τεχνολογίες όπως δεικνύουν αρχείων, πολιτικές ομμάτων, και την υπηρεσία ελέγχου ταυτότητας Kerberos.

Εντυχώς, το Ubuntu στήμα σας μπορεί να παρέχει όλες αυτές τις εγκαταστάσεις για να τους πελάτες των Windows και να μοιράζει πόρους δικτύου μεταξύ τους. #να απ τα κρία κομμάτια του λογισμικού που περιλαμβάνει το στήμα 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 απ τις συνθεις περιπτώσεις χρήσης Samba, και πς να εγκαταστήσετε και να ρυθμίσετε τα απαραίτητα πακέτα. Πρόσθετες λεπτομερές βοηθητικές οδηγίες και πληροφορίες για το Samba μπορούν να βρεθούν στο *Samba website*<sup>1</sup>.

---

<sup>1</sup> <http://www.samba.org>

## 2. File Server

Ένας από τους πιο σνηθές 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 ζητεί κωδικό πρόσβασης. Είναι το περιβάλλον σας απαιτείται πιο αυστηρή #λεγχό Εισόδου βλ. #μ#μ# 4, &#x201C;Securing File and Print Server&#x201D; [300]

### 2.1. #####

Το πρώτο βήμα είναι να εγκαταστήσετε το πακέτο `samba`. Από ένα τερματικό εντολές πληκτρολογήστε:

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

Αυτή είναι #λο, έχετε τώρα #τοίμη να ρυθμίσετε το Samba να διαμοιράζει αρχεία.

### 2.2. ##μ#####

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 #λες οι διαθέσιμες επιλογές στο αρχικό αρχείο ρυθμίσεων. Βλ#πε τη σελ#δα `smb.confman` # *Samba HOWTO Collection*<sup>2</sup> για περισσότερες πληροφορίες.

1. Πρώτον, επεξεργαστείτε τα ακόλουθα ζεύγη κλειδών / τιμών στον τομέα `[global]` του `/etc/samba/smb.conf`:

```
workgroup = EXAMPLE
...
security = user
```

Η παράμετρος `security` είναι πιο κάτω στον τομέα `[global]`, και σχολιζετε με προεπιλογή. Επ#σης, αλλάξτε το `EXAMPLE` ώστε να ταιριάζει καλύτερα με το περιβάλλον σας.

2. Δημιουργήστε ένα κενό τμήμα στο κάτω μέρος του αρχείου, # διαγράψτε το σχ#λιο κ#ποιου από τα παραδείγματα, για να μοιράζεται ο κατάλογος.

```
[share]
comment = Ubuntu File Server Share
```

<sup>2</sup> <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`<sup>3</sup> εκεί πρέπει να εξυπηρετούνται πληροφορίες σχετικές με `site`. Τεχνικές διαμοιραζόμενα του Samba μπορούν να τοποθετηθούν οπουδήποτε στο σύστημα αρχείων αρκεί τα δικαιώματα να είναι σωστά, αλλά συνιστάται 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 κοινά χρήστα χωρίς να παρέχουν έναν κωδικό.
  - *read only*: καθορίζει εάν το διαμοιραζόμενο είναι μόνο για ανάγνωση ή αν παρέχονται προνμία επεξεργασίας. Τα προνμία επεξεργασίας παρέχονται μόνο όταν η τιμή είναι `###`, όπως φαίνεται σε αυτό το παράδειγμα. Εάν η τιμή είναι `###`, τότε η πρόσβαση στο διαμοιραζόμενο είναι μόνο για ανάγνωση.
  - *create mask*: καθορίζει τις δειξ που θα έχουν τα καινούρια αρχεία όταν δημιουργηθούν.
3. Τώρα που το Samba έχει ρυθμιστεί, ο κατάλογος πρέπει να δημιουργηθεί και η δειξ να αλλάχουν. Απλά να τερματίσουμε πλήκτρολογώντας:

```
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, επανεκκινάμε των υπηρεσιών του `samba` για να ενεργοποιηθούν οι νέες ρυθμίσεις:

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



Για άλλη μια φορά, η ανώτερη ρύθμιση δίνει πρόσβαση σε κάθε πελάτη του τοπικού δικτύου. Για μια πιο ασφαλή ρύθμιση βλ. [μύθος 4, &#x201C;Securing File and Print Server&#x201D; \[300\]](#).

<sup>3</sup> <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 απλώς δημιουργήστε καινούρια τμήματα *[dir]* στο `/etc/samba/smb.conf`, και επανεκκινήστε το *Samba*. Απλώς σιγουρευτείτε ότι ο κατ'λογος που θέλετε να μοιραστείτε υπάρχει και οι δεικτές είναι σωστούς.



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. #####

- Για διαμορφώσεις του *Samba* σε βήθος δείτε το *Samba HOWTO Collection*<sup>4</sup>
- Ο οδηγός είναι επής διαθσιμος σε ##### μ#####<sup>5</sup>.
- #####μ##### ## *Samba*<sup>6</sup> του O'Reilly είναι #λλη μια καλ# παραπομπ#.
- Η σελ#δα wiki του *Ubuntu* ## ## *Samba* <sup>7</sup>.

---

<sup>4</sup> <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/>

<sup>5</sup> <http://www.amazon.com/exec/obidos/tg/detail/-/0131882228>

<sup>6</sup> <http://www.oreilly.com/catalog/9780596007690/>

<sup>7</sup> <https://help.ubuntu.com/community/Samba>

### 3. #####

Μια άλλη κοινή χρήση του Samba είναι η διαμόρφωση του ώστε να διαμοιράζει εγκατεστημένους εκτυπωτές είτε τοπικά είτε μέσω του διαδικτύου, σε έναν διακομιστή Ubuntu. Παρόμοια με το [#2, &#x201C;File Server&#x201D; \[295\]](#) αυτό το τμήμα θα διαμορφώσει το Samba ώστε να επιτρέπει σε κάθε πελάτη στο τοπικό δίκτυο να χρησιμοποιεί τους εγκατεστημένους εκτυπωτές χωρίς να ζητά νόμο χρήστη και κωδικ πρόσβασης.

Για μια πιο ασφαλής διαμόρφωση βλ. [#4, &#x201C;Securing File and Print Server&#x201D; \[300\]](#).

#### 3.1. #####

Πριν εγκαταστήσετε και διαμορφώσετε το Samba είναι καλό να έχετε ήδη μια λειτουργική εγκατάσταση CUPS. Δείτε [#4, &#x201C;CUPS - #####&#x201D; \[245\]](#) για λεπτομέρειες.

Για να εγκαταστήσετε το πακέτο `samba`, απλά τερματικό πληκτρολογήστε:

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

#### 3.2. #####

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 [#####](#) 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. #####

- Για διαμορφώσεις του Samba σε β#θος δε#τε το *Samba HOWTO Collection*<sup>8</sup>
- Ο οδηγ#ς ε#ναι επ#σης διαθ#σιμος σε ##### μ####<sup>9</sup>.
- #####μ##### ## Samba<sup>10</sup> του O'Reilly ε#ναι #λλη μια καλ# παραπομπ#.
- Επ#σης δε#τε το *CUPS Website*<sup>11</sup> για περισσ#τερες πληροφορ#ες για τη διαμ#ρφωση CUPS.
- Η σελ#δα wiki του *Ubuntu ### ## Samba*<sup>12</sup>.

---

<sup>8</sup> <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/>

<sup>9</sup> <http://www.amazon.com/exec/obidos/tg/detail/-/0131882228>

<sup>10</sup> <http://www.oreilly.com/catalog/9780596007690/>

<sup>11</sup> <http://www.cups.org/>

<sup>12</sup> <https://help.ubuntu.com/community/Samba>

## 4. Securing File and Print Server

### 4.1. ##### Samba

Υπάρχουν δύο επίπεδα ασφάλειας διαθσιμα στο πρωτοκόλλο δικτύου Common Internet Filesystem (CIFS) *user-level* και *share-level*. Η εκτέλεση της *security mode* του Samba επιτρέπει μεγαλύτερη ευελιξία, παρόντας τσσερις τρπους εφαρμογς ασφάλειας επιπδουχρστη και #ναν τρπο εφαρμογς επιπδουδιαμοιρασμο#:

- *security = user*: απαιτε# απ# τους πελ#τες να παρ#χουν #να #νομα χρ#στη και κωδικ# πρ#σβασης για να συνδεθον# στα διαμοιραζ#μενα. Οι λογαριασμο# χρ#στην του Samba ε#ναι διαφορετικο# απ# τους λογαριασμο#ς συστ#ματος, αλλ# το πακ#το libpam-smbpass θα συγχρον#σει τους χρ#στες και τους κωδικο#ς συστ#ματος με τη β#ση δεδομ#νων χρ#στην του Samba.
- *security = domain*: αυτ# η κατ#σταση επιτρ#πει στο διακομιστ# του Samba να εμφαν#ζεται στους πελ#τες των Windows σαν Πρωτεον Ελεγκτ#ς Τομ#α (Primary Domain Controller (PDC)), Εφεδρικ#ςΕλεγκτ#ς Τομ#α (Backup Domain Controller (BDC)), # Τμ#μα Μ#λους Διακομιστ# (Domain Member Server (DMS)). Δε#τε #μ#μ# 5, &#x201C;As a Domain Controller&#x201D; [305] για περισσ#τερες πληροφορ#ες.
- *security = ADS*: επιτρ#πει στο διακομιστ# Samba να συνδεθε# στον τομ#α Ενεργο# Καταλ#γου σαν #να ιθαγεν#ς μ#λος. Δε#τε #μ#μ# 6, &#x201C;Active Directory Integration&#x201D; [310] για λεπτομ#ρειες.
- *security = server*: αυτ# η κατ#σταση #χει απομ#νει απ# τ#τε που το samba δεν μπορο#σε να #νει μ#λος εν#ς διακομιστ#, και εξαιτ#ας ορισμ#νων θεμ#των ασφαλε#ας δεν πρ#πει να χρησιμοποιε#ται. Δε#τε το τμ#μα του οδηγου# Samba##### μ#####<sup>13</sup> για περισσ#τερες πληροφορ#ες.
- *security = share*: επιτρ#πει στους πελ#τες να συνδεθον# στα διαμοιραζ#μενα χωρ#ς να παρ#χουν #να #νομα χρ#στη και κωδικ# πρ#σβασης.

Η κατ#σταση ασφαλε#ας που επιλ#γεται θα βασ#ζεται στο περιβ#λλον σας και στο τι χρει#ζεστε να πετ#χει ο διακομιστ#ς Samba.

### 4.2. Security = User

Αυτ# το τμ#μα θα επαναδιαμορφ#σει το αρχε#ο και το διακομιστ# εκτυπωτ# Samba, απ# #μ#μ# 2, &#x201C;File Server&#x201D; [295] και #μ#μ# 3, &#x201C;##### μ#####&#x201D; [298], #στε να απαιτε# πιστοπο#ηση.

Πρ#τον, εγκαταστ#στε το πακ#το libpam-smbpass το οπο#ο θα συγχρον#σει τους χρ#στες του συστ#ματος στη β#ση δεδομ#νων χρ#στην του Samba:

<sup>13</sup> <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html#id349531>

```
sudo apt-get install libpam-smbpass
```



Εν επιλ#ξάτε τη διεργασ#α #####μ##### Samba κατ# τη δι#ρκεια της εγκατ#στασης τ#τε το libpam-smbpass ε#ναι #δη εγκατεστημ#νο.

Επεξεργαστε#τε το `/etc/samba/smb.conf`, και στον τομ#α [#####μ####] αλλ#ξτε:

```
guest ok = no
```

Τ#λος, επανεκκιν#στε το Samba για να τεθο#ν σε ισχ# οι ν#ες ρυθμ#σεις:

```
sudo restart smbd
```

```
sudo restart nmbd
```

Τ#ρα #ταν συνδ#εστε στους κοιν#χρηστους καταλ#γους # εκτυπωτ#ς θα σας ζητε#ται #νομα χρ#στης και κωδικ#ς.



Αν επιλ#ξετε να αντιστοιχ#σετε μια μον#δα δ#σκου στο διαμοιραζ#μενο μπορε#τε να τσεκ#ρετε το κουτ# επιλογ#ς &##201#;Επανασ#νδεση κατ# την Ε#σοδο&##201#;· το οπο#ο θα σας ζητ#σει να εισ#γετε το #νομα χρ#στη και τον κωδικ# πρ#σβασης μ#α φορα, τουλ#χιστον μ#χρι να αλλ#ξει ο κωδικ#ς.

#### 4.3. #####μ#####μ#####

Υπ#ρχουν πολλ#ς διαθ#σιμες επιλογ#ς για να αυξ#σετε την ασφ#λεια για κ#θε μεμονωμ#νο κοιν#χρηστο κατ#λογο. Χρησιμοποι#ντας το παρ#δειγμα [share], αυτ# το τμ#μα θα καλυψει ορισμ#νες κοιν#ς επιλογ#ς.

##### 4.3.1. #μ#####

Οι ομ#δες ορ#ζουν μια συλλογ# απ# υπολογιστ#ς # χρ#στες οι οπο#οι #χουν #να κοιν# επ#πεδο πρ#σβασης σε συγκεκριμ#νους π#ρους δικτ#ου και προσφ#ρουν #να επ#πεδο διακριτ#τητας για τον #λεγχο της πρ#σβασης σε αυτο#ς τους π#ρους. Για παρ#δειγμα, αν μια ομ#δα *qa* ορ#ζεται και περι#χει τους χρ#στες *freda*, *danika*, και *rob* και μια δε#τερη ομ#δα *support* #χει οριστε# και περι#χει τους χρ#στες *danika*, *jeremy*, και *vincent* τ#τε συγκεκριμ#νοι π#ροι του δικτ#ου διαμορφωμ#νοι για να επιτρ#πουν την ε#σοδο στην ομ#δα *qa* ακολο#θως θα επιτρ#ψει την ε#σοδο στους *freda*, *danika*, και *rob*, αλλ# #χι στους *jeremy* # *vincent*. Δεδομ#νου #τι ο χρ#στης *danika* αν#κει και στην ομ#δα *qa* και στην *support*, θα μπορε# να χρησιμοποιε# π#ρους διαμορφωμ#νους για πρ#σβαση και απ# τις δ#ο ομ#δες, εν# #λοι οι #λλοι χρ#στες #χουν πρ#σβαση μ#νο σε π#ρους που επιτρ#πουν πρ#σβαση στην ομ#δα στην οπο#α αν#κουν.

Απ# προεπιλογ# το Samba αναζητ# τις τοπικ#ς ομ#δες συστ#ματος που ορ#ζονται στο `/etc/group` για να καθορ#σει ποιοι χρ#στες αν#κουν σε ποιες ομ#δες. Για περισσ#τερες πληροφοριες για εισαγωγ# και διαγραφ# χρηστ#ν απ# ομ#δες βλ. #μ#μ# 1.2, &#x201C;##### ##&#x201D; [157].

#ταν ορ#ζετε ομ#δες στο αρχε#ο διαμ#ρφωσης του Samba, `/etc/samba/smb.conf`, η αναγνωρισμ#νη σ#νταξη ε#ναι να προλογ#σετε το #νομα της ομ#δας με #να σ#μβολο "@" . Για παρ#δειγμα, ε#ν επιθυμο#σατε να ορ#σετε μια ομ#δα με #νομα *sysadmin* σε #να συγκεκριμ#νο τμ#μα του `/etc/samba/smb.conf`, θα το κ#νατε εισ#γοντας το #νομα της ομ#δας ως **@sysadmin**.

#### 4.3.2. #####

Οι #δεις Αρχε#ων ορ#ζουν τα σαφ# δικαι#ματα που #χει #νας υπολογιστ#ς # χρ#στης σε #ναν συγκεκριμ#νο κατ#λογο, αρχε#ο, # σ#νολο αρχε#ων. Τ#τοιες #δεις μπορο#ν να οριστο#ν κ#νοντας επεξεργασ#α του αρχε#ου `/etc/samba/smb.conf` και ορ#ζοντας τις σαφε#ς #δεις εν#ς ορισμ#νου διαμοιρασμ#νου αρχε#ου.

Για παρ#δειγμα, ε#ν #χετε ορ#σει #να διαμοιρασμ#νο του Samba με #νομα *share* και επιθυμε#τε να δ#σετε #δεις *read-only* στην ομ#δα χρηστ#ν γνωστ#ν ως *qa*, αλλ# θ#λετε να επιτρ#πετε την επεξεργασ#α του διαμοιραζ#μενου απ# την ομ#δα που ονομ#ζεται *sysadmin* και τον χρ#στη με #νομα *vincent*, τ#τε θα μπορο#σατε να επεξεργαστε#τε το αρχε#ο `/etc/samba/smb.conf`, και να εισ#γετε τις ακ#λουθες τιμ#ς κ#τω απ# την εγγραφ# [*share*]:

```
read list = @qa
write list = @sysadmin, vincent
```

Μια #λλη πιθαν# #δεια του Samba ε#ναι να δηλ#σετε δικαι#ματα ##### σε #να συγκεκριμ#νο διαμοιρασμ#νο π#ρο. Οι χρ#στες που #χουν δικαι#ματα διαχειριστ# μπορο#ν να διαβ#σουν, να επεξεργαστο#ν και τροποποι#σουν κ#θε πληροφορ#α που περι#χεται στον π#ρο για τον οπο#ο #χουν δοθε# στο χρ#στη σαφ# δικαι#ματα διαχειριστ#.

Για παρ#δειγμα, ε#ν θ#λετε να δ#σετε στο χρ#στη *melissa* δικαι#ματα διαχειριστ# για το παρ#δειγμα *share*, θα επεξεργαζ#ασταν το αρχε#ο `/etc/samba/smb.conf`, και θα εισ#γατε την ακ#λουθη γραμμ# κ#τω απ# την εγγραφ# [#####μ###] :

```
admin users = melissa
```

Αφο# επεξεργαστε#τε το `/etc/samba/smb.conf`, επανεκκιν#στε το Samba για να εφαρμοστο#ν οι αλλαγ#ς:

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



Για να δουλ#ψουν οι ##### και ##### η κατ#σταση ασφαλε#ας του Samba ### πρ#πει να καθοριστε# σε ##### = #####μ###

Τ#ρα που το Samba #χει ρυθμιστε# #τσι #στε να περιορ#σει ποιες ομ#δες #χουν πρ#σβαση στο κοιν#χρηστο κατ#λογο, θα πρ#πει τα δικαι#ματα του συστ#ματος αρχε#ου να ενημερωθο#ν.

Τα παραδοσιακά δικαιώματα αρχών 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 παρόντας καλύτερο έλεγχο. Για παράδειγμα, για να ενεργοποιήσετε τις ACLs στο `/srv` να αρχίσει ο συστήματος EXT3, επεξεργαστείτε το `/etc/fstab` εισάγοντας την επιλογή `acl`:

```
UUID=66bcd2e-8861-4fb0-b7e4-e61c569fe17d /srv ext3 noatime,relatime,acl 0 1
```

Μετά κνίτε ξανά `mount` το διαμρίσμα:

```
sudo mount -v -o remount /srv
```



Το παραπάνω παράδειγμα υποθέτει το `/srv` σε διαφορετικό διαμρίσμα. Εάν το `/srv`, # που άλλο #χετε 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 ανγνώσης, επεξεργασίας και εκτύπωσης στο `/srv/samba/share`, στην ομάδα `qa` θα δοθούν δικαιώματα ανγνώσης και εκτύπωσης, και τα αρχεία θα ανήκουν στο νόμα 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 ##### σε όλα τα αρχεία του καταλόγου `/srv/samba/share`, κνί το οποίο μπορεί να θέλετε # να μην θέλετε.

Τώρα απ #ναν πελάτη των Windows θα πρέπει παρατηρήσετε τι τα νέα δικαιώματα αρχών είναι σε εφαρμογή. Δείτε τις σελίδες `acl` και `setfacl` για περισσότερες πληροφορίες πάνω στις POSIX ACLs.

#### 4.4. ##### Samba AppArmor

Το Ubuntu #ρχεται με την υπομονάδα ασφαλείας AppArmor, η οποία παρχει υποχρεωτικούς ελέγχους πρόσβασης. Το προεπιλεγμένο προφλ AppArmor για το Samba θα χρειαστεί να προσαρμόσετε στη ρύθμισή σας. Για περισσότερες πληροφορίες στο πώς να χρησιμοποιήσετε το AppArmor βλ. #μ#μ# 4, &#x201C;AppArmor&#x201D; [171].

Υπάρχουν προεπιλεγμένα προφλ 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, απ #να τερματικό εντολήν πληκτρολογήστε:

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



Αυτ# το πακ#το περι#χει προφ#λ για πολλ# #λλα binaries.

Απ# προεπιλογ# τα προφ#λ για τα `smbd` και `nmbd` βρ#σκονται σε κατ#σταση *complain* επιτρ#ποντας στο Samba να δουλε#ει χωρ#ς να τροποποιε# το προφ#λ, και μ#νο να καταγρ#φει σφ#λματα. Για να τοποθετ#σετε το προφ#λ `smbd` σε κατ#σταση *enforce*, και να δουλε#ει το Samba #πως αναμ#νεται, το προφ#λ θα χρειαστε# να επεξεργαστε# #στε να αντικατοπτρ#ζει #λους τους καταλ#γους που χρησιμοποιο#νται.

Επεξεργαστε#τε το `/etc/apparmor.d/usr.sbin.smbd` εισ#γοντας πληροφορ#ες για *[share]* απ# το αρχε#ο παραδε#γματος του διακομιστ#:

```
/srv/samba/share/ r,
/srv/samba/share/** rwkix,
```

Τ#ρα τοποθετ#στε το προφ#λ σε κατ#σταση *enforce* και επαναφορτ#στε το:

```
sudo aa-enforce /usr/sbin/smbd
cat /etc/apparmor.d/usr.sbin.smbd | sudo apparmor_parser -r
```

Θα πρ#πει τ#ρα να μπορε#τε να διαβ#σετε, να επεξεργαστε#τε και να εκτελ#σετε αρχε#α στον κοιν#χρηστο κατ#λογο #πως π#ντα, και το binary `smbd` θα #χει πρ#σβαση μ#νο σε ρυθμισμ#να αρχε#α και καταλ#γους. Σιγουρευτε#τε να εισ#γετε εγγραφ#ς για κ#θε κατ#λογο που ρυθμ#ζετε για να διαμοιρ#σει το Samba. Επ#σης, #ποια λ#θη θα καταγραφο#ν στο `/var/log/syslog`.

#### 4.5. #####

- Για διαμορφ#σεις του Samba σε β#θος δε#τε το *Samba HOWTO Collection*<sup>14</sup>
- Ο οδηγ#ς ε#ναι επ#σης διαθ#σιμος σε ##### μ#####<sup>15</sup>.
- Το #####μ##### ## *Samba*<sup>16</sup> του O'Reilly ε#ναι μια καλ# παραπομπ#.
- Το ##### 18<sup>17</sup> του Samba HOWTO Collection ε#ναι αφιερωμ#νο στην ασφ#λεια.
- Για περισσ#τερες πληροφορ#ες για το Samba και το ACLs δε#τε το *Samba ACLs page*<sup>18</sup>.
- Η σελ#δα wiki του *Ubuntu ### ## Samba*<sup>19</sup>.

<sup>14</sup> <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/>

<sup>15</sup> <http://www.amazon.com/exec/obidos/tg/detail/-/0131882228>

<sup>16</sup> <http://www.oreilly.com/catalog/9780596007690/>

<sup>17</sup> <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/securing-samba.html>

<sup>18</sup> <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/AccessControls.html#id397568>

<sup>19</sup> <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 συστήματα Windows NT4. Η μέζωση πλέονκτημα αυτής της ρύθμισης είναι η ικανότητα να συγκεντρώνει τις πιστοποιήσεις του χρήστη και της μηχανής. Το Samba μπορεί επίσης να χρησιμοποιήσει πολλαπλά προγράμματα υποστήριξης για να αποθηκεύει τις πληροφορίες του χρήστη.

### 5.1. ##### μ##

Αυτή η ενότητα καλύπτει τη ρύθμιση του Samba σαν ένα Κόριο Ελεγκτή Τομέα (Primary Domain Controller (PDC)) χρησιμοποιώντας το προεπιλεγμένο πρόγραμμα υποστήριξης smbpasswd.

1. Πρώτον, εγκαταστήστε τα Samba, και libpam-smbpass για να συγχρονίσετε τους λογαριασμούς χρήστη, πληκτρολογώντας τα ακόλουθα σε ένα τερματικό εντολόν:

```
sudo apt-get install samba libpam-smbpass
```

2. Μετά, ρυθμίστε το Samba τροποποιώντας το `/etc/samba/smb.conf`. Η κατάσταση ##### θα πρέπει να τεθεί σε #####, και η ##### θα πρέπει να ταιριάζει στον οργανισμό σας:

```
workgroup = EXAMPLE
...
security = user
```

3. In the commented `&#x201C;Domains&#x201D;` 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* αφαιρέστε τις επιλογές *logon home* και *logon path* με σχήλια.

- *domain logons*: παρήχει 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 να διαμοιραστεί [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 χρήστης 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` δετέ το `#μ#μ# 1.2, &#x201C;##### ###` `##### &#x201D; [157]` για λεπτομέρειες.

4. Διαγράψτε τα σχήλια 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 να διαμοιραστεί [netlogon] χρειάζεται να ρυθμιστεί. Για να ενεργοποιήσετε το διαμοιρασμένο, διαγράψτε τα σχήλια:

```
[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 Πρωτογενή Ιεραρχία Αρχείων Συστήματος (Filesystem Hierarchy Standard (FHS)), `/srv`<sup>20</sup> είναι η σωστή τοποθεσία για δεδομένα σχετικά με site που παρέχεται από το σύστημα.

6. Θα πρέπει να δημιουργήσετε τον κατάλογο `netlogon`, και να δείτε (για τήρα) αρχείο σεναρίου `logon.cmd`:

```
sudo mkdir -p /srv/samba/netlogon
```

<sup>20</sup> <http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM>



```
sudo touch /srv/samba/netlogon/logon.cmd
```

Μπορείτε να εισάγετε οποιοδήποτε εντολής σενάρου των Windows στο `logon.cmd` για να προσαρμόσετε το περιβάλλον του πελάτη.

7. Επανεκκίνηση του Samba για να μπορέσει ο νηός τομέας να ελγξει:

```
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 απ προεπιλογή, για να εισλθει ένας σταθμός εργασίας στον τομέα, μια ομάδα συστήματος πρέπει να αντιστοιχηθεί στην ομάδα των Windows *Domain Admins*. Χρησιμοποιώντας τη λειτουργία `net`, πληκτρολογείτε απ ένα τερματικό:

```
sudo net groupmap add ntgroup="Domain Admins" unixgroup=sysadmin rid=512 type=d
```



Αλλάξτε το `sysadmin` σε ποια ομάδα προτιμάτε. Επσης, ο χρήστης που χρησιμοποιείται για να εισλθει στον τομέα πρέπει να είναι μέλος της ομάδας `sysadmin`, καθώς και μέλος της ομάδας συστήματος `admin`. Η ομάδα `admin` επιτρέπει τη χρήση του `sudo`.

Εν ο χρήστης δεν έχει τα πιστοποιητικά του Samba ακόμη, μπορείτε να τα προσθέσετε με το βοηθητικό πρόγραμμα `smbpasswd`, αλλάζοντας το νόμα χρήστη `sysadmin` κατλληλα:

```
sudo smbpasswd -a sysadmin
```

Επσης, πρέπει να δοθούν ρητ δικαιώματα στην ομάδα *Domain Admins* (

```
net rpc rights grant -U sysadmin "EXAMPLE\Domain Admins" SeMachineAccountPrivilege \
SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege \
SeRemoteShutdownPrivilege
```

9. Θα μπορείτε τρά να προσχωρήσετε πελάτες των Windows στον Τομέα με τον ίδιο τρόπο που τους προσχωρήτε σε έναν τομέα NT4 που τρέχει σε διακομιστ Windows.

## 5.2. ##### μ #####

Με έναν Κριο Ελεγκτ Τομέα (Primary Domain Controller (PDC)) στο δκτυο είναι καλύτερο να έχετε έναν Ελεγκτ Τομέα Αντιγράφου Ασφαλείας (Backup Domain Controller (BDC)) επσης. Αυτ θα επιτρέπει στους πελάτες πιστοποιούνται σε περίπτωση που ο Κριος Ελεγκτς Τομέα δεν είναι διαθέσιμος.

ήταν ρυθμίζετε το Samba σαν Ελεγκτή Τομέα Αντιγράφου Ασφαλείας χρειάζεται να τροπο να συγχρονίζετε τις πληροφορίες λογαριασμών με τον Κρίο 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 αυτοδυναμός τρόπος να συγχρονίσετε τις πληροφορίες λογαριασμών, επειδή και οι δύο ελεγκτές τομέα μπορούν να χρησιμοποιήσουν τις ίδιες πληροφορίες σε πραγματικό χρόνο. Παράλλα αυτό, το να στήσετε έναν διακομιστή LDAP μπορεί να είναι πολύ περίπλοκο για ένα μικρό νομέο χρηστών και λογαριασμών υπολογιστών. Δείτε [μύθος 2, &#x201C;Samba ### LDAP&#x201D; \[120\]](#) για λεπτομέρειες.

1. Πρώτα, εγκαταστήστε τα `samba` και `libpam-smbpass`. Απλά να 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 σχόλιο `Domains` διαγράψτε τα σχόλια που προσθέστε:

```
domain logons = yes
domain master = no
```

4. Σιγουρευτείτε ότι ένας χρήστης έχει δικαιώματα ανήγνωσης των αρχείων στο `/var/lib/samba`. Για παράδειγμα, για να επιτραπεί 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 Κρίο Ελεγκτή Τομέα:

```
sudo scp -r username@pdc:/var/lib/samba /var/lib
```



Αντικαταστήστε το `username` με ένα γκενικό όνομα χρήστη και `pdc` με το όνομα του κεντρικού υπολογιστή ή την IP διεύθυνση του κανονικού Κρίου Ελεγκτή Τομέα.

6. Τέλος, επανεκκινήστε το `samba`:

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

Μπορείτε να ελέγξετε τι ο Ελεγκτής Τομέα Αντιγράφου Ασφάλειας δουλεύει σταματώντας το Samba daemon στον Κ#ριο Ελεγκτή Τομέα, μετ# προσπαθώντας να εισ#λθετε σε #ναν πελ#τη των Windows που #χει προσχωρήθε# στον τομέα.

Κ#τι #λλο που πρ#πει να θυμ#στε ε#ναι αν ρυθμ#σατε την επιλογ# *logon home* σαν κατ#λογο στον Κ#ριο Ελεγκτή Τομέα, και αυτ#ς γ#νει μη διαθ#σιμος, η πρ#σβαση στην μον#δα του χρ#στη *Home* θα ε#ναι επ#σης μη διαθ#σιμη. Για αυτ# το λ#γο ε#ναι καλ#τερο να ρυθμ#σετε το *logon home* να βρ#σκεται σε #ναν ξεχωριστ# διακομιστ# απ# τον Κ#ριο Ελεγκτή Τομέα και τον Ελεγκτή Τομέα Αντιγράφου Ασφάλειας.

### 5.3. #####

- Για διαμορφ#σεις του Samba σε β#θος δε#τε το *Samba HOWTO Collection*<sup>21</sup>
- Ο οδηγ#ς ε#ναι επ#σης διαθ#σιμος σε ##### μ#####<sup>22</sup>.
- Το ##### μ##### ## *Samba*<sup>23</sup> του O'Reilly ε#ναι μια καλ# παραπομπ#.
- Το #####<sup>24</sup> του Samba HOWTO Collection εξηγ# πως να στ#σετε #να Κ#ριο Ελεγκτή Τομέα.
- Το #####<sup>25</sup> του Samba HOWTO Collection εξηγ# πως να στ#σετε #ναν Ελεγκτή Τομέα Αντιγράφου Ασφάλειας.
- Η σελ#δα wiki του *Ubuntu ### ## Samba*<sup>26</sup>.

---

<sup>21</sup> <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/>

<sup>22</sup> <http://www.amazon.com/exec/obidos/tg/detail/-/0131882228>

<sup>23</sup> <http://www.oreilly.com/catalog/9780596007690/>

<sup>24</sup> <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-pdc.html>

<sup>25</sup> <http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-bdc.html>

<sup>26</sup> <https://help.ubuntu.com/community/Samba>

## 6. Active Directory Integration

### 6.1. ##### μ#####μ#### Samba

Μια άλλη χρήση του Samba είναι να ενοποιείται με ένα ήδη υπάρχων δίκτυο των Windows. Όταν είναι μέρος 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*<sup>27</sup>.

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 = lwopen
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 έχετε ικανό να έχετε πρόσβαση σε κάθε διαμοιρασμένο του Samba από έναν πελάτη των Windows. Παράλλα αυτό, σιγουρευτείτε ότι δώσατε πρόσβαση στους στους κατάλληλους χρήστες ομίδες του Ενεργού Καταλόγου στον διαμοιρασμένο κατάλογο. Δείτε το `#μ# 4, &#x201C;Securing File and Print Server&#x201D; [300]` για περισσότερες λεπτομέρειες.

### 6.2. ##### ## #### μ#####μ#### ## Windows

Τώρα που ο διακομιστής Samba είναι μέρος του τομέα Ενεργού Καταλόγου μπορείτε να έχετε πρόσβαση σε διαμοιρασμένα διακομιστή των Windows:

- Για να κνέτε `mount` ενός διαμοιρασμένου των Windows πληκτρολογήστε τα ακόλουθα σε ένα τερματικό εντολήν:

<sup>27</sup> <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 κνέτε `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 τρέχον 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 μ#α. Αυτό είναι χρήσιμο για τη δημιουργία σεναρίου και για μικρές λειτουργίες αρχείων. Για να εισήγετε την εντολή `smb: \>`, μια εντολή σαν FTP που επιτρέπει την εκτέλεση κανονικών αρχείων και εντολών καταλόγων, αλλά εκτελέστε:

```
smbclient //fs01.example.com/share -k
```



Αντικαταστήστε #λες 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. #####

For more `smbclient` options see the man page: **man smbclient**, also available *online*<sup>28</sup>.

<sup>28</sup> <http://manpages.ubuntu.com/manpages/raring/en/man1/smbclient.1.html>

The `mount.cifs` *man page*<sup>29</sup> is also useful for more detailed information.

Η σελίδα wiki του *Ubuntu* για το *Samba*<sup>30</sup>.

---

<sup>29</sup> <http://manpages.ubuntu.com/manpages/raring/en/man8/mount.cifs.8.html>

<sup>30</sup> <https://help.ubuntu.com/community/Samba>

---

## Κεφάλαιο 19. Αντιγραφή ασφαλείας

Υπάρχουν πολλοί τρόποι για την διατήρηση αντιγράφων ασφαλείας μιας εγκατάστασης Ubuntu. Το πιο σημαντικό πράγμα για τα αντιγραφή ασφαλείας είναι η ανάπτυξη ενός `##### #μ##### #####` που να περιχει τι θα αντιγραφεί, πο θα αντιγραφεί, και πως θα γίνεται η επαναφορά του.

Οι παρακάτω ενότητες περιχουν διφορούς τρόπους πραγματοποίησης αυτών των εργασιών.

## 1. #####

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. #####

Το παρακ#τω σεν#ριο εντολ#ν κελ#φους χρησιμοποιε# το <sup>tar</sup> για να δημιουργ#σει #να συμπιεσμ#νο αρχε#ο σε #να απομακρυσμ#νο σ#στημα αρχε#ων <sup>NFS</sup> που #χει προσαρτηθε#. Το #νομα του αρχε#ου προσδιορ#ζεται με τη χρ#ση επιπλ#ον εργαλε#ων γραμμ#ς εντολ#ν.

```
#!/bin/sh
#####
#
# ##### ##μ##### ##### ## NFS.
#
#####

# ## #####.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# ### ## ##μ##### ## #####.
dest="/mnt/backup"

# ##μ##### ### ##μ#### ### #####.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# #μ##### μ###μ#### #####.
echo "##μ##### ##### ## ##### $backup_files ### $dest/$archive_file"
date
echo

# ##μ##### ##### ## ##### μ# ## ##### ## tar.
tar czf $dest/$archive_file $backup_files

# #μ##### μ###μ#### #####.
echo
echo "# ##### ##μ##### #####"
date

# #μ##### ##μ##### ##### ## ##### ## $dest ### ## ##### ## μ##### ## #####.
ls -lh $dest
```



- *\$backup\_files*: μια μεταβλητ# που περι#χει τους καταλ#γους απ# τους οπο#ους θ#λετε να κρατ#σετε αντ#γραφο ασφαλε#ας. Η λ#στα θα πρ#πει να προσαρμοστε# #στε να ταιρι#ζει στις αν#γκες 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*: μεταβλητ# που περι#χει το #####μ# #νομα του συστ#ματος. Προσθ#τοντας το #νομα του συστ#ματος στο #νομα του αρχε#ου, σας δ#νεται η επιλογ# να τοποθετε#τε καθημεριν# αρχε#α, απ# πολλ# συστ#ματα, στον #διο κατ#λογο.
- *\$archive\_file*: το πλ#ρες #νομα του αρχε#ου.
- *\$dest*: destination of the archive file. The directory needs to be created and in this case *mounted* before executing the backup script. See #μ#μ# 2, &#x201C;#####&#x201D; [240] for details of using NFS.
- μ###μ### #####: προαιρετικ# μην#ματα που εμφαν#ζονται στην κονσ#λα χρησιμοποι#ντας το εργαλε#ο `echo`.
- `tar czf $dest/$archive_file $backup_files`: η εντολ# `tar` που χρησιμοποιε#ται για τη δημιουργ#α του αρχε#ου.
  - `c`: δημιουργε# #να αρχε#ο.
  - `z`: περν#ει το αρχε#ο μ#σα απ# το εργαλε#ο `gzip`, συμπι#ζοντας #τσι το αρχε#ο.
  - `f`: output to an archive file. Otherwise the tar output will be sent to STDOUT.
- `ls -lh $dest`: προαιρετικ# εντολ# που εμφαν#ζει μια πλ#ρη λ#στα `(-l)` σε φιλικ# προς τον #νθρωπο μορφ# `(-h)` των αρχε#ων του καταλ#γου προορισμο#. Αυτ# ε#ναι χρ#σιμο για #ναν γρ#γορο #λεγχο του μεγ#θους του αρχε#ου. Αυτ#ς ο #λεγχος δεν θα πρ#πει να αντικαθιστ# τον #λεγχο του αρχε#ου.

This is a simple example of a backup shell script; however there are many options that can be included in such a script. See #μ#μ# 1.4, &#x201C;#####&#x201D; [317] for links to resources providing more in-depth shell scripting information.

## 1.2. #####

### 1.2.1. #####

Ο απλο#στερος τρ#πος για να εκτελ#σετε το παραπ#νω σεν#ριο εντολ#ν δημιουργ#ας αντιγρ#φων ασφαλε#ας ε#ναι να αντιγρ#ψετε τα περιεχ#μενα σε #να αρχε#ο, `backup.sh` για παρ#δειγμα. Μετ# απ# #να τερματικ#, εκτελ#στε:

```
sudo bash backup.sh
```

Αυτ#ς ε#ναι #νας πολ# καλ#ς τρ#πος για να ελ#γξετε το σεν#ριο εντολ#ν #στε να σιγουρευτε#τε πως τα π#ντα δουλε#ουν #πως περιμ#νατε.

### 1.2.2. ##### μ# ## cron

Το εργαλε#ο cron μπορε# να χρησιμοποιηθε# για την αυτοματοπο#ηση της εκτ#λεσης του σεναρ#ου εντολ#ν. Η υπηρεσ#α cron, επιτρ#πει την εκτ#λεση σεναρ#ων εντολ#ν, # εντολ#ν, κ#ποια συγκεκριμ#νη #ρα και ημερομην#α.

Το cron ρυθμ#ζεται μ#σα απ# καταχωρ#σεις σε #να αρχε#ο crontab. Τα αρχε#α crontab χωρ#ζονται σε πεδ#α:

```
# 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 ημ#ρα του μ#να την οπο#α εκτελε#ται η εντολ#.
- *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 εντολ# που θα εκτελεστε#.

Για να προσθ#σετε # να τροποποι#σετε καταχωρ#σεις σε #να αρχε#ο crontab, θα πρ#πει να χρησιμοποιηθε# η εντολ# crontab -e. Επ#σης, το περιεχ#μενο εν#ς αρχε#ου crontab μπορε# να προβληθε# χρησιμοποι#ντας την εντολ# crontab -l.

Για να εκτελ#σετε το σεν#ριο εντολ#ν backup.sh που υπ#ρχει παραπ#νω χρησιμοποι#ντας το cron, πλ#κτρολογ#στε το ακ#λουθο σε #να τερματικ#:

```
sudo crontab -e
```



Χρησιμοποι#ντας το sudo με την εντολ# crontab -e, επεξεργ#ζεστε το crontab του χρ#στη root. Αυτ# ε#ναι απαρα#τητο αν δημιουργε#τε αντ#γραφα ασφαλε#ας καταλ#γων που #χει πρ#σβαση μ#νο ο χρ#στης root.

Προσθ#στε την ακ#λουθη καταχ#ρηση στο αρχε#ο crontab:

```
# m h dom mon dow    command
0 0 * * * bash /usr/local/bin/backup.sh
```

Το σεν#ριο εντολ#ν backup.sh θα εκτελε#ται τ#ρα κ#θε μ#ρα 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 μ#μ# 1.4, &#x201C;#####&#x201D; [317].

### 1.3. #####

Μ#λις #να αρχε#ο δημιουργηθε#, ε#ναι σημαντικ# να το ελ#γξετε. Μπορε#τε να ελ#γξετε το αρχε#ο βλ#ποντας τα αρχε#α που περι#χει, αλλ# ο καλ#τερος #λεγχος ε#ναι να #####  
#να αρχε#ο απ# το συμπιεσμ#νο αρχε#ο.

- To see a listing of the archive contents. From a terminal prompt type:

```
tar -tzvf /mnt/backup/#####-#####.tgz
```

- Για να επαναφ#ρετε #να αρχε#ο απ# το συμπιεσμ#νο αρχε#ο σε #ναν διαφορετικ# κατ#λογο, πληκτρολογ#στε:

```
tar -xzvf /mnt/backup/#####-#####.tgz -C /tmp etc/hosts
```

Η επιλογ# -C στο tar, κατευθ#νει τα αποσυμπιεσμ#να αρχε#α στον προσδιορισμ#νο κατ#λογο. Το παραπ#νω παρ#δειγμα θα αποσυμπι#σει το αρχε#ο /etc/hosts στο /tmp/etc/hosts. Το tar επαναδημιουργε# τη δομ# καταλ#γων που περι#χει.

Επ#σης, παρατηρ#στε πως η αρχικ# "/" δεν συμπεριλαμβ#νεται στη διαδρομ# του αρχε#ου που θα επαναφερθε#.

- Για να επαναφ#ρετε #λα τα αρχε#α που υπ#ρχουν στο συμπιεσμ#νο αρχε#ο, πληκτρολογ#στε τα ακ#λουθα:

```
cd /
sudo tar -xzvf /mnt/backup/#####-#####.tgz
```



Αυτ# θα αντικαταστ#σει τα τρ#χοντα αρχε#α στο σ#στημα αρχε#ων.

### 1.4. #####

- Για περισσ#τερες πληροφορ#ες σχετικ# με τα σεν#ρια εντολ#ν κελ#φους, δε#τε τον #####  
#####μ##### Bash<sup>1</sup>
- Το βιβλ#ο *Teach Yourself Shell Programming in 24 Hours*<sup>2</sup> ε#ναι διαθ#σιμο στο διαδ#κτυο και ε#ναι μια σπουδα#α πηγ# για σεν#ρια εντολ#ν κελ#φους.
- Η ##### Wiki ### CronHowto<sup>3</sup> περι#χει λεπτομ#ρειες για προχωρημ#νες επιλογ#ς του cron.
- Δε#τε το ##### ### GNU tar<sup>4</sup> για περισσ#τερες επιλογ#ς του tar.
- The Wikipedia *Backup Rotation Scheme*<sup>5</sup> article contains information on other backup rotation schemes.

<sup>1</sup> <http://tldp.org/LDP/abs/html/>

<sup>2</sup> <http://safari.sampublishing.com/0672323583>

<sup>3</sup> <https://help.ubuntu.com/community/CronHowto>

<sup>4</sup> <http://www.gnu.org/software/tar/manual/index.html>

<sup>5</sup> [http://en.wikipedia.org/wiki/Backup\\_rotation\\_scheme](http://en.wikipedia.org/wiki/Backup_rotation_scheme)

- Το σενάριο εντολών κελφους χρησιμοποιεί το `tar` για να δημιουργήσει το αρχείο, αλλά υπάρχουν πολλή #λλα εργαλεία γραμμής εντολών που μπορούν να χρησιμοποιηθούν. Για παράδειγμα:
  - *cpio*<sup>6</sup>: χρησιμοποιείται για την αντιγραφή αρχείων προς και απ# συμπίεσμένα αρχεία.
  - *dd*<sup>7</sup>: part of the coreutils package. A low level utility that can copy data from one format to another.
  - *rsnapshot*<sup>8</sup>: a file system snapshot utility used to create copies of an entire file system.
  - *rsync*<sup>9</sup>: a flexible utility used to create incremental copies of files.

---

<sup>6</sup> <http://www.gnu.org/software/cpio/>

<sup>7</sup> <http://www.gnu.org/software/coreutils/>

<sup>8</sup> <http://www.rsnapshot.org/>

<sup>9</sup> <http://www.samba.org/ftp/rsync/rsync.html>

## 2. Archive Rotation

The shell script in `#μ#μ# 1, &#x201C;#####&#x201D; [314]` 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.

Αυτ# ε#ναι το ν#ο σεν#ριο εντολ#ν:

```
#!/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 σεν#ριο μπορε# να εκτελεστε# χρησιμοποι#ντας τις #διες μεθ#δους #πως στο #μ#μ# 1.2, &#x201C;##### &#x201D; [315].

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. #####

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.

Αυτ# ε#ναι το σεν#ριο κελ#φους τροποποιημ#νο #στε να χρησιμοποιε# μια συσκευ# κασ#τας:

```
#!/bin/bash
#####
#
# ##### ##μ##### ##### ##### ## ##### #####.
#
#####

# ## ## #####.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# ### ## ##μ##### ## ##### #####.
dest="/dev/st0"

# ##μ##### μ###μ#### #####.
echo "##μ##### ##### ## ##### $backup_files ## $dest"
date
echo

# ##### ## # ##### ##### ##### #####.
mt -f $dest rewind

# ##μ##### ##### ## ##### μ# ## ##### ## tar.
tar czf $dest $backup_files

# #####μ# ## ##### ##### ##### ## #####.
mt -f $dest rewoffl

# ##μ##### μ###μ#### #####.
echo
echo "# ##μ##### ##### ##### #####"
date
```



Το προεπιλεγμ#νο #νομα για μ#α συσκευ# κασ#τας SCSI ε#ναι /dev/st0.

Χρησιμοποι#στε την κατ#λληλη διαδρομ# συσκευ#ς για το σ#στημ# σας.

Η επαναφορ# απ# μ#α συσκευ# δισκ#τας ε#ναι βασικ# το #διο με την επαναφορ# απ# #να αρχε#ο. Απλ# γυρ#στε την κασ#τα στην αρχ# και χρησιμοποι#στε τη διαδρομ# της συσκευ#ς αντ# για μ#α διαδρομ# αρχε#ου. Για παρ#δειγμα για να επαναφ#ρετε το αρχε#ο /etc/hosts στο /tmp/etc/hosts εκτελ#στε τα ακ#λουθα:

```
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. #####

Bacula is made up of several components and services used to manage which files to backup and backup locations:

- Bacula Director: μια υπηρεσ#α που ελ#γχει #λες τις εργασ#ες αντιγρ#φων ασφαλε#ας, επαναφορ#, επαλ#θευσης και αρχε#ων.
- Bacula Console: μια εφαρμογ# που επιτρ#πει την επικοινων#α με το Director. Υπ#ρχουν τρεις εκδ#σεις του Console:
  - #κδοση γραμμ#ς εντολ#ν που βασ#ζεται σε κε#μενο.
  - Γραφικ# περιβ#λλον χρ#στη (GUI) GTK+ που βασ#ζεται στο Gnome.
  - Γραφικ# περιβ#λλον (GUI) wxWidgets.
- Bacula File: επ#σης γνωστ# ως το πρ#γραμμά Bacula Client. Αυτ# η εφαρμογ# εγκαθ#σταται σε μηχαν#ματα απ# τα οπο#α θα δημιουργηθο#ν αντ#γραφα ασφαλε#ας και ε#ναι υπε#θυνο για τα δεδομ#να που ζητο#νται απ# το Director.
- Bacula Storage: τα προγρ#μματα που πραγματοποιο#ν την αποθ#κευση και την επαναφορ# αρχε#ων στα φυσικ# μ#σα.
- Bacula Catalog: ε#ναι υπε#θυνο για την διατ#ρηση των ευρετηρ#ων των αρχε#ων και των β#σεων δεδομ#νων των τ#μων για #λα τα αρχε#α για τα οπο#α διατηρο#νται αντ#γραφα ασφαλε#ας, επιτρ#ποντας γρ#γορο εντοπισμ# και επαναφορ# των αρχειοθετημ#νων αρχε#ων. Το Catalog υποστηρ#ζει τρεις διαφορετικ#ς β#σεις δεδομ#νων: MySQL, PostgreSQL και SQLite.
- Bacula Monitor: επιτρ#πει την παρακολο#θηση του Director, των υπηρεσι#ν του File και του Storage. Προς το παρ#ν, το Monitor ε#ναι διαθ#σιμο μ#νο ως εφαρμογ# με γραφικ# περιβ#λλον GTK+.

Αυτ#ς οι υπηρεσ#ες και εφαρμογ#ς μπορο#ν να εκτελεστο#ν σε πολλο#ς εξυπηρετητ#ς και πελ#τες, # μπορο#ν να εγκατασταθο#ν σε #να μηχαν#μα, αν κρατ#τε αντ#γραφα ασφαλε#ας εν#ς μ#νο δ#σκου # τ#μου.

#### 3.2. #####



If using MySQL or PostgreSQL as your database, you should already have the services available. Bacula will not install them for you.

Υπ#ρχουν πολλ# πακ#τα που περι#χουν τα διαφορετικ# μ#ρη του Bacula. Για να εγκαταστ#σετε το Bacula, σε #να τερματικ# πληκτρολογ#στε:



```
sudo apt-get install bacula
```

Απ# προεπιλογ#, εγκαθιστ#ντας το πακ#το *bacula*, θα χρησιμοποιηθε# μια β#ση δεδομ#νων MySQL για τον κατ#λογο. Αν θ#λετε να χρησιμοποι#σετε SQLite # PostgreSQL, για τον κατ#λογο, εγκαταστ#στε το *bacula-director-sqlite3* # το *bacula-director-pgsql* αντ#στοιχα.

Κατ# τη διαδικασ#α εγκατ#στασης, θα σας ζητηθε# να δ#σετε πιστοποιητικ# για τον ##### της β#σης δεδομ#νων και για τον ##### της β#σης δεδομ#νων του *bacula*.

Ο διαχειριστ#ς της β#σης δεδομ#νων θα πρ#πει να #χει τα κατ#λληλα δικαι#ματα για να δημιουργ#σει μια β#ση δεδομ#νων. Δε#τε το #μ#μ# 1, &#x201C;MySQL&#x201D; [216] για περισσ#τερες πληροφορ#ες.

### 3.3. #####

Τα αρχε#α ρυθμ#σεων του Bacula ε#ναι μορφοποιημ#να β#σει των καταχωρ#σεων που περιλαμβ#νουν ##### μ#σα σε αγκλ#ες &#x201C;{ }&#x201D;. Κ#θε μ#ρος του Bacula #χει #να ξεχωριστ# αρχε#ο στον κατ#λογο */etc/bacula*.

Τα δι#φορα μ#ρη του Bacula πρ#πει να εξουσιοδοτηθ#ν μεταξ# τους. Αυτ# επιτυγχ#νεται με τη χρ#ση της οδηγ#ας κωδικ# πρ#σβασης *password*. Για παρ#δειγμα, ο κωδικ#ς πρ#σβασης της καταχ#ρησης *Storage* στο αρχε#ο */etc/bacula/bacula-dir.conf* πρ#πει να ε#ναι ο #διος με αυτ#ν της καταχ#ρησης *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 παραπ#νω παρ#δειγμα αλλ#ζει το #νομα της εργασ#ας σε *BackupServer* που ε#ναι το #νομα του μηχαν#ματος. Αντικαταστ#στε το &#x201C;BackupServer&#x201D; με το κατ#λληλο #νομα υπολογιστ#, # με κ#ποιο #λλο περιγραφικ# #νομα.

Το *Console* μπορε# να χρησιμοποιηθε# για να λ#βετε πληροφορ#ες απ# το *Director* για εργασ#ες, αλλ# για να χρησιμοποι#σετε το *Console* με #ναν χρ#στη μ#-root, ο χρ#στης θα πρ#πει να ε#ναι στην ομ#δα *bacula*. Για να προσθ#σετε #ναν χρ#στη στην ομ#δα *bacula* πλ#κτρολογ#στε τα ακ#λουθα σε #να τερματικ#:

```
sudo adduser $username bacula
```



Αντικαταστ#στε το *\$username* με το πραγματικ# #νομα χρ#στη. Επ#σης, αν προσθ#τετε τον τρ#χοντα χρ#στη στην ομ#δα, θα πρ#πει να αποσυνδεθε#τε και να επανασυνδεθε#τε για να ισχ#σουν τα ν#α δικαι#ματα.

### 3.4. #####

Αυτ# η εν#τητα περιγρ#φει π#ς να δημιουργ#σετε αντ#γραφα ασφαλε#ας συγκεκριμ#νων καταλ#γων εν#ς υπολογιστ# σε μια τοπικ# συσκευ# κασ#τας.

- Πρ#τα, η συσκευ# ##### πρ#πει να ρυθμιστε#. Επεξεργαστε#τε το `/etc/bacula/bacula-sd.conf` και προσθ#στε:

```
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.

Μπορε#τε επ#σης να αποσχολι#σετε κ#ποιο απ# τα #λλα παραδε#γματα στο αρχε#ο.

- Αφo# επεξεργαστε#τε το `/etc/bacula/bacula-sd.conf`, η υπηρεσ#α `Storage` θα πρ#πει να επανεκκινηθε#:

```
sudo service bacula-sd restart
```

- Τ#ρα προσθ#στε μ#α καταχ#ρηση `Storage` στο `/etc/bacula/bacula-dir.conf` για να χρησιμοποι#σετε τη ν#α συσκευ#:

```
# 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 = "Cv70F6pflt6pBopT4vQ0nigDrR0v3LT3Cgkiyjc"
    Device = "Tape Drive"
    Media Type = tape
}
```

Η οδηγ#α *Address* πρ#πει να ε#ναι το Πλ#ρωσ πιστοποιημ#νο #νομα τομ#α (FQDN) του εξυπηρετητ#. Αλλ#ξετε το *backupserver* με το πραγματικ# #νομα του υπολογιστ#.

Επ#σης, σιγουρευτε#τε πως η οδηγ#α *Password* ε#ναι #δια με τον κωδικ# πρ#σβασης στο /etc/bacula/bacula-sd.conf.

- Δημιουργ#στε #να ν#ο *FileSet*, που θα καθορ#σει για ποιους καταλ#γους θα δημιουργηθ#ν αντ#γραφα ασφαλε#ας, προσθ#τοντας:

```
# 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.

- Μετ#, δημιουργ#στε #να ν#ο *Schedule* για την εργασ#α δημιουργ#ας αντιγρ#φων ασφαλε#ας:

```
# LocalhostBackup Schedule -- Daily.
Schedule {
    Name = "LocalhostDaily"
    Run = Full daily at 00:01
}
```

Η εργασ#α θα εκτελε#ται κ#θε μ#ρα στις 00:01 # 12:01 π.μ. Υπ#ρχουν πολλ#ς #λλες επιλογ#ς προγραμματισμο# διαθ#σιμες.

- Τ#λος, δημιουργ#στε την εργασ#α (*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 εργασ#α θα δημιουργε# #να ##### αντ#γραφο ασφαλε#ας κ#θε μ#ρα στη συσκευ# κασ#τας.

- Κ#θε κασ#τα θα πρ#πει να #χει μια #####. Αν η τρ#χουσα κασ#τα δεν #χει ετικ#τα, το Bacula θα σας στε#λει #να email για να σας ενημερ#σει. Για να β#λετε ετικ#τα σε μ#α κασ#τα χρησιμοποι#ντας το Console πληκτρολογ#στε τα ακ#λουθα σε #να τερματικ#:

```
bconsole
```

- Στην γραμμ# εντολ#ν του Bacula Console, πληκτρολογ#στε:

```
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
```

- Πληκτρολογ#στε το ν#ο #νομα του ##μ##:

```
Enter new Volume name: #####
Defined Pools:
    1: Default
    2: Scratch
```

Αντικαταστ#στε το ##### με την επιθυμητ# ετικ#τα.

- Τ#ρα, επιλ#ξτε το *Pool*:

```
Select the Pool (1-2): 1
Connecting to Storage daemon TapeDrive at backupserver:9103 ...
Sending label command for Volume "Sunday" Slot 0 ...
```

Συγχαρητ#ρια, #χετε τ#ρα ρυθμ#σει το *Bacula* #στε να δημιουργε# αντ#γραφα ασφαλε#ας του τοπικο# υπολογιστ# σε μ#α προσαρτημ#νη συσκευ# κασ#τας.

<sup>10</sup> <http://www.bacula.org/en/rel-manual/index.html>

### 3.5. #####

- Για περισσ#τερες επιλογ#ς ρυθμ#σεων του *Bacula* αναφερθε#τε στο ##### ##### *Bacula*<sup>10</sup>
- Η ##### ##### *Bacula*<sup>11</sup> περι#χει τις τελευτα#ες ειδ#σεις και εκδ#σεις του *Bacula*.
- Also, see the *Bacula Ubuntu Wiki*<sup>12</sup> page.

---

<sup>11</sup> <http://www.bacula.org/>

<sup>12</sup> <https://help.ubuntu.com/community/Bacula>

---

## Κεφάλαιο 20. Εικονικοποίηση

Η εικονικοποίηση υιοθετείται από πολλούς διαφορετικούς περιβάλλοντα και καταστάσεις. Εάν είστε προγραμματιστής, η εικονικοποίηση μπορεί να σας πάρει ένα περιορισμένο περιβάλλον στο οποίο μπορείτε με ασφάλεια να κνέτε σχεδόν κάθε έδους ανάπτυξη χωρίς να πειρίζετε 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 κ#νει διεπαφ# με δι#φορες τεχνολογι#ς εικονικοπο#ησης. Πριν ξεκιν#σετε με το `libvirt` ε#ναι καλ# να σιγουρευτε#τε #τι το υλικ# σας υποστηρ#ζει τις κατ#λληλες επεκτ#σεις εικονικοπο#ησης για το KVM. Πληκτρολογε#στε τα ακ#λουθα απ# #να τερματικ# εντολ#ν:

```
kvm-ok
```

Θα εμφανιστε# #να μ#νυμα που θα σας πληροφορε# αν ο επεξεργαστ#ς σας ##### # υποστηρ#ζει εικονικ#ς μηχαν#ς (hardware virtualization).



Στους περισσ#τερους υπολογιστ#ς των οπο#ων ο επεξεργαστ#ς υποστηρ#ζει εικονικοπο#ηση, ε#ναι απαρα#τητο να ενεργοποι#σετε μια επιλογ# στο BIOS.

### 1.1. #####

Αυτο# ε#ναι διαφορετικο# τρ#ποι να επιτρ#ψετε σε μια εικονικ# μηχαν# να #χει πρ#σβαση στο εξωτερικ# διαδ#κτυο. Η προεπιλεγμ#νη διαμ#ρφωση του εικονικο# διαδικτ#ου ε#ναι διαδικτ#ωση *usermode*, η οπο#α χρησιμοποιε# το πρωτ#κόλλο SLIRP και κ#νηση NATed μ#σω της διεπαφ#ς του κεντρικο# υπολογιστ# στο εξωτερικ# δ#κτυο.

Για να επιτρ#ψετε εξωτερικ#ς κεντρικ#ς υπολογιστ#ς να #χουν πρ#σβαση #μεσα σε εικονικ#ς μηχαν#ς μια ##### πρ#πει να ρυθμιστε#. Αυτ# επιτρ#πει στις εικονικ#ς διεπαφ#ς να συνδεθον# σε εξωτερικ# δ#κτυα μ#σω της φυσικ#ς διεπαφ#ς, κ#νοντ#ς τες να εμφαν#ζονται σαν κανονικο# κεντρικ#ς υπολογιστ#ς στο υπ#λοιπο δ#κτυο. Για πληροφορε#ς σχετικ#ς με το πω# να στ#σετε μια γ#φυρα βλ. #μ#μ# 1.4, &#x201C;#####&#x201D; [41].

### 1.2. #####

Για να εγκαταστ#σετε τα απαρα#τητα πακ#τα, απ# #να τερματικ# εντολ#ν πληκτρολογε#στε:

```
sudo apt-get install kvm libvirt-bin
```

Αφο# εγκαταστ#σετε το `libvirt-bin`, ο χρ#στης που χρησιμοποιε#τε για να διαχειρ#ζεται εικονικ#ς μηχαν#ς θα πρ#πει να ενταχθε# στην ομ#δα *libvirtd*. #τσι θα επιτραπε# στο χρ#στη πρ#σβαση σε ειδικ#ς επιλογ#ς δικτ#ωσης.

Σε #να τερματικ# πληκτρολογ#στε:

```
sudo adduser $USER libvirtd
```



Εάν ο χρήστης που έχει επιλεγεί είναι ο τρέχων χρήστης, θα πρέπει να αποσυνδεθείτε και να συνδεθείτε ξανά για να ισχύσει η καινούρια ιδιότητα μιλους στην ομάδα.

Εστέ 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 να πληκτρολογήσετε και μια οθόνη θα πρέπει να συνδεθούν στη φυσική μηχανή.

Σε περίπτωση εικονικής μηχανής να Γραφική Περιβάλλον Εργασίας (Graphical User Interface (GUI)) είναι ανάλυση του φυσικού πληκτρολογίου και ποντικίου. Αντ' να εγκαταστήσετε να Γραφική Περιβάλλον Εργασίας η εφαρμογή *virt-viewer* μπορεί να χρησιμοποιηθεί για τη σύνδεση σε μια κονσόλα εικονικής μηχανής χρησιμοποιώντας το VNC. Δείτε το [μύμ 1.6, &#x201C;#####μμ#####&#x201D; \[333\]](#) 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*<sup>1</sup> for details.

Ακμή 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 εκτελέσετε σενάρια μετά την εγκατάσταση, κλπ. Για λεπτομέρειες βλ. [μύμ 2, &#x201C;JeOS ### vmbuilder&#x201D; \[335\]](#)

Libvirt can also be configured work with Xen. For details, see the Xen Ubuntu community page referenced below.

### 1.3. virt-install

`virt-install#####` μρος του `#####virtinst`. Για να το εγκαταστήσετε απ' να τερματικό εντολές 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.

<sup>1</sup> <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 μονοπύτι 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`: εξηγεί την εικονική κονσόλα του επισκεπτή χρησιμοποιώντας VNC.
- `--noautoconsole`: δε θα συνδεθεί αυτόματα στην κονσόλα της εικονικής μηχανής.
- `-v`: δημιουργεί έναν πλήρως εικονικό επισκεπτή.

Αφού εκκινήσετε το `virt-install` μπορείτε να συνδεθείτε στην κονσόλα της εικονικής μηχανής είτε τοπικά χρησιμοποιώντας ένα Γραφικό Περιβάλλον Εργασίας 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`: μονοπύτι του αρχείου, λογικό τμήμα, διαμερίσματος που θα χρησιμοποιηθεί απ την καινούρια εικονική μηχανή.
- `--connect`: προσδιορίζει σε ποιο hypervisor να συνδεθεί.

Επίσης, χρησιμοποιείτε τις επιλογές `-d` ή `--debug` για να λήσετε προβλήματα με το `virt-clone`.



Αντικαταστήστε τα `web_devel` και `database_devel` με κατάλληλα ονόματα εικονικών μηχανών.

## 1.5. #####

### 1.5.1. virsh

Υπάρχουν πολλές λειτουργίες διαθέσιμες για να διαχειριστείτε εικονικές μηχανές και το `libvirt`. Η λειτουργία `virsh` μπορεί να χρησιμοποιηθεί απ τη γραμμή εντολών. Μερικά παραδείγματα:

- Για να καταγράφο#ν οι εικονικ#ς μηχαν#ς:

```
virsh -c qemu:///system list
```

- Για να εκκιν#σετε μια εικονικ# μηχαν#:

```
virsh -c qemu:///system start web_devel
```

- Ομο#ως, για να εκκιν#σετε μια εικονικ# μηχαν# κατ# την εκκ#νηση:

```
virsh -c qemu:///system autostart web_devel
```

- Επανεκκιν#στε μια εικονικ# μηχαν# με:

```
virsh -c qemu:///system reboot web_devel
```

- Η ##### των εικονικ#ν μηχαν#ν μπορε# να αποθηκευτε# σε #να αρχε#ο #στε να αποκατασταθε# αργ#τερα. Το ακ#λουθο θα αποθηκε#σει την κατ#σταση της εικονικ#ς μηχαν#ς σε #να αρχε#ο που θα ονομαστε# σ#μφωνα με την ημερομην#α:

```
virsh -c qemu:///system save web_devel web_devel-022708.state
```

#ταν αποθηκευτε# η εικονικ# μηχαν# δε θα εκτελε#τε πλ#ον.

- Μια αποθηκευμ#νη εικονικ# μηχαν# μπορε# να αποκατασταθε# χρησιμοποι#ντας:

```
virsh -c qemu:///system restore web_devel-022708.state
```

- Για να τερματ#σετε μια εικονικ# μηχαν# κ#ντε:

```
virsh -c qemu:///system shutdown web_devel
```

- Μια συσκευ# CDROM μπορε# να φορτωθε# σε μια εικονικ# μηχαν# πληκτρολογ#ντας:

```
virsh -c qemu:///system attach-disk web_devel /dev/cdrom /media/cdrom
```



Στο παραπ#νω παραδε#γματα αντικαταστ#στε το *web\_devel* με το κατ#λληλο #νομα της εικονικ#ς μηχαν#ς, και το *web\_devel-022708.state* με #να περιγραφικ# #νομα αρχε#ου.

### 1.5.2. #####

Το πακ#το *virt-manager* περι#χει μια γραφικ# λειτουργ#α για να διαχειρ#ζεστε τοπικ#ς και απομακρυσμ#νες εικονικ#ς μηχαν#ς. Για να εγκαταστ#σετε το *virt-manager* πληκτρολογ#στε:

```
sudo apt-get install virt-manager
```

Αφο# το `virt-manager` απαιτε# #να περιβ#λλον Γραφικ#ς Διεπαφ#ς Χρ#στη (Graphical User Interface (GUI)) συν#σταται να το εγκαταστ#σετε σε #να σταθμ# εργασιας # μηχαν# ελ#γχου αντ# σε #να διακομιστ# παραγωγ#ς. Για να συνδεθε#τε στην τοπικ# υπηρεσια `libvirt` πληκτρολογε#στε:

```
virt-manager -c qemu:///system
```

Μπορε#τε να συνδεθε#τε στην υπηρεσια `libvirt` που εκτελε#τε σε #ναν #λλο κεντρικ# υπολογιστ# πληκτρολογ#ντας τα ακ#λουθα σε #να τερματικ# εντολ#ν:

```
virt-manager -c qemu+ssh://virtnode1.mydomain.com/system
```



Το παραπ#νω παρ#δειγμα υποθ#τει #τι η συνδεσιμ#τητα SSH μεταξ# του συστ#ματος διαχε#ρισης και του `virtnode1.mydomain.com` #χει #δη διαμορφωθε#, και χρησιμοποιε# κλειδι# SSH για ταυτοπο#ηση. ##### SSH χρησιμοποιο#νται γιατ# το `libvirt` στ#λνει την προτροπ# κωδικικο# σε #λλη διαδικασια. Για πληροφοριες στο πως να διαμορφ#σετε SSH δε#τε #μ#μ# 1, &#x201C;OpenSSH Server&#x201D; [83]

## 1.6. #####

Η εφαρμογ# `virt-viewer` σας επιτρ#πει να συνδεστε στην κονσ#λα εικονικ#ς μηχαν#ς. Το `virt-viewer` απαιτε# μια Γραφικ# Διεπαφ# Χρ#στη (Graphical User Interface (GUI)) για να συνδεστε με την εικονικ# μηχαν#.

Για να εγκαταστ#σετε το `virt-viewer` απ# #να τερματικ# πληκτρολογε#στε:

```
sudo apt-get install virt-viewer
```

#ταν μια εικονικ# μηχαν# #χει εγκατασταθε# και εκτελε#τε μπορε#τε να συνδεθε#τε στην κονσ#λα της εικονικ#ς μηχαν#ς χρησιμοποι#ντας:

```
virt-viewer -c qemu:///system web_devel
```

#μοια με το `virt-manager`, το `virt-viewer` μπορε# να συνδεθε# σε #ναν απομακρυσμ#νο κεντρικ# υπολογιστ# χρησιμοποι#ντας SSH με κλειδι# ταυτοπο#ησης, επ#σης:

```
virt-viewer -c qemu+ssh://virtnode1.mydomain.com/system web_devel
```

Βεβαιωθε#τε να αντικαταστ#σετε το `web_devel` με το κατ#λληλο #νομα εικονικ#ς μηχαν#ς.

Ε#ν #χει διαμορφωθε# να χρησιμοποιε# #####μ### διεπαφ# δικτ#ου μπορε#τε επ#σης να εγκαταστ#σετε πρ#σβαση SSH στην εικονικ# μηχαν#. Δε#τε #μ#μ# 1, &#x201C;OpenSSH Server&#x201D; [83] και #μ#μ# 1.4, &#x201C;#####&#x201D; [41] για περισσ#τερες λεπτομ#ρειες.

### 1.7. #####

- See the *KVM*<sup>2</sup> home page for more details.
- Για περισσότερες λεπτομότητες σχετικά με το *libvirt* δείτε το *libvirt home page*<sup>3</sup>
- Η ιστοσελίδα *Virtual Machine Manager*<sup>4</sup> έχει περισσότερες πληροφορίες για την ανάπτυξη *virt-manager*.
- Επίσης, περστείτε απ το *#ubuntu-virt* κανάλι IRC στο *freenode*<sup>5</sup> για να συζητήσετε για την τεχνολογία εικονικοποίησης στο *Ubuntu*.
- Άλλη μια καλή πηγή είναι η σελίδα *Ubuntu Wiki KVM*<sup>6</sup>.
- For information on *Xen*, including using *Xen* with *libvirt*, please see the *Ubuntu Wiki Xen*<sup>7</sup> page.

---

<sup>2</sup> <http://www.linux-kvm.org/>

<sup>3</sup> <http://libvirt.org/>

<sup>4</sup> <http://virt-manager.et.redhat.com/>

<sup>5</sup> <http://freenode.net/>

<sup>6</sup> <https://help.ubuntu.com/community/KVM>

<sup>7</sup> <https://help.ubuntu.com/community/Xen>

## 2. JeOS ### vmbuilder

### 2.1. #####

#### 2.1.1. ## ##### ## JeOS

Το *Ubuntu JeOS* (προφ#ρεται #Τζους#) ε#ναι μια αποδοτικ# παραλλαγ# του λειτουργικ# συστ#ματος Διακομιστ# *Ubuntu*, διαμορφωμ#νο συγκεκριμ#να για εικονικ#ς συσκευ#ς. Δεν ε#ναι πλ#ον διαθ#σιμο σαν CD-ROM ISO για μεταφ#ρτωση, αλλ# μ#νο σαν επιλογ# ε#τε:

- Καθ#ς εγκαθιστ#τε απ# το Server Edition ISO (πατ#ντας *F4* στην πρ#τη οθ#νη θα σας επιτρ#πει να επιλ#ξετε #Ελ#χιστη Εγκατ#σταση#, που ε#ναι η επιλογ# πακ#του ισοδ#ναμη με το JeOS).
- # να στηθε# χρησιμοποιντας το *vmbuilder* του *Ubuntu*, το οπο#ο περιγρ#φεται εδ#.

Το JeOS ε#ναι εξειδικευμ#νη εγκατ#σταση της #κδοσης Διακομιστ# *Ubuntu* με #να συντονισμ#νο πυρ#να ο οπο#ος περιχ#ει μ#νο τα βασικ# στοιχε#α που χρει#ζονται για να εκτελεστε# σε #να εικονικ# περιβ#λλον.

Το *Ubuntu JeOS* #χει ρυθμιστε# #στε να εκμεταλλε#εται βασικ#ς τεχνολογ#ες απ#δοσης στα τελευτα#α προ##ντα εικονικοπο#ησης απ# το *VMware*. Αυτ#ς ο συνδυασμ#ς του μειωμ#νου μεγ#θους και τις βελτιστοποιημ#νης επ#δοσης διασφαλ#ζει #τι η #κδοση *Ubuntu JeOS* παρ#χει μια #κρως αποτελεσματικ# χρ#ση των π#ρων του διακομιστ# σε μεγ#λες εικονικ#ς αναπτ#ξεις.

Χωρ#ς περιττο#ς οδηγο#ς, και μ#νο τα ελ#χιστα απαιτομ#ενα πακ#τα, το *ISVs* μπορε# να διαμορφ#σει το υποστηριζμ#νο OS ακριβ#ς #πως επιθυμ#ν. #χουν τη σιγουρι# #τι η ενημερ#σεις, ε#τε για ασφ#λεια ε#τε για λ#γους εν#σχυσης, θα ε#ναι περιορισμ#νες στο ελ#χιστο που απαιτε#ται στο συγκεκριμ#νο περιβ#λλον τους. Σε αντ#λλαγμα, οι χρ#στες που αναπτ#σσουν εικονικ#ς συσκευ#ς χτισμ#νες σε JeOS θα πρ#πει να περ#σουν απ# λ#γες ενημερ#σεις και γ# αυτ# λιγ#τερη συντ#ρηση απ# αυτ# που θα ε#χαν με μ#α κανονικ# πλ#ρη εγκατ#σταση εν#ς διακομιστ#.

#### 2.1.2. ## ##### ## vmbuilder

Με το *vmbuilder*, δεν ε#ναι πλ#ον απαρα#τητο να κ#νετε λ#ψη εν#ς JeOS ISO. Το *vmbuilder* θα βρει τα δι#φορα πακ#τα και θα φτι#ξει μια εικονικ# μηχαν# προσαρμοσμ#νη στις αν#γκες σας σε περ#που #να λεπτ#. Το *vmbuilder* ε#ναι #να script που αυτοματοποιε# τη διαδικασ#α δημιουργ#ας μιας #τοιμης προς χρ#ση εικονικ#ς μηχαν#ς βασισμ#νης στο Linux. Οι hypervisor που υποστηρ#ζονται αυτ# τη στιγμ# ε#ναι το *KVM* και το *Xen*.

Μπορε#τε να περ#σετε επιλογ#ς γραμμ#ς εντολ#ν για να προσθ#σετε επιπλ#ον πακ#τα, να αφαιρ#σετε πακ#τα, να επιλ#ξετε ποια #κδοση του *Ubuntu*, ποι#ν καθρ#φτη κλπ. Σε πρ#σφατο υλικ# με μεγ#λη RAM, να κ#νετε *tmpdir* στο */dev/shm* # να χρησιμοποισετε #να

tmpfs, και #ναν τοπικ# καθρ#φτη, μπορε#τε να εκκιν#σετε αυτ#ματα #να VM σε λιγ#τερο απ# #να λεπτ#.

Πρωτοεμφαν#στηκε ως shell script στο Ubuntu 8.04 LTS, το ubuntu-vm-builder ξεκ#νησε με μικρ# #μφαση ως <sup>hack</sup> για να βοηθ#σει τους προγραμματιστ#ς να δοκιμ#σουν τον καινο#ριο τους κ#δικα σε μια εικονικ# μηχαν# χωρ#ς να πρ#πει να ξεκιν#σουν απ# το μηδ#ν κ#θε φορ#. Καθ#ς αρκετο# διαχειριστ#ς του Ubuntu #ρχισαν να προσ#χουν αυτ# το script, κ#ποιοι απ# αυτο#ς συν#χισαν να το βελτι#νουν και να το προσαρμ#ζουν για τ#σες περιπτ#σεις χρ#σης που ο Soren Hansen (ο δημιουργ#ς του script και ειδικ#ς στην εικονικοπο#ηση του Ubuntu, #χι ο πα#κτης του γκολφ) αποφ#σισε να το ξαναγρ#ψει απ# το μηδ#ν για το Intrepid ως script της python με μερικο#ς ν#ους στ#χους στη σχεδ#αση:

- Να το αναπτ#ξει #στε να μπορε# να επαναχρησιμοποιηθε# απ# #λλες διανομ#ς.
- Να χρησιμοποιε# μηχανισμο#ς plugin για #λες τις αλληλεπιδρ#σεις εικονικοπο#ησης #στε #λλοι να μπορο#ν ε#κολα να προσθ#σουν λογικ# για #λλα περιβ#λλοντα εικονικοπο#ησης.
- Να παρ#χει μια ε#κολη να διατηρηθε# διεπαφ# ιστο# σαν επιλογ# στη διεπαφ# γραμμ#ς εντολ#ν.

Αλλ# οι βασικ#ς αρχ#ς και εντολ#ς να παραμε#νουν #διες.

## 2.2. #####

Υποθ#τουμε #τι #χει εγκαταστ#σει και διαμορφ#σει τα libvirt και KVM τοπικ# στη μηχαν# ου χρησιμοποιε#τε. Για πληροφορ#ες στο πως να το κ#νετε, παρακαλ# αναφερθε#τε στο:

- #μ#μ# 1, &#x201C;libvirt&#x201D; [329]
- Η σελ#δα Wiki KVM<sup>8</sup>

Επ#σης υποθ#τουμε #τι ξ#ρετε πως να χρησιμοποι#σετε #ναν επεξεργαστ# κειμ#νου με β#ση κε#μενο #πως οι nano # vi. Ε#ν δεν #χετε χρησιμοποι#σει καν#ναν απ# τους δ#ο στο παρελθ#ν, μπορε#τε να δε#τε μια επισκ#πηση των διαφ#ρων επεξεργαστ#ν κειμ#νου που ε#ναι διαθ#σιμοι διαβ#ζοντας τη σελ#δα *PowerUsersTextEditors*<sup>9</sup>. Αυτ# το εγχειρ#διο οδηγι#ν #χει δημιουργηθε# σε KVM, αλλ# η βασικ# αρχ# πρ#πει να παραμε#νει σε #λλες τεχνολογ#ες εικονικοπο#ησης.

### 2.2.1. ##### vmbuilder

Το #νομα του πακ#του που χρει#ζεται να εγκαταστ#σετε ε#ναι python-vm-builder. Σε #να τερματικ# εντολ#ν πληκτρολογε#στε:

```
sudo apt-get install python-vm-builder
```

<sup>8</sup> <https://help.ubuntu.com/community/KVM>

<sup>9</sup> <https://help.ubuntu.com/community/PowerUsersTextEditors>



Εάν τρέχετε Hardy, μπορείτε ακόμα να εκτελέσετε τα περισσότερα απ' αυτά χρησιμοποιώντας την παλιά έκδοση του πακέτου που ονομάζεται `ubuntu-vm-builder`, υπάρχουν μνο λήγες αλλαγές στη σύνταξη του πακέτου.

### 2.3. #####μ## ### ##### ##

Το να καθορίσετε μια εικονική μηχανή με το `vmbuilder` του Ubuntu είναι αρκετά απλό, αλλά εδ είναι κάποια πράγματα που πρέπει να λάβετε υπόψη:

- Εάν σκοπεύετε να στελέξετε μια εικονική συσκευή, μην υποθέσετε ότι ο τελικός χρήστης θα ξέρει πώς να επεκτείνει το μέγεθος του δίσκου ή να αλλάξει τις ανηγές του, ή ότι έχετε σχεδιάσει για έναν μεγάλο εικονικό δίσκο για να επιτρέψει στη συσκευή σας να μεγαλώνει, ή εξηγήστε αρκετά καλά στις βοηθητικές οδηγίες πώς να δεσμεύουν περισσότερο χώρο. Σίως είναι καλά ιδέα να αποθηκεύει δεδομένα σε κάποιο ξεχωριστό εξωτερικό μέσο αποθήκευσης.
- Δεδομένου ότι η RAM είναι πολύ πιο εκόλο να δεσμευτεί σε ένα VM, το μέγεθος της RAM θα πρέπει να τεθεί σε τι πιστεύετε είναι ασφαλές για τη συσκευή σας.

Η εντολή `vmbuilder` έχει <sup>2</sup> κριές παραμέτρους: την ##### (hypervisor) και την στοχοθετημένη #####. Προαιρετικές παράμετροι είναι πολλές και μπορούν να βρεθούν χρησιμοποιώντας την ακόλουθη εντολή:

```
vmbuilder kvm ubuntu --help
```

#### 2.3.1. #####μ#####

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 τι θλούμε να χρησιμοποιήσουμε τον εικονικό πυρήνα `kernel` (αυτός χρησιμοποιείται για το στίσιμο μιας εικονικής JeOS), η `--arch` δηλώνει τι θλούμε να χρησιμοποιήσουμε μια μηχανή 32 bit, η `-o` λεί στο `vmbuilder` να αντικαταστήσει την προηγούμενη έκδοση του VM και η `--libvirt` λεί να ενημερωθεί το τοπικό εικονικό περιβάλλον να προσθήσει το VM που προκύπτει στη λίστα διαθέσιμων μηχανών.

Σημειώσεις:

- Λόγω της φάσεως των λειτουργιών που εκτελούνται απ' το `vmbuilder`, χρειάζεται να έχουμε διακαιμάτα βήσης, γι' αυτό το `sudo`.
- Εάν η εικονική σας μηχανή χρειάζεται να χρησιμοποιήσει πνω απ' 3Gb ram, πρέπει να στίσετε μηχανή 64 bit (`--arch amd64`).

- Μέχρι το Ubuntu 8.10, ο εικονικός πυρήνας ήταν φτιαγμένος μόνο για αρχιτεκτονική 32 bit, έτσι αν θέλετε να ορμάτε μηχανή amd64 στο Hardy, πρέπει να χρησιμοποιήσετε διακομιστή *--flavour* αντί αυτού.

### 2.3.2. ##### JeOS

#### 2.3.2.1. ##### JeOS

##### 2.3.2.1.1. ##### IP

Σαν εικονική συσκευή που μπορεί να ανατεθεί σε διάφορα πολύ διαφορετικά δίκτυα, είναι πολύ δύσκολο να γνωρίζουμε πώς ακριβώς θα είναι το δίκτυο. Για να απλοποιήσουμε τη διαμρφώση, είναι καλή ιδέα να ακολουθήσουμε μια προσγγιση παρόμοια με αυτή που συνθώς κίνουν οι κατασκευαστές υλικού, να αναθέτουν μια σταθερή IP διεθυσνη στη συσκευή σε δίκτυα ιδιωτικής κλήσης τα οποία θα παρήχετε στις βοηθητικές οδηγίες. Μια διεθυσνη με εμπλήεια 192.168.0.0/255 είναι συνθώς μια καλή επιλογή.

Για να το κνουμε θα χρησιμοποιήσουμε τις ακόλουθες παραμέτρους:

- *--ip ADDRESS*: διεθυσνη IP σε μορφή με τελεές (εξορισμός σε *dhcp* εάν δεν διεκρινήζεται)
- *--hostname NAME*: Set NAME as the hostname of the guest.
- *--mask VALUE*: μάσκα IP σε μορφή με τελεές (εξορισμός: 255.255.255.0)
- *--net VALUE*: IP διεθυσνη δικτύου (εξορισμός: X.X.X.0)
- *--bcast VALUE*: IP εκπομπής (εξορισμός: X.X.X.255)
- *--gw ADDRESS*: διεθυσνη πυλήνα (εξορισμός: X.X.X.1)
- *--dns ADDRESS*: Διεθυσνη ονόματος διακομιστή (εξορισμός: X.X.X.1)

Υποθτούμε για τήρα τι η τιμές εξορισμός είναι αρκετά καλές, έτσι η προκπτούσα επκλήση γνεται:

```
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. #####

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 [μμμ 1.4](#), [&x201C;#####&x201D](#); [41] for more information. Also, if the interface name is different change *br0* to the actual bridge interface.



## 2.3.2.2. ###μ###μ##

Ο διαμερισμός σε μια εικονική συσκευή θα πρέπει να ληφεί υπψιν τι σχεδιάζετε να κνέτε με αυτό. Επειδή οι περισσότερες συσκευές θλουν να χουν ξεχωριστό μσο αποθήκευσης για δεδομένα, το να χουν ένα ξεχωριστό */var* θα βγαζε νόημα.

Για να το κνουμε αυτό το `vmbuilder` μας παρχει 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 νόμα αρχείου κειμένου `vmbuilder.partition` το οποίο θα περιχει τα ακόλουθα:

`root 8000`

`swap 4000`

`---`

`/var 20000`



Σημειώστε ότι χρησιμοποιούμε εικόνες εικονικού δίσκου, τα πραγματικά μεγέθη που βζουμε εδώ είναι τα μγιστα μεγέθη αυτών των τμών.

Η γραμμή εντολών μας τ#ρα 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 επιτ#ψει μεγάλες συμβολοσειρές εντολών να αναδιπλ#νονται στην επ#μενη γραμμή.

## 2.3.2.3. #####

Ξαν# στ#νοντας μια εικονική συσκευή, θα πρέπει να παρ#χετε έναν εξορισμό χρ#στη και κωδικ# που θα είναι γενικ# #στε να μπορ#σετε να τα συμπεριλ#βετε στις βοηθητικές οδηγίες. Θα δο#με αργ#τερα σε αυτό το εγχειρίδιο πως θα παρ#χουμε ασφ#λεια ορ#ζοντας ένα σεν#ριο που θα εκτελε#ται την πρ#τη φορ# που ο χρ#στης εισ#ρχεται στη συσκευή, που, μεταξ# #λλων, θα του ζητ#ει να αλλ#ξει κωδικ#. Σε αυτό το παρ#δειγμα θα χρησιμοποι#σω το `'user'` σαν νόμα χρ#στη, και το `'default'` σαν κωδικ#.

Για να το κ#νουμε αυτ# χρησιμοποιο#με προαιρετικ#ς παραμ#τρους:

- `--user USERNAME`: Ορ#ζει το #νομα του χρ#στη που θα προστεθε#. Εξορισμο#: `ubuntu`.
- `--name FULLNAME`: Ορ#ζει το πλ#ρες #νομα το χρ#στη που θα προστεθε#. Εξορισμο#: `Ubuntu`.
- `--pass PASSWORD`: Ορ#ζει τον κωδικ# χρ#στη. Εξορισμο#: `ubuntu`.

Η προκ#πτουσα γραμμ# εντολ#ς γ#νεται:

```
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. #####μ#####

Σε αυτ# το παρ#δειγμα θα εγκαταστ#σουμε το πακ#το (Limesurvey) που #χει πρ#σβαση στη β#ση δεδομ#νων MySQL και #χει διεπαφ# ιστο#. Επομ#νως θα χρειαστο#με το Λειτουργικ# μας Σ#στημα να μας παρ#χει:

- Apache
- PHP
- MySQL
- OpenSSH Server
- Limesurvey (σαν εφαρμογ# παρ#δειγμα που #χουμε πακετ#ρει)

Αυτ# γ#νεται χρησιμοποιο#ντας το `vmbuilder` ορ#ζοντας την επιλογ# `--addpkg` πολλ#ς φορ#ς:

```
--addpkg PKG
##### ## PKG ##### (μ##### ## #####)
```

#μωσ, λ#γω του τρ#που που λειτουργε# το `vmbuilder`, τα πακ#τα που πρ#πει να κ#νουν ερωτ#σεις στον χρ#στη κατ# τη δι#ρκεια της φ#σης πριν την εγκατ#σταση δεν υποστηρ#ζονται και πρ#πει αντ# αυτ#ν να εγκατασταθο#ν #ταν μπορε# να συμβε# διαδραστικ#τητα. Αυτ# ε#ναι η περ#πτωση Limesurvey, την οπο#α θα πρ#πει να εγκαταστ#σουμε αργ#τερα, #ταν συνδεθε# ο χρ#στης.

#λλα πακ#τα που ρωτο#ν απλ# ερ#τηση `debconf`, #πως ο `mysql-server` που ζητ#ει να οριστε# κωδικ#ς, το πακ#το μπορε# να εγκατασταθε# αμ#σως, αλλ# θα πρ#πει να το αναδιαμορφ#σουμε την πρ#τη φορ# που θα συνδεθε# ο χρ#στης.

Ε#ν κ#ποια πακ#τα που πρ#πει να εγκαταστ#σουμε δεν ε#ναι στο `main`, πρ#πει να ενεργοποι#σουμε τα επιπλ#ον αποθετ#ρια χρησιμοποιο#ντας `--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.
```

Εφ#σον το Limesurvey δεν ε#ναι μ#ρος του αρχε#ου αυτ# τη στιγμ#, θα ορ#σουμε τη διε#θυνση PPA (αρχε#ο προσωπικο# πακ#του) #στε να προστεθε# στο VM /etc/apt/source.list, #ρα προσθ#τουμε τις ακ#λουθες επιλογ#ς στην γραμμ# εντολ#ν:

```
--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. #####

#### 2.3.4.1. #####

#ταν το vmbuilder δημιουργε# το σ#στημ# σας, πρ#πει να μεταφ#ρει καθ#να απ# τα πακ#τα που το απαρτ#ζουν απ# το διαδ#κτυο απ# #να απ# τα επ#σημα αποθετ#ρια, το οπο#ο, αν#λογα με το σ#στημ# σας και την ταχ#τητα της σ#νδεσ#ς σας με το διαδ#κτυο και το φ#ρτο του mirror, μπορε# να #χει μεγ#λη επ#δραση στον πραγματικ# χρ#νο δημιουργ#ας. Για να μειωθε#, συν#σταται να #χετε ε#τε #να τοπικ# αποθετ#ριο (το οπο#ο μπορε# να δημιουργηθε# με τη χρ#ση του apt-mirror) ε#τε να χρησιμοποι#σετε #ναν proxy προσωριν#ς αποθ#κευσης #πως το apt-proxy. Η δε#τερη επιλογ# ε#ναι πιο απλ# στην υλοπο#ηση και απαιτε# λιγ#τερο χ#ρο, #τσι την επιλ#ξαμε για αυτ# το μ#θημα. Για να το εγκαταστ#σετε, απλ# πληκτρολογ#στε:

```
sudo apt-get install apt-proxy
```

#ταν ολοκληρωθε# αυτ#, ο (#δειος) διαμεσολαβητ#ς σας ε#ναι #τοιμος για χρ#ση στο http://mirroraddress:9999 και θα βρε#τε το αποθετ#ριο ubuntu στο /ubuntu. Για να το χρησιμοποι#σει το vmbuilder, θα πρ#πει να χρησιμοποι#σουμε την επιλογ# --mirror:

```
--mirror=URL ##### ## ##### Ubuntu ### URL ##### #####
http://archive.ubuntu.com/ubuntu for official
arches and http://ports.ubuntu.com/ubuntu-ports
otherwise
```

#ρα προσθ#τουμε στη γραμμ# εντολ#ς:

```
--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 reseting this address later on.

#### 2.3.4.2. #####

Εν εμάστε σε να μεγαλύτερο περιβλλον, μπορε να χει νημα να στσουμε ναν τοπικ καθρφη τον αποθετηρων Ubuntu. Το πακτο apt-mirror παρχει να σενριο το οποο χειρζεται τη δημιουργα καθρεφτην για εςς. Πρπει να υπολογσετε να χετε περπου 20 gigabyte ελεθερου χρου αν υποστηριζμενη κδοση και αρχιτεκτονικ#.

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
```

Παρατηρεστε τι τα πακτα πηγς δεν ενα στον καθρφη καθς χρησιμοποιοονται σπνια σε σχση με τα binaries και δεν πινουν πολ χρο, αλλ μπορο ν εκολα να προστεθο ν στη λστα.

ταν ο καθρφτης τελεισει την αντιγραφ (και αυτ μπορε να διαρκσει πολ), πρπει να ρυθμσετε τον Apache στε τα αρχεα καθρφη σας (στο /var/spool/apt-mirror ε ν δεν αλλξάτε την προεπιλογ), να εκδδονται απ τον διακομιστ Apache. Για περισστερες πληροφορες στον Apache δετε μμ 1, &#x201C;HTTPD - Apache2 #####&#x201D; [194].

#### 2.4. # #####

Δο επιλογς ε να διαθσιμες σε εμς:

- Η προτεινμενη μθοδος για να το κνετε ε να να δημιουργσετε να πακτο Debian. Μιας και αυτ ε να εκτς πεδου εφαρμογς αυτο του εχειριδου, δε θα το

εκτελ#sουμε εδ# και θα καλ#sουμε το χρ#στη να διαβ#σει τις βοηθητικ#ς οδηγ#ες για το πω# να το κ#νει στο *Ubuntu Packaging Guide*<sup>10</sup>. Σε αυτ# την περ#πτωση ε#ναι επ#σης καλ# ιδ#α να στ#σετε #να αποθετ#ριο για το πακ#το #στε οι ενημερ#σεις να τις τραβ#ξετε βολικ# απ# εκε#. Δε#τε το #ρθρο *Debian Administration*<sup>11</sup> για #να εγχειρ#διο οδηγι#ν π#νω σε αυτ#.

- Εγκαταστ#στε την εφαρμογ# χειροκ#νητα στο /opt #πως συν#σταται απ# τις ##### μ#μ# FHS<sup>12</sup>.

Στην περ#πτωσ# μας θα χρησιμοποι#sουμε το Limesurvey σαν παρ#δειγμα εφαρμογ#ς ιστο# για την οπο#α επιθυμ#με να παρ#χουμε μια εικονικ# συσκευ#. #πως επισημ#νθηκε πριν, #χουμε δημιουργ#σει #κδοση του πακ#του διαθ#σιμο στο PPA (Αρχε#ο Προσωπικο# Πακ#του).

## 2.5. #####

### 2.5.1. #####

Για να διαμορφωθε# το σ#στημ# σας #στε να ενημερ#νεται αυτ#ματα σε τακτικ# β#ση, θα εγκαταστ#sουμε απλ# το `unattended-upgrades`, #ρα προσθ#τουμε την ακ#λουθη επιλογ# στη γραμμ# εντολ#ς μας:

```
--addpkg unattended-upgrades
```

Καθ#ς #χουμε β#λει το πακ#το εφαρμογ#ς μας στο PPA, η διαδικασ#α θα ενημερ#σει #χι μ#νο το σ#στημα, αλλ# και την εφαρμογ# κ#θε φορ# που ενημερ#νουμε την #κδοση στο PPA.

### 2.5.2. ##### ACPI

Για να μπορε# να διαχειρ#ζεται η εικονικ# σας μηχαν# γεγον#τα εκκ#νησης και τερματισμ#, ε#ναι καλ# ιδ#α να εγκαταστ#σετε το πακ#το `acpid` επ#σης. Για να το κ#νουμε αυτ# απλ# προσθ#τουμε την ακ#λουθη επιλογ#:

```
--addpkg acpid
```

## 2.6. #####

Εδ# ε#ναι η εντολ# με #λες τις επιλογ#ς που συζητ#θηκαν παραπ#νω:

```
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 \
```

<sup>10</sup> <https://wiki.ubuntu.com/PackagingGuide>

<sup>11</sup> <http://www.debian-administration.org/articles/286>

<sup>12</sup> <http://www.pathname.com/fhs/>

```
--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. #####

Εάν ενδιαφέρεστε να μ#θετε περισσ#τερα, #χετε απορ#ες # προτ#σεις, παρακαλ# επικοινων#στε με την Ομ#δα Διακομιστ# Ubuntu στο:

- IRC: #ubuntu-server on freenode
- Λ#στα Ηλεκτρονικ#ς Αλληλογραφ#ας: *ubuntu-server at lists.ubuntu.com*<sup>13</sup>
- Επ#σης δε#τε τη σελ#δα *JeOSVMBuilder Ubuntu Wiki*<sup>14</sup>.

---

<sup>13</sup> <https://lists.ubuntu.com/mailman/listinfo/ubuntu-server>

<sup>14</sup> <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. #####**

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. #####μ###**

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 -ml 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.html](http://swift.openstack.org/development_saio.html) <sup>15</sup>.

### 3.8. Support and Troubleshooting

Community Support

- *OpenStack Mailing list*<sup>16</sup>
- *The OpenStack Wiki search*<sup>17</sup>
- *Launchpad bugs area*<sup>18</sup>
- Join the IRC channel #openstack on freenode.

### 3.9. #####

- *Cloud Computing - Service models*<sup>19</sup>
- *OpenStack Compute*<sup>20</sup>
- *OpenStack Image Service*<sup>21</sup>
- *OpenStack Object Storage Administration Guide*
- *Installing OpenStack Object Storage on Ubuntu*<sup>22</sup>
- <http://cloudglossary.com/>

### 3.10. #####

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.

---

<sup>15</sup> [http://swift.openstack.org/development\\_saio.html](http://swift.openstack.org/development_saio.html)

<sup>16</sup> <https://launchpad.net/~openstack>

<sup>17</sup> <http://wiki.openstack.org>

<sup>18</sup> <https://bugs.launchpad.net/nova>

<sup>19</sup> [http://en.wikipedia.org/wiki/Cloud\\_computing#Service\\_Models](http://en.wikipedia.org/wiki/Cloud_computing#Service_Models)

<sup>20</sup> [docs.openstack.org/trunk/openstack-compute/](https://docs.openstack.org/trunk/openstack-compute/)

<sup>21</sup> <http://docs.openstack.org/diablo/openstack-compute/starter/content/GlanceMS-d2s21.html>

<sup>22</sup> <http://docs.openstack.org/trunk/openstack-object-storage/admin/content/installing-openstack-object-storage-on-ubuntu.html>

- *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. #####**

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 [Apparmor \[354\]](#) 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 IV 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 re-usable abstractions file `/etc/apparmor.d/abstractions/lxc/container-base`. An easy way to start a new profile therefore is to do the same, then add extra permissions at the bottom of your policy.

After creating the policy, load it using:

```
sudo apparmor_parser -r /etc/apparmor.d/lxc-containers
```

The profile will automatically be loaded after a reboot, because it is sourced by the file `/etc/apparmor.d/lxc-containers`. Finally, to make container `CN` use this new `lxc-CN-profile`, add the following line to its configuration file:

```
lxc.aa_profile = lxc-CN-profile
```

**`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/default/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 oneiric1 -- -r oneiric
```

passes the arguments `'-r oneiric1'` 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 *jdoo* from the host into the container using the *-b jdoo* option. This will copy *jdoo*'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 *lxcgust* package will be automatically installed. Alternatively, if the *--trim* option is specified, then the *lxcgust* 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  $\leq 14$ . *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 [4.3.6, &#x201C;Consoles&#x201D; \[362\]](#) 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 [4.3.5, &#x201C;Monitoring container status &#x201D; \[362\]](#)) 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](#)<sup>23</sup> for more).

---

<sup>23</sup> <https://www.ibm.com/developerworks/linux/library/l-lxc-containers/>

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...
  ...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 [4.4.5, &#x201C;Other configuration options&#x201D; \[368\]](#) 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 [4.10, &#x201C;#####&#x201D; \[373\]](#) 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
lxc-cgroup	View and set container control group settings
lxc-checkconfig	Verify host support for containers
lxc-checkpoint	(NOT SUPPORTED) Checkpoint a running container
lxc-clone	Clone a new container from an existing one
lxc-console	Open a console in a running container
lxc-create	Create a new container
lxc-destroy	Destroy an existing container
lxc-execute	Run a command in a (not running) application container
lxc-freeze	Freeze a running container
lxc-info	Print information on the state of a container
lxc-kill	Send a signal to a container's init
lxc-list	List all containers
lxc-ls	List all containers with shorter output than lxc-list
lxc-monitor	Monitor state changes of one or more containers
lxc-netstat	Execute netstat in a running container
lxc-ps	View process info in a running container
lxc-restart	(NOT SUPPORTED) Restart a checkpointed container
lxc-restore	Restore containers from backups made by lxc-backup
lxc-setcap	(NOT RECOMMENDED) Set file capabilities on LXC tools
lxc-setuid	(NOT RECOMMENDED) Set or remove setuid bits on LXC tools
lxc-shutdown	Safely shut down a container
lxc-start	Start a stopped container

Command	Synopsis
<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. #####

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 [#4.2.6, &#x201C;Apparmor&#x201D; \[354\]](#) 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.devttydir** 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 [#4.3.4, \*Lifecycle management hooks\*; \[361\]](#) 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 [#4.3.4, \*Lifecycle management hooks\*; \[361\]](#), 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 [#4.9, \*#####\*; \[373\]](#) 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

*4.3.1, &#x201C;Creating Containers&#x201D; [356]* 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. #####

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 [4.2.6, Apparmor](#); [354]

### 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 [4.4.5, Other configuration options](#); [368] for details of how to configure a container to use seccomp. By default, no seccomp policy is loaded.

## 4.10. #####

- The DeveloperWorks article *LXC: Linux container tools*<sup>24</sup> was an early introduction to the use of containers.
- The *Secure Containers Cookbook*<sup>25</sup> demonstrated the use of security modules to make containers more secure.
- Manual pages referenced above can be found at:

---

<sup>24</sup> <https://www.ibm.com/developerworks/linux/library/l-lxc-containers/>

<sup>25</sup> <http://www.ibm.com/developerworks/linux/library/l-lxc-security/index.html>

*capabilities*<sup>26</sup>

*lxc.conf*<sup>27</sup>

- The upstream LXC project is hosted at *Sourceforge*<sup>28</sup>.
- LXC security issues are listed and discussed at *the LXC Security wiki page*<sup>29</sup>
- 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.

---

<sup>26</sup> <http://manpages.ubuntu.com/manpages/en/man7/capabilities.7.html>

<sup>27</sup> <http://manpages.ubuntu.com/manpages/en/man5/lxc.conf.5.html>

<sup>28</sup> <http://lxc.sf.net>

<sup>29</sup> <http://wiki.ubuntu.com/LxcSecurity>

---

## Κεφάλαιο 21. Σύσχεση

# 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 ξεκιν#σετε να χρησιμοποιε#τε το `drbd`, πρ#τα εγκαταστ#στε τα απαρα#τητα πακ#τα. Σε #να τερματικ# πληκτρολογ#στε:

```
sudo apt-get install drbd8-utils
```



Αν χρησιμοποιε#τε τον ##### ως μ#ρος μιας εικονικ#ς μηχαν#ς, θα πρ#πει να μεταγλωττ#σετε (compile) χειροκ#νητα την μον#δα `drbd`. Μπορε# να ε#ναι ευκολ#τερο να εγκαταστ#σετε το πακ#το `linux-server` στην εικονικ# μηχαν#.

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. #####

Οι δ#ο υπολογιστ#ς σε αυτ# το παρ#δειγμα θα ονομαστο#ν `drbd01` και `drbd02`. Θα πρ#πει να #χουν ρυθμισμ#νη επ#λυση ονομ#των (name resolution) ε#τε μ#σα απ# DNS # με το αρχε#ο `/etc/hosts`. Δε#τε το ##### 8, ##### μ##### μ## (DNS) [141] για λεπτομ#ρειες.

- Για να ρυθμ#σετε το `drbd`, στο πρ#το μηχ#νημα επεξεργαστε#τε 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;
    }
}

```



Υπ#ρχουν πολλ#ς #λλες επιλογ#ς στο `/etc/drbd.conf`, αλλ# για αυτ# το παρ#δειγμα, οι προεπιλεγμ#νες τιμ#ς ε#ναι καλ#ς.

- Τ#ρα αντιγρ#ψτε το `/etc/drbd.conf` στο δε#τερο μηχ#νημα:

```
scp /etc/drbd.conf drbd02:~
```

- Και στο `drbd02` μετακιν#στε το αρχε#ο στο `/etc`:

```
sudo mv drbd.conf /etc/
```

- Τ#ρα, χρησιμοποιο#ντας το εργαλε#ο `drbdadm`, αρχικοποι#στε την αποθ#κευση μετα# δεδομ#νων. Σε κ#θε εξυπηρετητ# εκτελ#στε:

```
sudo drbdadm create-md r0
```

- Μετ#, και στα δ#ο μηχαν#ματα, εκκιν#στε την υπηρεσ#α `drbd`:

```
sudo service drbd start
```

- Στο `drbd01`, # σε οποιοδ#ποτε σ#στημα θ#λετε να ε#ναι το πρωτε#ον (primary), πληκτρολογ#στε το ακ#λουθο:

```
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 σταματ#σετε να παρακολουθε#τε τα αποτελ#σματα, πι#στε `Ctrl+c`.

- Τ#λος, προσθ#στε #να σ#στημα αρχε#ων στο `/dev/drbd0` και προσαρτ#στε το:

```

sudo mkfs.ext3 /dev/drbd0
sudo mount /dev/drbd0 /srv

```

## 1.2. #####μ#

Για να ελ#γξετε πως τα δεδομ#να συγχρον#ζονται πραγματικ# μεταξ# των υπολογιστ#, αντιγρ#ψτε κ#ποια αρχε#α στον `drbd01`, τον πρωτε#οντα, στο `/srv`:

```
sudo cp -r /etc/default /srv
```

Μετ#, αποπροσαρτ#στε το /srv:

```
sudo umount /srv
```

##### τον ##### εξυπηρετητ# στον ρ#λο του #####:

```
sudo drbdadm secondary r0
```

Τ#ρα στον ##### εξυπηρετητ# ##### το στον ρ#λο του #####:

```
sudo drbdadm primary r0
```

Τ#λος, προσαρτ#στε την κατ#τμηση:

```
sudo mount /dev/drbd0 /srv
```

Χρησιμοποι#ντας την εντολ# *ls* θα πρ#πει να δε#τε το /srv/default αντιγραμμ#νο απ# τον πρ#ην ##### υπολογιστ# *drbd01*.

### 1.3. #####

- Για περισσ#τερες πληροφορ#ες για το DRBD, δε#τε τον ##### *DRBD*<sup>1</sup>.
- The *drbd.conf man page*<sup>2</sup> contains details on the options not covered in this guide.
- Also, see the *drbdadm man page*<sup>3</sup>.
- The *DRBD Ubuntu Wiki*<sup>4</sup> page also has more information.

---

<sup>1</sup> <http://www.drbd.org/>

<sup>2</sup> <http://manpages.ubuntu.com/manpages/raring/en/man5/drbd.conf.5.html>

<sup>3</sup> <http://manpages.ubuntu.com/manpages/raring/en/man8/drbdadm.8.html>

<sup>4</sup> <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. #####μ####

Για να εγκαταστήσετε το openvpn πληκτρολογήστε σε ένα τερματικό:

```
sudo apt-get install openvpn
```

## 1.2. ##μ#### #####μ##

The first step in building an OpenVPN configuration is to establish a PKI (public key infrastructure). The PKI consists of:

- ένα ξεχωριστό πιστοποιητικό (επής 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. #####

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/
```

Μετ#, επεξεργαστε#τε το `/etc/openvpn/easy-rsa/vars` προσαρμ#ζοντας τα ακ#λουθα στο περιβ#λλον 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"
```

Πληκτρολογ#στε τα παρακ#τω για να δημιουργ#σετε τον κ#ριο πιστοποιητικ# συγγραφ#α (CA) πιστοποιητικ# και κλειδ#:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-ca
```

### 1.2.2. ##### μ#####

Στη συν#χεια, θα δημιουργ#σει #να πιστοποιητικ# και το ιδιωτικ# κλειδ# για το διακομιστ#:

```
./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
```

#λα τα πιστοποιητικ# και τα κλειδι# #χουν δημιουργηθε# στον υποκατ#λογο κλειδι#/. Η κοιν# πρακτικ# ε#ναι να τα αντιγρ#ψετε στο `/etc/openvpn/`:

```
cd keys/
cp myservername.crt myservername.key ca.crt dh1024.pem /etc/openvpn/
```

### 1.2.3. #####

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
```

Αντιγρ#ψτε τα ακ#λουθα αρχε#α στον πελ#τη χρησιμοποι#ντας μια ασφαλ# μ#θοδο:

- /etc/openvpn/ca.crt
- /etc/openvpn/easy-rsa/keys/client1.crt
- /etc/openvpn/easy-rsa/keys/client1.key

Δεδομένου ότι μνο τα πιστοποιητικά πελτη και τα κλειδιά απαιτούνται στο μηχνημα του πελτη, θα πρέπει να τα αποσρετε απ τον διακομιστ.

### 1.3. ##### μ#### μ##### μ#####

Μαζ με την εγκατσταση OpenVPN πηρατε για δεγμα αυτ τα αρχεα ρυθμσεων (και πολλ περιστερα, αν, αν επιλξετε):

```
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
```

Ξεκινστε με την αντιγραφ και την αποσυμπεση του server.conf.gz στο φκελο /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 ]
```

Τρα, ελγξε αν το OpenVPN δημιοργησε να περιβλλον 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. #####

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
```

Αντιγράψτε το αρχείο `client.conf` δεγμά 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 ξεκινάτε 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 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
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.

Ελ#γξτε τις διαδρομ#ς 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. #####μ#####μ####

Πρ#τη αντιμετ#πιση προβλημ#των

- Ελ#γξτε το syslog σας · π.χ. `grep -i vpn /var/log/syslog`
- Μπορε# ο πελ#της να συνδεθε# με το μηχ#νημα του διακομιστ#; #σως #να τε#χος προστασ#ας εμποδ#ζει την πρ#σβαση; Ελ#γξτε το syslog του διακομιστ#.
- Πελ#της και διακομιστ#ς πρ#πει να χρησιμοποιο#ν το #διο πρωτ#κολλο και θ#ρα, π.χ. θ#ρα UDP 1194, δε#τε θ#ρα και επιλογ#ς ρυθμ#σεων πρωτοκ#λλου
- Πελ#της και διακομιστ#ς πρ#πει να χρησιμοποιο#ν #διες ρυθμ#σεις σχετικ# με τη συμπ#εση, δε#τε το αρχε#ο `comp-lzo` επιλογ# ρυθμ#σεων
- 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. #####μ#####μ##### VPN ### #####μ####

Το παραπ#νω ε#ναι πολ# απλ# εργ#ζομενος με VPN. Ο πελ#της μπορε# να #χει πρ#σβαση στις υπηρεσ#ες της μηχαν#ς διακομιστ# VPN μ#σα απ# μια κρυπτογραφημ#νη σ#ραγγα. Αν θ#λετε να προσεγγ#σετε περισσ#τερους διακομιστ#ς # οτιδ#ποτε σε #λλα δ#κτυα, ωθ#στε ορισμ#νες γραμμ#ς προς τους πελ#τες. Π.χ. Ε#ν το δ#κτυο της εταιρε#ας σας μπορε# να συνοψιστε# στο δ#κτυο 192.168.0.0/16, θα μπορο#σατε να ωθ#σετε αυτ# τη γραμμ# προς τους πελ#τες. Αλλ# θα πρ#πει επ#σης να αλλ#ξει η δρομολ#γηση για το δρ#μο της επιστροφ#ς - διακομιστ#ς σας πρ#πει να γνωρ#ζουν μια διαδρομ# προς το δ#κτυο του πελ#τη VPN.

# μπορε# να ωθ#σει μια προεπιλεγμ#νη π#λη για #λους τους πελ#τες να στε#λει #λη την κυκλοφορ#α τους στο διαδ#κτυο μ#σω της π#λης VPN πρ#τα και απ# εκε# μ#σω του τε#χους προστασ#ας της εταιρε#ας στο διαδ#κτυο. Αυτ# το τμ#μα σας δε#χνει μερικ#ς πιθαν#ς επιλογ#ς.

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 ip.txt
```

Πι#στε διακομιστ#ς DNS για τον πελ#τη.

```
push "dhcp-option DNS 10.0.0.2"
```

```
push "dhcp-option DNS 10.1.0.2"
```

Επιτρ#ψτε την επικοινων#α πελ#τη σε πελ#τη

```
client-to-client
```

Ενεργοπο#ηση συμπ#εσης στη σ#νδεση 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 #####<sup>1</sup> για περαιτέρω συμβουλές σε θέματα ασφαλείας.

#### 1.6.2. ##### VPN ### #####

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. #####

Make sure you have the `bridge-utils` package installed:

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

Before you setup OpenVPN in bridged mode you need to change your interface configuration. Let's assume your server has an interface `eth0` connected to the internet and an interface `eth1` connected to the LAN you want to bridge. Your `/etc/network/interfaces` would like this:

```
auto eth0
iface eth0 inet static
address 1.2.3.4
netmask 255.255.255.248
default 1.2.3.1
```

---

<sup>1</sup> <http://openvpn.net/index.php/open-source/documentation/howto.html#security>



```

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 έχετε προετοιμασμένοι ότι αυτό δεν θα μπορεί να λειτουργήσει όπως αναμένετε και τι θα χέσετε την απομακρυσμένη σύνδεση. Βεβαιωθείτε ότι μπορείτε να λύσετε τα προβλήματα χοντάς τοπικά πρόσβαση.

```
sudo service network restart
```

1.6.2.2. #####

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 συν#χεια το κ#νετε εκτελ#σιμο:

```
sudo chmod 755 /etc/openvpn/up.sh
```

Αφο# διαμορφ#σετε το διακομιστ#, επανεκκιν#στε το openvpn πληκτρολογ#ντας:

```
sudo service openvpn restart
```

1.6.2.3. #####

Πρ#τα εγκαταστ#στε το openvpn στον (υπολογιστ#) πελ#τη:

```
sudo apt-get install openvpn
```

Στη συν#χεια με το διακομιστ# ρυθμισμ#νο και τα πιστοποιητικ# του πελ#τη αντιγραμμ#να στον κατ#λογο /etc/openvpn/, δημιουργ#στε #να αρχε#ο διαμ#ρφωσης πελ#τη, αντιγρ#φοντας το παρ#δειγμα. Σε #να τερματικ# στο μηχ#νημα πελ#τη εισ#γετε:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn
```

Τ#ρα επεξεργαστε#τε το /etc/openvpn/client.conf αλλ#ζοντας τις ακ#λουθες επιλογ#ς:

```
dev tap
```

```
;dev tun
```

Τ#λος, επανεκκιν#στε το openvpn:

```
sudo service openvpn restart
```

Τ#ρα θα πρ#πει να μπορε#τε να συνδεθε#τε στο απομακρυσμ#νο LAN μ#σω του VPN.

## 1.7. #####

### 1.7.1. Linux ##### GUI ### ## 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 γράψει 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 ### 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.

```
# ##### client.ovpn ### ## 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 µ# GUI ### Win 7

First download and install the latest *OpenVPN Windows Installer*<sup>2</sup>. 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 it's startup type to automatic. When you start the OpenVPN MI GUI the first time you need to run it as an administrator. You have to right click on it and you will see that option.

You will have to write your OpenVPN config in a textfile and place it in C:\Program Files\OpenVPN\config\client.ovpn along with the CA certificate. You could put the user certificate in the user's home directory like in the 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
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 ### 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

---

<sup>2</sup> <http://www.openvpn.net/index.php/open-source/downloads.html>

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*<sup>3</sup>. And here is the OpenWRT project's homepage: <http://openwrt.org>

Συνδεθείτε στο OpenWRT δρομολογητή σας και εγκαταστήστε το OpenVPN:

```
opkg ##μ#####  
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 τεχνούς προστασίας.

## 1.8. #####

- Δείτε την ιστοσελίδα *OpenVPN*<sup>4</sup> για περισσότερες πληροφορίες.
- *OpenVPN hardening security guide*<sup>5</sup>
- Επίσης, το *OpenVPN: Building and Integrating Virtual Private Networks*<sup>6</sup> είναι ένας καλός πηρος.

---

<sup>3</sup> <http://wiki.openwrt.org/doc/howto/vpn.overview>

<sup>4</sup> <http://openvpn.net/>

<sup>5</sup> <http://openvpn.net/index.php/open-source/documentation/howto.html#security>

<sup>6</sup> <http://www.packtpub.com/openvpn/book>

---

## Κεφάλαιο 23. Άλλες Χρήσιμες Εφαρμογές

Υπάρχουν πολλές πολύ χρήσιμες εφαρμογές αναπτυγμένες από την Ομάδα Διακομιστών Ubuntu, και άλλες η οποία είναι καλές ενσωματωμένες στην έκδοση Διακομιστών 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, # πολλών διακομιστών Ubuntu, πολύ πιο εύκολη.

## 1. pam motd

Όταν εισήρθε σε ένα διακομιστή Ubuntu μπορεί να έχετε προσέξει το ενημερωτικό Μηνύμα της Ημέρας (MTH). Αυτά οι πληροφορίες αποκτούνται και προβλλονται 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 προβλλονται 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 Ωκεανία και Ατμοσφαιρική Διαχείριση και προβλλεί από την Εθνική Υπηρεσία Καιρού. Για να βρείτε τοπικές πληροφορίες θα χρειαστείτε την τετραψφία #νδείξη τοποθεσίας ICAO. Αυτή μπορεί να προσδιοριστεί κλώνοντας περιήγηση της ιστοσελίδας #####<sup>1</sup>.

Παράλο που η Εθνική Υπηρεσία Καιρού είναι αντιπροσωπευτική της κυβέρνησης των Ηνωμένων Πολιτειών υπάρχουν σταθμοί καιρού διαθέσιμοι σε όλο τον κόσμο. Παράλλα αυτό 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 καιρό με την τοπική #νδείξη ICAO:

```
#!/bin/sh
#
#
# Prints the local weather information for the MOTD.
#
#
# Replace KINT with your local weather station.
# Local stations can be found here: http://www.weather.gov/tg/siteloc.shtml
```

<sup>1</sup> <http://www.weather.gov/tg/siteloc.shtml>

```
echo
weather -i KINT
echo
```

- Κ#ντε το σεν#ριο εκτελ#σιμο:

```
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` επιτρ#πει τα περιεχ#μενα του `/etc` να αποθηκε#ονται ε#κολα στο αποθετ#ριο Συστ#ματος Ελ#γχου #κδοσης (ΣΕΕ). Αγκιστρ#νει στο `apt` για να παραδ#δει αυτ#ματα αλλαγ#ς στο `/etc` #ταν εγκαθιστ#νται # αναβαθμ#ζονται πακ#τα. Τοποθετ#ντας το `/etc` κ#τω απ# τον #λεγχο #κδοσης θεωρε#ται β#λτιστη πρακτικ# του κλ#δου, και ο στ#χος του `etckeeper` ε#ναι να κ#νει αυτ# τη διαδικασ#α #σο πιο αν#δυνη γ#νεται.

Εγκαταστ#στε το `etckeeper` πληκτρολογ#ντας τα ακ#λουθα σε #να τερματικ#:

```
sudo apt-get install etckeeper
```

Το κ#ριο αρχε#ο διαμ#ρφωσης `/etc/etckeeper/etckeeper.conf`, ε#ναι σχετικ# απλ#. Η κ#ρια επιλογ# ε#ναι ποιος ΕΕΣ να χρησιμοποιηθε#. Εξορισμο# το `etckeeper` ε#ναι διαμορφωμ#νο να χρησιμοποιε# το `bzr` για #λεγχο #κδοσης. Το αποθετ#ριο αρχικοποιε#ται αυτ#ματα (και παραδ#δεται για πρ#τη φορ#) κατ# την εγκατ#σταση του πακ#του. Ε#ναι πιθαν# να το αναιρ#σετε αυτ# πληκτρολογ#ντας την ακ#λουθη εντολ#:

```
sudo etckeeper uninit
```

Εξορισμο#, το `etckeeper` θα παραδ#σει μη παραδοτ#ες αλλαγ#ς που γ#νονται στο `/etc` καθημερικ#. Αυτ# μπορε# να απενεργοποιηθε# χρησιμοποι#ντας την επιλογ# διαμ#ρφωσης `AVOID_DAILY_AUTOCOMMITS`. Θα παραδ#δει επ#σης αυτ#ματα αλλαγ#ς πριν και μετ# την εγκατ#σταση πακ#του. Για μ#α πιο ακριβ# καταγραφ# αλλαγ#ν, συστ#νεται να παραδ#νεται τις αλλαγ#ς χειροκ#νητα, μαζ# με #να μ#νυμα παρ#δοσης, χρησιμοποι#ντας:

```
sudo etckeeper commit "..##### ### ##### #####....."
```

Χρησιμοποι#ντας επιλογ#ς ΕΕΣ μπορε#τε να προβ#λετε πληροφορ#ες ιστορικο# στο `/etc`:

```
sudo bzr log /etc/passwd
```

Για να επιδε#ξετε την ολοκλ#ρωση με το σ#στημα διαχε#ρισης πακ#του, εγκαταστ#στε το `postfix`:

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

#ταν η εγκατ#σταση ολοκληρωθε#, #λα τα αρχε#α διαμ#ρφωσης `postfix` θα πρ#πει να παραδοθο#ν στο αποθετ#ριο:

```
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 #να παρ#δειγμα για το πως το `etckeeper` ανιχνε#ει χειροκ#νητες αλλαγ#ς, προσθ#στε #να ν#ο κεντρικ# υπολογιστ# στο `/etc/hosts`. Χρησιμοποι#ντας το `bzr` μπορε#τε να δε#τε ποια αρχε#α #χουν τροποποιηθε#:

```
sudo bzr status /etc/
modified:
  hosts
```

Τ#ρα παραδ#στε τις αλλαγ#ς:

```
sudo etckeeper commit "new host"
```

Για περισσ#τερες πληροφορ#ες για το `bzr` βλ. [#μ#μ# 1, &#x201C;Bazaar&#x201D; \[283\]](#).

### **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:

- Προβολ# του μενο# Βο#θειας
- Change Byobu's background color
- Change Byobu's foreground color
- Toggle status notifications
- Αλλαγ# του συν#λου των δεσμευτικ#ν κλειδι#ν
- Αλλαγ# της συχν#τητας απ#δρασης
- Create new windows
- Διαχε#ριση των προεπιλεγμ#νων παραθ#ρων
- 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* - Μετακ#νηση του κ#ρσορα αριστερ# κατ# #ναν χαρακτ#ρα
- *j* - Μετακ#νηση του κ#ρσορα κ#τω κατ# μια γραμμ#
- *k* - Μετακ#νηση του κ#ρσορα π#νω κατ# μ#α γραμμ#
- *l* - Μετακ#νηση του κ#ρσορα δεξι# κατ# #να χαρακτ#τα
- *O* - Μετακ#νηση στην αρχ# της τρ#χουσας γραμμ#ς
- *\$* - Μετακ#νηση στο τ#λος της τρ#χουσας γραμμ#ς
- *G* - Μετακ#νηση στην ορισμ#νη γραμμ# (εξορισμο# στο τ#λος της διαθ#σιμης μν#μης)
- */* - Αναζ#τηση μπροστ#

- ? - Αναζ#τηση π#σω
- $n$  - Μετακ#νηση στο επ#μενο τα#ριασμα, ε#τε μπροστ# ε#τε π#σω

#### **4. #####**

- See the *update-motd man page*<sup>2</sup> for more options available to update-motd.
- Το #ρθο για Debian Πακ#το της Ημ#ρας #####<sup>3</sup> #χει περισσ#τερες λεπτομ#ρειες για τη χρ#ση της λειτουργ#ας καιρο#
- Δε#τε την ιστοσελ#δα *etckeeper*<sup>4</sup> για περισσ#τερες λεπτομ#ρειες για τη χρ#ση του etckeeper.
- The *etckeeper Ubuntu Wiki*<sup>5</sup> page.
- Για τα τελευτα#α ν#α και πληροφορ#ες για το bzi δε#τε την ιστοσελ#δα *bzi*<sup>6</sup>.
- Για περισσ#τερες πληροφορ#ες για την οθ#νη δε#τε την #####<sup>7</sup>.
- And the *Ubuntu Wiki screen*<sup>8</sup> page.
- Also, see the *byobu project page*<sup>9</sup> for more information.

---

<sup>2</sup> <http://manpages.ubuntu.com/manpages/raring/en/man1/update-motd.1.html>

<sup>3</sup> <http://debaday.debian.net/2007/10/04/weather-check-weather-conditions-and-forecasts-on-the-command-line/>

<sup>4</sup> <http://kitenet.net/~joey/code/etckeeper/>

<sup>5</sup> <https://help.ubuntu.com/community/etckeeper>

<sup>6</sup> <http://bazaar-vcs.org/>

<sup>7</sup> <http://www.gnu.org/software/screen/>

<sup>8</sup> <https://help.ubuntu.com/community/Screen>

<sup>9</sup> <https://launchpad.net/byobu>

---

## Παράρτημα **A. 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*<sup>1</sup> to track its bug reports. In order to file a bug about Ubuntu Server on Launchpad, you will need to *create an account*<sup>2</sup>.

### **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 ##### 3, ##### [21] 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.
```

```
.....
```

---

<sup>1</sup> <https://launchpad.net/>

<sup>2</sup> <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 [##### 3, ##### \[21\]](#) 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. #####

- See the *Reporting Bugs*<sup>3</sup> Ubuntu wiki page.
- Also, the *Apport*<sup>4</sup> page has some useful information. Though some of it pertains to using a GUI.

---

<sup>3</sup> <https://help.ubuntu.com/community/ReportingBugs>

<sup>4</sup> <https://wiki.ubuntu.com/Apport>