



Community Experience Distilled

Learning Zimbra Server Essentials

Learn to use the robust Zimbra server like a pro using this practical, hands-on guide

Abdelmonam Kouka

[PACKT]
PUBLISHING

Learning Zimbra Server Essentials

Learn to use the robust Zimbra server like a pro using this practical, hands-on guide

Abdelmonam Kouka



BIRMINGHAM - MUMBAI

Learning Zimbra Server Essentials

Copyright © 2013 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: October 2013

Production Reference: 1171013

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78328-139-8

www.packtpub.com

Cover Image by Prashant Timappa Shetty (sparkling.spectrum.123@gmail.com)

Credits

Author

Abdelmonam Kouka

Project Coordinator

Akash Poojary

Reviewers

Danny Allen

Viorel Anghel

Maarten Vekens

Proofreader

Sandra Hopper

Indexer

Hemangini Bari

Acquisition Editor

Pramila Balan

Production Coordinator

Nitesh Thakur

Commissioning Editor

Manasi Pandire

Cover Work

Nitesh Thakur

Technical Editor

Siddhi Rane

Copy Editors

Tanvi Gaitonde

Aditya Nair

Kirti Pai

Laxmi Subramanian

About the Author

Abdelmonam Kouka is a Tunisian computer engineer. He got his engineering diploma in computer science in 2007 from one of the best engineering schools in Tunisia (ENSI), After this he got a master's degree in Information Security from the same school (ENSI) in 2009 and a master's degree in free and open source software from ISI/UVT in 2011. Starting from 2012 and until writing this book, he was a student at master level in Innovation Management (DICAMP.eu project).

He is not only a nonstop student; in fact, after getting his engineering degree in 2007, and in parallel to his masters marathon, he started working as a software developer in HR Access, and then a Zimbra consultant in another company. After that he came back to development with Alcatel-Lucent as a Java/JEE developer to finish with Alcatel-Lucent as an IP/MPLS Expert. He left Alcatel-Lucent in December 2012 to launch in partnership with his friend Ayed Akrouf, their own startup TAC-TIC (www.tac-tic.net), which provides ICT services such as software development, open source consulting, and IP/MPLS engineering and support.

Starting with his engineering study period and during all his professional experience, he was an open source activist, a member/co-founder of Ubuntu-tn community, Sabily community, and APOS association; he was also a member of Linux Arabic Community, Arabeyes, CULLT, DFSA, and a lot of other open source clubs and associations and initiatives.

I would like to thank my friend, my brother, and my partner Ayed Akrouf for his support and involvement in this project; this support was indispensable to realize this book. He helped me to prepare the lab in our TAC-TIC company to test every step described in this book.

I would also like to thank my mother Chadlia and my brother Iskander for their encouragement and support all the time during the work on this book, especially during long nights, my preferred time to prepare technical labs.

About the Reviewers

Danny Allen is a full-stack web developer who focuses on usability, localization, and accessibility issues as a founder and director of the user experience development consultancy, Wonderscore Ltd.

He is skilled across a wide range of technology including PHP, Python, JavaScript, HTML5, and CSS3. His recent work has involved design and implementation of e-learning and government projects in the United Kingdom.

He first encountered Zimbra many years ago when he wanted to set up his own e-mail server to handle the domains of his many side projects. At the time, Zimbra was not easy to set up – a book like this would have saved hours of frustration and been most helpful!

Viorel Anghel is an experienced system and network administrator with more than 15 years of experience in Linux and Unix. He is interested in high scalability, availability, and infrastructure management tools.

He is currently doing consulting work through Gemini Solutions (www.GeminiSols.com).

Maarten Vekens is a 32-year-old freelance system administrator. He is currently living currently in Brussels, Belgium.

He is an amateur cyclist who travels around the world and enjoys the cultural life.

He started his IT career 14 years ago, at one of the biggest Petrochemical companies in the world. After some other projects, he was asked to join the IT staff at Belga News Agency. During this project, he started to work with VMware Zimbra.

In 2012, he started his own company, TakeIToff (www.takeitoff.be), together with his best friend, Vincent Oomen. The main focus stays on system administration and program management.

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit www.PacktPub.com for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at service@packtpub.com for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.



<http://PacktLib.PacktPub.com>

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read, and search across Packt's entire library of books.

Why Subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On demand and accessible via web browser

Free Access for Packt account holders

If you have an account with Packt at www.PacktPub.com, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Table of Contents

Preface	1
Chapter 1: Single Server Installation	5
The prerequisites for Zimbra	5
Preparing the environment	6
Assumptions	6
System requirements	7
Installing the Ubuntu server	7
Preparing the OS (Ubuntu server) for the Zimbra installation	9
DNS configuration	10
Zimbra installation	17
Preinstallation	17
Installation	18
Running Zimbra for the first time	28
Summary	32
Chapter 2: Multiserver Installation	33
The prerequisites for Zimbra	33
Preparing the environment	34
Multiserver configuration examples	34
Assumptions	35
System requirements	36
Installing the Ubuntu server	36
Preparing Ubuntu for Zimbra installation	37
DNS configuration	37
Additional network configuration on the MTA server	44
Syncing servers	46
Installing Zimbra	47
Understanding the prerequisites	48
Package installation	48

Installing the first Zimbra server – LDAP master server	49
Installing Zimbra MTA on a server	57
Post installation	64
Running Zimbra for the first time	65
Summary	68
Chapter 3: Securing Zimbra	69
<hr/>	
Problems and issues	69
Internal solutions	70
Enabling DSPAM	70
Updating ClamAV independently of Zimbra updates	72
Step 1 – backing up your existing release	72
Step 2 – updating	72
Using ASSP with Zimbra	75
Improving SpamAssassin	77
salocal.cf.in	77
Sender Policy Framework (SPF)	79
Razor2	80
Pyzor	81
How to configure SpamAssassin	81
Adding DCC	83
External solutions	83
Barracuda spam and virus firewall	83
MailCleaner	84
IronPort	85
Maia Mailguard	85
Untangle	86
Summary	86
Chapter 4: Managing Configuration	87
<hr/>	
Understanding global configuration management	87
General global settings	89
Attachments	89
Global MTA settings	90
Global IMAP and POP settings	91
Configuration per COS	91
Managing server settings	92
General information	92
Services	93
MTA	94
IMAP/POP	94
Managing SSL certificates	95
Checking installed certificates	96
Installing certificates	96
Summary	97

Chapter 5: Configuring User Accounts	99
Managing user accounts	99
Creating user accounts	100
Creating aliases	101
Creating distribution lists	102
Creating resources	103
Customizing accounts	104
Summary	105
Chapter 6: Monitoring the Zimbra Server	107
Prerequisites	107
Monitoring servers	107
Review server status	108
Enable or disable server services	109
Server performance statistics	110
Configuring disk space notifications	111
Monitoring servers	111
Monitoring mailbox quotas	114
View quotas	114
Increase or decrease quotas	115
Monitoring authentication	115
Monitoring authentication failures	115
Viewing logfiles	117
Summary	118
Index	119

Preface

Learning Zimbra Server Essentials is a new book with a new concept. There is no big speech, just the essentials of essentials. This book is written by an open source expert who knows exactly what an expert needs—only necessary steps and useful tips, that's all.

This book is special as the author has both written and implemented what he is writing in a test lab environment; so by following it, you will get a real solution that works without any headache.

What this book covers

Chapter 1, Single Server Installation, serves as a quick installation guide for a single-server case.

Chapter 2, Multiserver Installation, provides an installation guide for a multiserver case.

Chapter 3, Securing Zimbra, serves as an administration guide to secure Zimbra.

Chapter 4, Managing Configuration, provides an administration guide to configure Zimbra.

Chapter 5, Configuring User Accounts, serves as an administration guide to configure user accounts.

Chapter 6, Monitoring the Zimbra Server, provides an IT guide for the Zimbra server.

What you need for this book

To use this book, you need only basic knowledge about the Linux OS and the required Linux environment.

Who this book is for

This book can be used by anyone who would like to install Zimbra, either a simple user in a small business or an IT administrator in a big company.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text, folder names, filenames, file extensions, pathnames, dummy URLs and user input are shown as follows: "The dependencies (`libperl5.14`, `libgmp3c2`, `build-essential`, `sqlite3`, `sysstat`, and `ntp`) should have been installed beforehand."


A block of code is set as follows:


```
blacklist_from sales@abcde.com
whitelist_from bill@xyz.net
blacklist_from *@abc-xyz.net
```

Any command-line input or output is written as follows:

```
sudo apt-get update
sudo apt-get upgrade
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "At the **Software Selection** screen, you must select the **DNS Server** and the **OpenSSH Server** choices for installation, no other options."

 [Warnings or important notes appear in a box like this.]

 [Tips and tricks appear like this.]

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book – what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to feedback@packtpub.com, and mention the book title through the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on www.packtpub.com/authors.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Downloading the example code

You can download the example code files for all Packt books you have purchased from your account at <http://www.packtpub.com>. If you purchased this book elsewhere, you can visit <http://www.packtpub.com/support> and register to have the files e-mailed directly to you.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books – maybe a mistake in the text or the code – we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting <http://www.packtpub.com/support>, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded to our website, or added to any list of existing errata, under the Errata section of that title.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at copyright@packtpub.com with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at questions@packtpub.com if you are having a problem with any aspect of the book, and we will do our best to address it.

1

Single Server Installation

This chapter serves as a quick installation guide for single servers.

The topics covered in this chapter are:

- The prerequisites for Zimbra
- Preparing the environment
- Downloading Zimbra (we will take an Ubuntu version as an example)
- Installing and configuring Zimbra
- Running Zimbra for the first time

By the end of this chapter, the user should have a running Zimbra server on his Linux system.

The prerequisites for Zimbra

Let's dive into the prerequisites for Zimbra:

- Zimbra supports only 64-bit LTS versions of Ubuntu, release 10.04 and above. If you would like to use a 32-bit version, you should use Ubuntu 8.04.x LTS with Zimbra 7.2.3.
- Having a clean and freshly installed system is preferred for Zimbra; it requires a dedicated system and there is no need to install components such as Apache and MySQL, since the Zimbra server contains all the components it needs. Note that installing Zimbra with another service (such as a web server) on the same server can cause operational issues.

- The dependencies (`libperl5.14`, `libgmp3c2`, `build-essential`, `sqlite3`, `sysstat`, and `ntp`) should be installed beforehand.
- Configure a fixed IP address on the server.
- Have a domain name and a well-configured DNS (A and MX entries) that points to the server.

Preparing the environment

Certain things need to be kept in mind while preparing the environment.

Assumptions

This book will need to make use of some specific information as input to the Zimbra installation process, which in most cases will be different for each user. Therefore, we will note some of the most frequently used ones in this section. Remember that you should specify your own values rather than using the arbitrary values that I have provided. The following is the list of assumptions used in this chapter:

- **OS version:** ubuntu-12.04.2-server-amd64
- **Zimbra version:** zcs-8.0.3_GA_5664.UBUNTU12_64.20130305090204
- **OS server name:** mail
- **Internet domain:** zimbra-essentials.com
- **OS server IP address:** 172.16.126.14
- **OS server IP subnet mask:** 255.255.255.0
- **OS server IP gateway:** 172.16.126.1
- **Internal DNS address:** 172.16.126.11
- **External DNS address:** 8.8.8.8
- **Ubuntu admin ID:** abdelmonam
- **Ubuntu admin password:** Z!mbra@dmln
- **Zimbra admin password:** zimbrabook

To be able to understand the following sections – especially when we need to perform a configuration – the reader should know how to harness the *vi* Editor. If you don't, you should develop your skill set or use another editor instead.

You can find good basic training for the *vi* Editor at <http://www.cs.colostate.edu/helpdocs/vi.html>.

System requirements

For the various system requirements, please refer to the following link:

http://www.zimbra.com/docs/os/8.0.2/single_server_install/wwhelp/wwhimpl/common/html/wwhelp.htm#href=SS_Install_8.0.2_OS.ZCS_System_Requirements.html&single=true

If you are using another version of Zimbra, please check the relevant requirements on the Zimbra website.

Installing the Ubuntu server

As declared in the *Assumptions* section, we will use the Ubuntu server release 12.04.2 LTS 64-bit. You can download it from <http://www.ubuntu.com/download/server>.

Newbies in Ubuntu can follow the tutorial given at <http://ubuntuserverguide.com/2012/05/how-to-install-ubuntu-server-12-04-lts-precise-pangolin-included-screenshot.html>.

More advanced users and geeks who like to achieve perfection can follow the guide given at <https://help.ubuntu.com/12.04/serverguide/serverguide.pdf>.

Before starting the installation, keep in mind that for this book we made the following choices:

1. In this book, we will use a split DNS setup, in which the server resides on a **DeMilitarized Zone (DMZ)** and must resolve to its proper internal (DMZ subnet) IP address instead of the public IP address that is issued on the Internet. This is an environment where a firewall/router provides the address translation from the public IP (announced to the world) to the DMZ IP (also called **DNAT**, which stands for **Destination Network Address Translation**) so that translation is not known to the server itself. This configuration is recommended for security, but it makes pieces of the Zimbra setup more difficult than they might otherwise have been.
2. The Ubuntu installation process wants to configure your local network using DHCP. You can accept it and then modify it after installation, but there is no need to do the job twice, so cancel it before it gets that far and then manually configure it with a static IP address (don't forget to replace the one we chose for this book with yours), netmask, and gateway. Don't use a public DNS for your nameserver configuration; rather, use the same IP address that you have assigned to the machine as its proper static IP (which will not allow you to resolve domain names on the Internet until we perform some more configurations later, but it saves unnecessary headaches later).

3. When the installation prompts you for a hostname, configure only a one-word hostname, as we chose in the *Assumptions* section; in our case, it is `mail`; don't give the fully qualified domain name (`mail.zimbra-essentials.com`). On the next screen, where it calls for the domain name, assign `zimbra-essentials.com` (without the hostname).
4. After finishing the base system installation step, the installer process will ask you for credentials (username and password for that user). You can use whatever username you want except `admin` and `zimbra`. Whatever you choose, those credentials will be what you use to log in at the command line after finishing the installation process, and the same password will be the password for `sudo` commands. Make sure you remember what you enter here!
5. At the **Software Selection** screen, you must select **DNS Server** and **OpenSSH Server** for installation, no other options. This will authorize remote administration (SSH) and will mandatorily set up `bind9` for a split DNS.

Let's start the installation. Follow these steps:

1. First of all, choose the appropriate language.
2. Choose **Install Ubuntu Server** and then press *Enter*.
3. When it prompts for the hostname, type in `mail` and then press *Enter*.
4. The hard disk setup is simple if you are using a single drive; however, in the case of a server, it's not the best way to do things. There are a lot of options for partitioning your drives. In our case, we just make a little partition (2x RAM) for swapping, and what remains will be used for the whole system. Others can recommend separate partitions for `mailstore`, `system`, and so on. Feel free to use the recommendation you want depending on your IT architecture; use your own judgment here or ask your IT manager.
5. After finishing the partitioning task, you will be asked to enter the username and password; you can choose what you want except `admin` and `zimbra`.
6. When asked if you want to encrypt the home directory, select **No** and then press *Enter*.
7. Press *Enter* to accept an empty entry for the HTTP proxy.
8. Choose **Install security updates automatically** and then press *Enter*.
9. Highlight **DNS server** and **OpenSSH server** for installation. Press the Space bar to enable each choice, and finally press *Enter* to continue. Note that OpenSSH allows us to connect to the server remotely after installation.
10. Select **Yes** and then press *Enter* to install the GRUB boot loader to the master boot record.

The installation should have completed successfully.

Note that you can get the following frequently encountered error:

```
ERROR: Installation can not proceed. Please fix your /etc/hosts file
to contain:
<ip> <FQHN> <HN>
Where <IP> is the ip address of the host,
<FQHN> is the FULLY QUALIFIED host name, and
<HN> is the (optional) hostname-only portion
```

To resolve this, see the result of the following command:

```
hostname --fqdn
```

The output should match the FQDN in the host's file, or it won't work.



Downloading the example code

You can download the example code files for all Packt books you have purchased from your account at <http://www.packtpub.com>. If you purchased this book elsewhere, you can visit <http://www.packtpub.com/support> and register to have the files e-mailed directly to you.

Preparing the OS (Ubuntu server) for the Zimbra installation

In order to prepare the OS for the Zimbra installation, the following steps need to be performed:

1. Log in to the newly installed system and update and upgrade Ubuntu using the following commands:

```
sudo apt-get update
sudo apt-get upgrade
```

2. Install the dependencies as follows:

```
sudo apt-get install libperl5.14 libgmp3c2 build-essential sqlite3
sysstat ntp
```

3. Zimbra recommends (but there's no obligation) to disable and remove Apparmor:

```
sudo /etc/init.d/apparmor stop
sudo /etc/init.d/apparmor teardown
```

```
sudo update-rc.d -f apparmor remove
sudo aptitude remove apparmor apparmor-utils
```

4. Set the static IP for your server as follows:

Open the network interfaces file using the following command:

```
sudo vi /etc/network/interfaces
```

Then replace the following line:

```
iface eth0 inet dhcp
```

With:

```
iface eth0 inet static
address 172.16.126.14
netmask 255.255.255.0
gateway 172.16.126.1
network 172.16.126.0
broadcast 172.16.126.255
```

Restart the network process by typing in the following:

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



Sanity test!

To verify that your network configuration is configured properly, type in `ifconfig` and ensure that the settings are correct. Then try to ping any working website (such as `google.com`) to see if that works.

DNS configuration

The following steps need to be performed for the DNS configuration:

1. Type in the following command to ensure the BIND server is running:

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

You should get the following:

```
* bind9 is running
```

This is because we installed it within the Ubuntu installation process. If you forgot to install it at that step, you should install it now using the following command:

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

2. Edit your `hosts` file using the following:

```
sudo vi /etc/hosts
```

And change the following:

```
127.0.0.1      localhost
127.0.1.1      mail
```

To:

```
127.0.0.1      localhost.localdomain    localhost
172.16.126.14  mail.zimbra-essentials.com  mail
```

3. Set a hostname for your server. Later, this will become the name of your Zimbra e-mail server.

```
sudo vi /etc/hostname
```

Edit it to the following:

```
mail.zimbra-essentials.com
```

4. In general, we edit DNS servers using the following:

```
sudo vi /etc/resolv.conf
```

But for Ubuntu 12.04, you should use the following:

```
sudo vi /etc/resolvconf/resolv.conf.d/base
```

Set the default settings to the following:

```
nameserver 127.0.0.1
nameserver 172.16.126.11
nameserver 8.8.8.8
domain zimbra-essentials.com
search zimbra-essentials.com
```

5. Type in the following commands:

```
sudo touch /var/cache/bind/db.zimbra-essentials.com
sudo touch /var/cache/bind/db.126.16.172.in-addr.arpa
sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options.backup
sudo cp /etc/bind/named.conf.local /etc/bind/named.conf.local.backup
```

```
sudo cp /etc/bind/named.conf.default-zones /etc/bind/named.conf.default-zones.backup
```

Note here that for the reverse DB, `db.126.16.172.in-addr.arpa`, we put the first three octets of the IP address in the reversed order.

6. Stop the DNS server using the following command:

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

7. Edit your DNS options using the following:

```
sudo vi /etc/bind/named.conf.options
```

And set the following:

```
options {
    directory "/var/cache/bind";
    query-source address * port 53;
    forwarders {
        8.8.8.8; # this is Google DNS
    };
    # we use forwarders to forward DNS queries for external
    # DNS names to DNS servers outside of that network.
    auth-nxdomain no;      # conform to RFC1035
    listen-on-v6 { any; };
};
```



The `query-source address` entry is to allow your server to hit the DNS if the DNS ports for outgoing requests are blocked. If you do not need it, you may leave it commented.

8. Edit your local DNS file using the following:

```
sudo vi /etc/bind/named.conf.local
```

And set the following:

```
acl internals {
    127.0.0.0/8; # for localhost access
    172.16.126.0/24; # for access from my LAN, set yours
    # you can add all internal networks you allow to
    # access your zimbra server in this section
};
```

```

view "internal" {
    match-clients { internals; };
    recursion yes;
    zone "zimbra-essentials.com" {
        type master;
        file "/var/cache/bind/db.zimbra-essentials.com";
    };
    zone "126.16.172.in-addr.arpa" {
        type master;
        file "/var/cache/bind/db.126.16.172.in-addr.arpa";
    };
};

```

9. Edit your reverse zone file using the following:

```
sudo vi /var/cache/bind/db.126.16.172.in-addr.arpa
```

And set the following:

```

$TTL 86400
@      IN      SOA      mail.zimbra-essentials.com.  admin.zimbra-
essentials.com.  (
                201305301916      ; Serial (increment after edit)
                604800             ; Refresh
                86400              ; Retry
                2419200            ; Expire
                86400)             ; Negative Cache TTL
      NS      mail.zimbra-essentials.com.
1      PTR      mail.zimbra-essentials.com.

```

10. Edit your zone file using the following:

```
sudo vi /var/cache/bind/db.zimbra-essentials.com
```

And set the following:

```

; zimbra-essentials.com
$TTL      86400
@      IN      SOA      mail.zimbra-essentials.com.  admin.zimbra-
essentials.com.  (
                201305301921      ; Serial (increment after edit)

```



```
        604800          ; Refresh
        86400          ; Retry
        2419200        ; Expire
        604800)        ; Negative Cache TTL
; Define the nameservers and the mail servers
@      IN      NS          172.16.126.14.
      IN      MX          10    mail.zimbra-essentials.com.
      IN      A           172.16.126.14
mail   IN      A           172.16.126.14
```

11. Since we used views, we should declare them in the default zone.
Run the following command:

```
sudo vi /etc/bind/named.conf.default-zones
```

And set the following:

```
acl internals-default {
    127.0.0.0/8; // for access from localhost
    172.16.126.0/24; // for access from my LAN, set yours
};

view "internal-default" {
    match-clients { internals-default; };
    recursion yes;

    zone "." {
        type hint;
        file "/etc/bind/db.root";
    };

    // be authoritative for the localhost forward and reverse zones,
    // and for broadcast zones as per RFC 1912

    zone "localhost" {
        type master;
        file "/etc/bind/db.local";
    };
};
```

```
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
};
```

12. Ensure all config files have the correct ownership and permissions:

```
sudo chown root:bind /var/cache/bind/db.*
sudo chmod 0644 /var/cache/bind/db.*
```

13. Start your DNS server using the following:

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

14. Our DNS server should be working properly at this point. To verify this, run the following command:

```
nslookup mail.zimbra-essentials.com
```

We should see that our internal DNS server (127.0.0.1) returned the result of our internal IP address (172.16.126.14) for our FQDN of mail.zimbra-essentials.com.

```
abdelmonam@mail:~$ nslookup mail.zimbra-essentials.com
```

```
Server:          127.0.0.1
```

```
Address:         127.0.0.1#53
```

```
Name: mail.zimbra-essentials.com
```

```
Address: 172.16.126.14
```

15. Run the following command:

```
dig zimbra-essentials.com mx
```

Ensure that you get the NOERROR status along the output of this command. Verify that there is an MX record for your FQDN, an NS record for your internal IP, and an A record that links your FQDN to your internal IP.

```
abdelmonam@mail:~$ nslookup mail.zimbra-essentials.com
Server:          127.0.0.1
Address:         127.0.0.1#53
Name:            mail.zimbra-essentials.com
Address: 172.16.126.14
```

```
abdelmonam@mail:~$ dig zimbra-essentials.com mx
```

```
; <<> DiG 9.8.1-P1 <<> zimbra-essentials.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53708
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 1

;; QUESTION SECTION:
zimbra-essentials.com.          IN      MX

;; ANSWER SECTION:
zimbra-essentials.com.      86400 IN      MX      10 mail.zimbra-
essentials.com.

;; AUTHORITY SECTION:
zimbra-essentials.com.      86400 IN      NS      172.16.126.14.

;; ADDITIONAL SECTION:
mail.zimbra-essentials.com. 86400 IN      A      172.16.126.14

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu May 30 20:22:34 2013
;; MSG SIZE rcvd: 103
```



A proper DNS configuration is FUNDAMENTAL! Don't install Zimbra if your DNS is not working properly; installing Zimbra with an improperly working DNS may result in an install that can do everything except send mails, even from a Zimbra user to himself!

If you have some difficulties in configuring DNS, the following are three useful links:

- <http://blog.zimbra.com/blog/archives/2007/06/making-zimbra-bind-work-together.html>
- http://wiki.zimbra.com/wiki/Split_dns
- www.zimbra.com/forums/administrators/585-solved-dns-nutshell.html

Zimbra installation

There are two stages in any Zimbra installation, as we'll now discuss.

Preinstallation

Here we take care of some prerequisites:

1. Let's start by downloading Zimbra Collaboration Suite release 8.0.3 from the Zimbra website:

```
http://www.zimbra.com/downloads/os-downloads.html
```

Or you can get it from the following direct link using the `wget` command:

```
wget http://files2.zimbra.com/downloads/8.0.3_GA/zcs-8.0.3_GA_5664.UBUNTU12_64.20130305090204.tgz
```

2. Unpack the downloaded Zimbra package as follows:

```
tar xzvf zcs-8.0.3_GA_5664.UBUNTU12_64.20130305090204.tgz
```

3. Access the Zimbra package as follows:

```
cd zcs-8.0.3_GA_5664.UBUNTU12_64.20130305090204
```

Installation

In the installation step, first of all (and to make things simple), let's rename the Zimbra package as follows:

```
mv zcs-8.0.3_GA_5664.UBUNTU12_64.20130305090204 zcs
cd zcs/
```

Then we launch the installation process and run the following command:

```
sudo ./install
```

We will get the following output. If we don't make our choices, it means we agree with the default values. Hit the *Enter* key to proceed.

```
abdelmonam@mail:~/zcs$ sudo ./install.sh
```

```
[sudo] password for abdelmonam:
```

```
Operations logged to /tmp/install.log.10489
```

```
Checking for existing installation...
```

For a normal installation, you should have a server that does not have a Zimbra package installed; so you should get output in this format:

```
<PACKAGE_NAME>...NOT FOUND
```

Where <PACKAGE_NAME> can be `zimbra-ldap`, `zimbra-logger`, `zimbra-mta`, `zimbra-snmp`, `zimbra-store`, `zimbra-apache`, `zimbra-spell`, `zimbra-convertd`, `zimbra-memcached`, `zimbra-proxy`, `zimbra-archiving`, `zimbra-cluster`, `zimbra-core`.

The next step is to accept the license. You will be prompted to accept the license agreement; answer with `y`.

```
Do you agree with the terms of the software license agreement? [N] y
```

Then the installation process will check for prerequisites.

```
Checking for prerequisites...
```

```
FOUND: NPTEL
```

```
FOUND: netcat-openbsd-1.89-4ubuntu1
```

```
FOUND: sudo-1.8.3p1-1ubuntu3.4
FOUND: libidn11-1.23-2
FOUND: libpcre3-8.12-4
FOUND: libgmp3c2-2:4.3.2+dfsg-2ubuntu1
FOUND: libexpat1-2.0.1-7.2ubuntu1.1
FOUND: libstdc++6-4.6.3-1ubuntu5
FOUND: libperl5.14-5.14.2-6ubuntu2.3
```

Checking for suggested prerequisites...

```
FOUND: perl-5.14.2
FOUND: sysstat
FOUND: sqlite3
```

Prerequisite check complete.

If your system lacks some dependencies, the installation process will be aborted. You should install the required dependencies before resuming the installation.

If you pass this step successfully, the next one will be the selection of packages to install. In this chapter we are looking at single installations, so we will install all the required packages on the same server. The following are the choices we have made:

Select the packages to install

```
Install zimbra-ldap [Y]
Install zimbra-logger [Y]
Install zimbra-mta [Y]
Install zimbra-snmp [Y]
Install zimbra-store [Y]
Install zimbra-apache [Y]
Install zimbra-spell [Y]
Install zimbra-memcached [N]
Install zimbra-proxy [N]
```

As you can see, we don't make any choice—we only press *Enter* on each line to accept the default choice.

After that, the installer checks the necessary space for installation as follows:

```
Checking required space for zimbra-core
```

```
Checking space for zimbra-store
```

If there is insufficient space on your hard disk, the installation process will be aborted. You should free the needed space before resuming installation.

The installer will ask you if you accept that the system will be modified. Accept by entering `y`.

```
The system will be modified. Continue? [N] y
```

Then a classic operation to guarantee the work of the new installation takes place; the installer does a cleanup operation to remove any old installation of Zimbra.

```
Removing /opt/zimbra
```

```
Removing zimbra crontab entry...done.
```

```
Cleaning up zimbra init scripts...done.
```

```
Cleaning up /etc/ld.so.conf...done.
```

```
Cleaning up /etc/security/limits.conf...done.
```

```
Finished removing Zimbra Collaboration Server.
```

Once the cleanup operation has finished, the installation of the chosen packages starts:

```
Installing packages
```

```
zimbra-core.....zimbra-core_8.0.3.GA.5664.UBUNTU12.64_amd64.deb...  
done
```

```
zimbra-ldap.....zimbra-ldap_8.0.3.GA.5664.UBUNTU12.64_amd64.deb...  
done
```

```
zimbra-logger.....zimbra-logger_8.0.3.GA.5664.UBUNTU12.64_amd64.  
deb...done
```

```
zimbra-mta.....zimbra-mta_8.0.3.GA.5664.UBUNTU12.64_amd64.deb...done
```

```
zimbra-snmp.....zimbra-snmp_8.0.3.GA.5664.UBUNTU12.64_amd64.deb...  
done
```

```
zimbra-store.....zimbra-store_8.0.3.GA.5664.UBUNTU12.64_amd64.deb...  
done
```

```
zimbra-apache.....zimbra-apache_8.0.3.GA.5664.UBUNTU12.64_amd64.  
deb...done
```

```
zimbra-spell.....zimbra-spell_8.0.3.GA.5664.UBUNTU12.64_amd64.deb...
done
```

```
Operations logged to /tmp/zmsetup.05302013-235652.log
```

```
Installing LDAP configuration database...done.
```

```
Setting defaults...
```

After installing the packages, the configuration steps start. The first step is to align the Zimbra configuration with the DNS one. Accept to change the domain name and then enter yours; here is what we do:

```
DNS ERROR resolving MX for mail.zimbra-essentials.com
```

```
It is suggested that the domain name have an MX record configured in DNS
```

```
Change domain name? [Yes]
```

```
Create domain: [mail.zimbra-essentials.com] zimbra-essentials.com
```

```
MX: mail.zimbra-essentials.com (172.16.126.14)
```

```
Interface: 127.0.0.1
```

```
Interface: ::1
```

```
Interface: 172.16.126.14
```

```
done.
```

```
Checking for port conflicts
```

Finally, you will get the final configuration menu. Values that need to be set are indicated using stars (*), but of course you can modify any value you want.

```
Main menu
```

```

1) Common Configuration:
2) zimbra-ldap:           Enabled
3) zimbra-store:         Enabled
   +Create Admin User:    yes
   +Admin user to create: admin@zimbra-essentials.
com
***** +Admin Password   UNSET
   +Anti-virus quarantine user: virus-quarantine.iy3kye8t@
zimbra-essentials.com
```


Single Server Installation

```
+Enable automated spam training:      yes
+Spam training user:                  spam.hns2daxszi@zimbra-
essentials.com
+Non-spam(Ham) training user:        ham.huyi_gqfpe@zimbra-
essentials.com
+SMTP host:                          mail.zimbra-essentials.com
+Web server HTTP port:               80
+Web server HTTPS port:             443
+Web server mode:                   https
+IMAP server port:                  143
+IMAP server SSL port:              993
+POP server port:                   110
+POP server SSL port:              995
+Use spell check server:            yes
+Spell server URL:                  http://mail.zimbra-
essentials.com:7780/aspell.php
+Configure for use with mail proxy:  FALSE
+Configure for use with web proxy:   FALSE
+Enable version update checks:      TRUE
+Enable version update notifications: TRUE
+Version update notification email:  admin@zimbra-essentials.
com
+Version update source email:       admin@zimbra-essentials.
com

4) zimbra-mta:                      Enabled
5) zimbra-snmpp:                    Enabled
6) zimbra-logger:                   Enabled
7) zimbra-spell:                    Enabled
8) Default Class of Service Configuration:
r) Start servers after configuration  yes
s) Save config to file
x) Expand menu
q) Quit
```

Address unconfigured (**) items (? - help) 3

As you can see, we chose to start by configuring `zimbra-store` (menu number 3). We get the following submenu:

Store configuration

```
1) Status: Enabled
2) Create Admin User: yes
3) Admin user to create: admin@zimbra-essentials.
com
** 4) Admin Password UNSET
5) Anti-virus quarantine user: virus-quarantine.iy3kye8t@
zimbra-essentials.com
6) Enable automated spam training: yes
7) Spam training user: spam.hns2daxszi@zimbra-
essentials.com
8) Non-spam(Ham) training user: ham.huyi_gqfpe@zimbra-
essentials.com
9) SMTP host: mail.zimbra-essentials.com
10) Web server HTTP port: 80
11) Web server HTTPS port: 443
12) Web server mode: https
13) IMAP server port: 143
14) IMAP server SSL port: 993
15) POP server port: 110
16) POP server SSL port: 995
17) Use spell check server: yes
18) Spell server URL: http://mail.zimbra-
essentials.com:7780/aspell.php
19) Configure for use with mail proxy: FALSE
20) Configure for use with web proxy: FALSE
21) Enable version update checks: TRUE
22) Enable version update notifications: TRUE
23) Version update notification email: admin@zimbra-essentials.
com
24) Version update source email: admin@zimbra-essentials.
com
```

Select, or 'r' for previous menu [r] 4

By choosing submenu number 4, we can set the admin password. We use the following to do so:

```
Password for admin@zimbra-essentials.com (min 6 characters): [CiMVj7HPE]
zimbrabook
```

Store configuration

```
1) Status: Enabled
2) Create Admin User: yes
3) Admin user to create: admin@zimbra-essentials.com
4) Admin Password set
5) Anti-virus quarantine user: virus-quarantine.iy3kye8t@
zimbra-essentials.com
6) Enable automated spam training: yes
7) Spam training user: spam.hns2daxszi@zimbra-
essentials.com
8) Non-spam(Ham) training user: ham.huyi_gqfpe@zimbra-
essentials.com
9) SMTP host: mail.zimbra-essentials.com
10) Web server HTTP port: 80
11) Web server HTTPS port: 443
12) Web server mode: https
13) IMAP server port: 143
14) IMAP server SSL port: 993
15) POP server port: 110
16) POP server SSL port: 995
17) Use spell check server: yes
18) Spell server URL: http://mail.zimbra-
essentials.com:7780/aspell.php
19) Configure for use with mail proxy: FALSE
20) Configure for use with web proxy: FALSE
21) Enable version update checks: TRUE
22) Enable version update notifications: TRUE
23) Version update notification email: admin@zimbra-essentials.
com
24) Version update source email: admin@zimbra-essentials.
com
```

Select, or 'r' for previous menu [r] r

By entering the letter r, we will go to the previous menu, which is as follows:

Main menu

- 1) Common Configuration:
- 2) zimbra-ldap: Enabled
- 3) zimbra-store: Enabled
- 4) zimbra-mta: Enabled
- 5) zimbra-snmp: Enabled
- 6) zimbra-logger: Enabled
- 7) zimbra-spell: Enabled
- 8) Default Class of Service Configuration:
- r) Start servers after configuration yes
- s) Save config to file
- x) Expand menu
- q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply

Select from menu, or press 'a' to apply config (? - help) a

And then, by choosing the letter a on the principal menu, we apply the changes we performed.

The installer will ask you to save a configuration to a file; accept it by pressing *Enter*. You will get the `config` file path. It then informs you that the system will be modified; agree with *y*. The installation process will finish the remaining steps automatically:

```
Save configuration data to a file? [Yes]
Save config in file: [/opt/zimbra/config.17192]
Saving config in /opt/zimbra/config.17192...done.
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.05302013-235652.log
Setting local config values...done.
Initializing core config...Setting up CA...done.
Deploying CA to /opt/zimbra/conf/ca ...done.
```

Creating SSL zimbra-store certificate...done.
Creating new zimbra-ldap SSL certificate...done.
Creating new zimbra-mta SSL certificate...done.
Installing mailboxd SSL certificates...done.
Installing MTA SSL certificates...done.
Installing LDAP SSL certificate...done.
Initializing ldap...done.
Setting replication password...done.
Setting Postfix password...done.
Setting amavis password...done.
Setting nginx password...done.
Creating server entry for mail.zimbra-essentials.com...done.
Setting Zimbra IP Mode...done.
Saving CA in ldap ...done.
Saving SSL Certificate in ldap ...done.
Setting spell check URL...done.
Setting service ports on mail.zimbra-essentials.com...done.
Adding mail.zimbra-essentials.com to zimbraMailHostPool in default COS...done.
Setting zimbraFeatureTasksEnabled=TRUE...done.
Setting zimbraFeatureBriefcasesEnabled=FALSE...done.
Setting MTA auth host...done.
Setting TimeZone Preference...done.
Initializing mta config...done.
Setting services on mail.zimbra-essentials.com...done.
Creating domain zimbra-essentials.com...done.
Setting default domain name...done.
Creating domain zimbra-essentials.com...already exists.
Creating admin account admin@zimbra-essentials.com...done.
Creating root alias...done.
Creating postmaster alias...done.
Creating user spam.hns2daxszi@zimbra-essentials.com...done.
Creating user ham.huyi_gqfpe@zimbra-essentials.com...done.
Creating user virus-quarantine.iy3kye8t@zimbra-essentials.com...done.
Setting spam training and Anti-virus quarantine accounts...done.

```
Initializing store sql database...done.
Setting zimbraSmtphostname for mail.zimbra-essentials.com...done.
Configuring SNMP...done.
Setting up syslog.conf...done.
Starting servers...done.
Installing common zimlets...
com_zimbra_srchhighlighter...done.
com_zimbra_phone...done.
com_zimbra_ymemoticons...done.
com_zimbra_tooltip...done.
com_zimbra_attachcontacts...done.
com_zimbra_adminversioncheck...done.
com_zimbra_email...done.
com_zimbra_attachmail...done.
com_zimbra_date...done.
com_zimbra_clientuploader...done.
com_zimbra_url...done.
com_zimbra_proxy_config...done.
com_zimbra_cert_manager...done.
com_zimbra_viewmail...done.
com_zimbra_bulkprovision...done.
com_zimbra_webex...done.
Finished installing common zimlets.
Restarting mailboxd...done.
Creating galsync account for default domain...done.
```

You have the option of notifying Zimbra of your installation.
This helps us to track the uptake of the Zimbra Collaboration Server.

```
The only information that will be transmitted is:
The VERSION of zcs installed (8.0.3_GA_5664_UBUNTU12_64)
The ADMIN EMAIL ADDRESS created (admin@zimbra-essentials.com)
Notify Zimbra of your installation? [Yes] no
Notification skipped
Setting up zimbra crontab...done.
Moving /tmp/zmsetup.05302013-235652.log to /opt/zimbra/log
Configuration complete - press return to exit
```

Running Zimbra for the first time

After finishing the installation successfully, Zimbra should be running. To check if all Zimbra components are running, all you need to do is run the following commands:

```
abdelmonam@mail:~$ sudo -i
[sudo] password for abdelmonam:
root@mail:~# su - zimbra
zimbra@mail:~$ zmcontrol status
Host mail.zimbra-essentials.com
antisppam                Running
antivirus                Running
ldap                    Running
logger                  Running
mailbox                 Running
mta                     Running
snmp                   Running
spell                   Running
stats                   Running
zmconfigd               Running
```

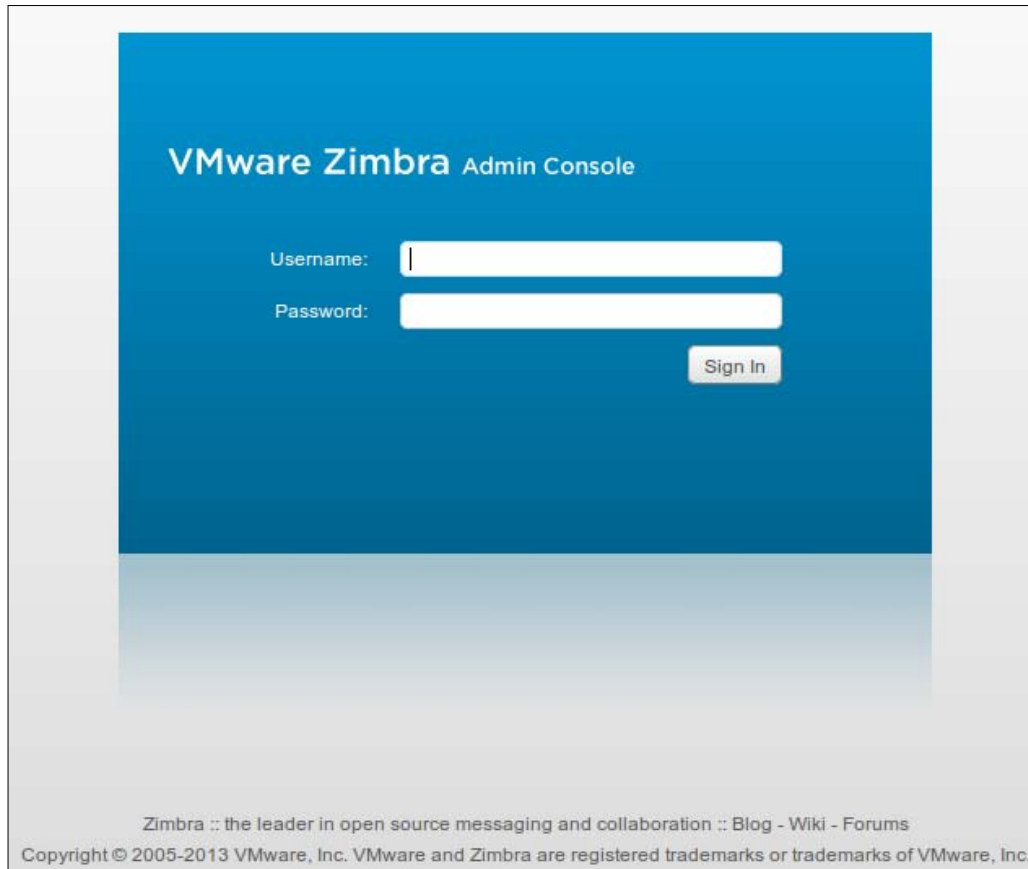
Running all services can take some time, so please wait for a few minutes and check again. If one service (or more) is not running, you should stop and start Zimbra again via the following commands:

```
Zmcontrol stop
Zmcontrol start
```

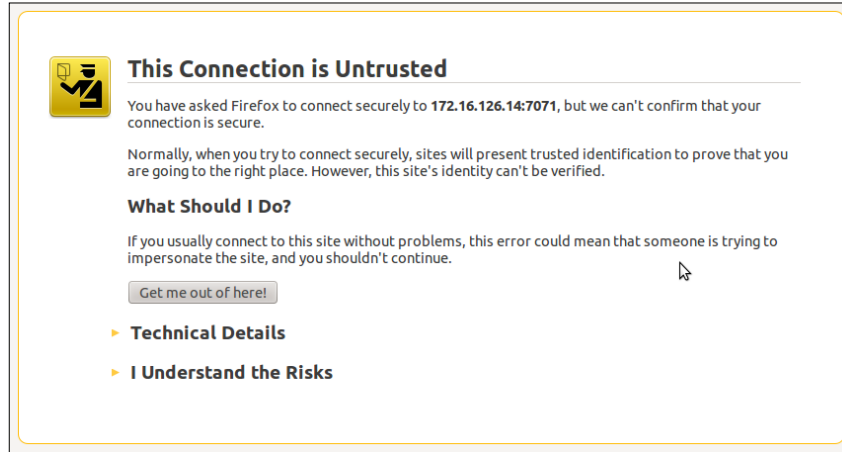
When running Zimbra for the first time, you need to go to the admin console to configure it. To do that, all you need to do is go to the following address:

<https://172.16.126.14:7071/zimbraAdmin>

You will get the following interface:



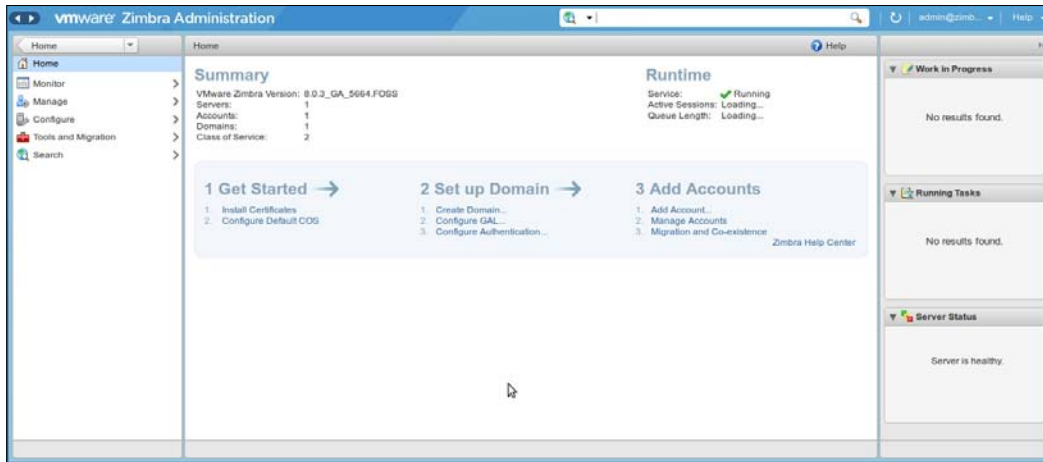
Note that, depending on your browser, you may receive an SSL certification exception the first time. For me, with Firefox, I got the following:



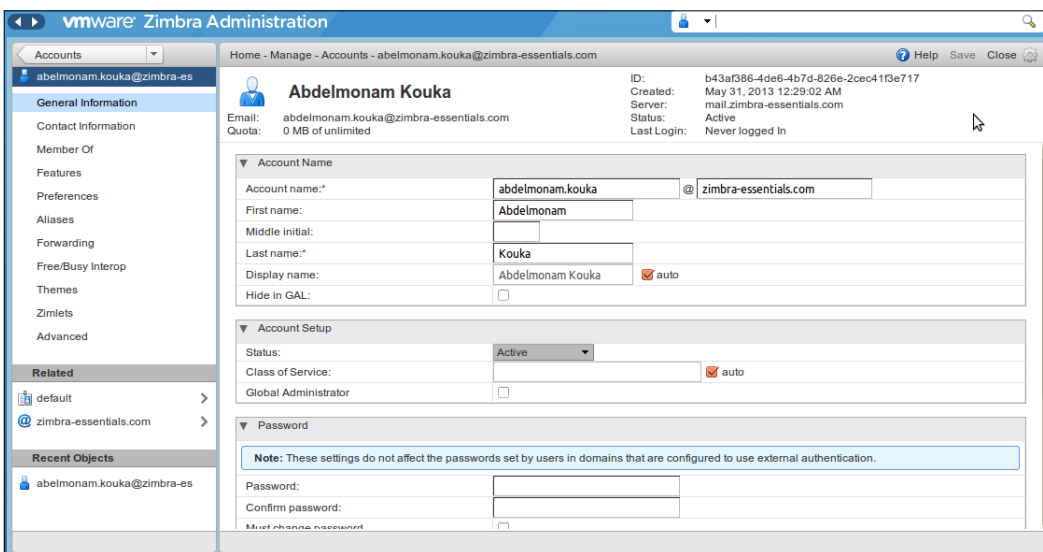
Don't worry; accept it. As we explained before, the Zimbra installation process generates a local certificate, which is not signed by any certification authority; that's why some browsers show this warning. In the professional context, you should get a certificate signed by a trusted certification authority. In this manner, you will avoid that warning. We will see this point demonstrated in a later chapter of this book.




After logging in, you can start managing your Zimbra server. The following is the screen you will get immediately after logging in, and it shows an overview of the Zimbra server:



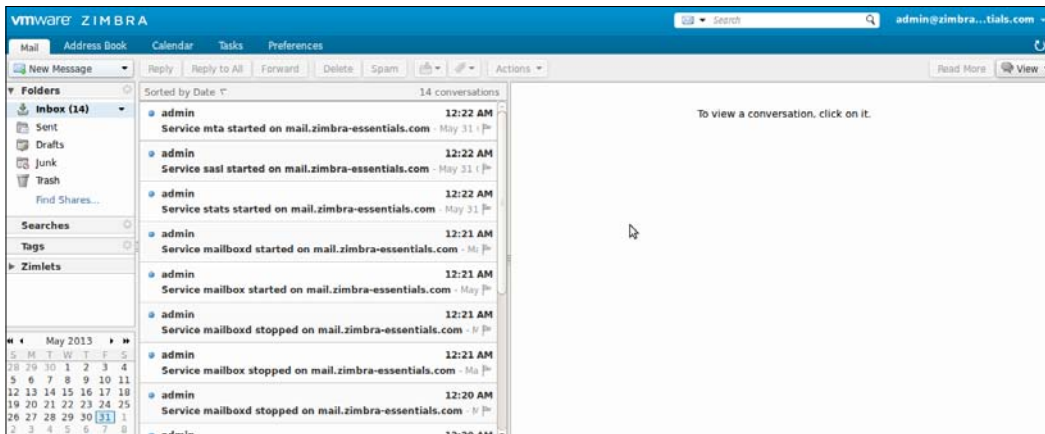
You can create other mail accounts and manage them. We will explain this process in a later chapter. The following screenshot is an example of this:



To access the mail account for the administrator (or any other created user), you should go to <https://172.16.126.14/>.

 Depending on your browser, you will get an SSL exception the first time. Accept it.

The following screenshot shows the mailbox of the admin:



Summary

In this chapter we saw a step-by-step explanation of how to install Zimbra in a single server environment. We started by describing the prerequisites and moved on to preparing the environment. Next, we ran through all the installation steps, until finally running Zimbra and testing it.

This chapter is enough for those who would like to install Zimbra for testing or for small businesses. But for bigger businesses, Zimbra should be installed in distributed environments, which is the subject of the next chapter.

2

Multiserver Installation

This chapter serves as an installation guide for Zimbra in a multiserver environment.

The topics covered in this chapter are as follows:

- Knowing the prerequisites for Zimbra multiserver installation
- Preparing the environment
- Downloading Zimbra (we will take a version of Ubuntu as an example)
- Installing and configuring different Zimbra servers
- Post-install configuration
- Running Zimbra for the first time

By the end of this chapter, the user should have a running Zimbra server in a multiserver environment.

The prerequisites for Zimbra

For Zimbra multiserver installation, we need the same prerequisites as those in *Chapter 1, Single Server Installation*.

In addition, in the specific context of multiserver setup, we need to perform the following actions:

- The system clocks should be synced on all servers. We will explain how to do that later in this chapter.
- Configure the file `/etc/resolv.conf` on all servers to point at the server on which we installed the bind (it can be installed on any Zimbra server or on a separate server). We will explain this point in detail later.

Preparing the environment

Before starting the Zimbra installation process, we should prepare the environment. In the first part of this section, we will see the different possible configurations and then, in the second part, we will present the needed assumptions to apply the chosen configuration.

Multiserver configuration examples

One of the greatest advantages of Zimbra is its scalability: we can deploy it for a small business with few mail accounts as well as for a huge organization with thousands of mail accounts.

There are many possible configuration options; the following are the most used out of those:

- **Small configuration:** All Zimbra components are installed on only one server; this is the case in the first chapter in this book.
- **Medium configuration:** Here, LDAP and message store are installed on one server and Zimbra MTA on a separate server. Note here that we can use more Zimbra MTA servers, so we can scale more easily for large incoming or outgoing e-mail volume.
- **Large configuration:** In this case, LDAP will be installed on a dedicated server and we will have multiple mailbox and MTA servers, so we can scale more easily for a large number of users.
- **Very large configuration:** The difference between this configuration and a large one is the existence of an additional LDAP server, so we will have a Master LDAP and its replica.

For this chapter, we choose the medium configuration; so, we will install LDAP and mailbox in one server and MTA on the other server.

Install different servers in the following order (for medium configuration, 1 and 2 are combined in only one step):



1. First of all, install and configure the LDAP server.
2. Then, install and configure Zimbra mailbox servers.
3. Finally, install Zimbra MTA servers and finish the whole installation configuration.

New installations of Zimbra limit spam/ham training to the first installed MTA. If you uninstall or move this MTA, you should enable spam/ham training on another MTA as one host should have this enabled to run `zmtrainsa --cleanup`. To do this, execute the following command:

```
zmlocalconfig -e zmtrainsa_cleanup_host=TRUE
```

Assumptions

In this book, we will use some specific information as input in the Zimbra installation process, which, in most cases, will be different for each user. Therefore, we will note some of the most redundant ones in this section. Remember that you should specify your own values rather than using the arbitrary values that I have provided. The following is the list of assumptions used in this chapter:

- **OS version:** ubuntu-12.04.2-server-amd64
- **Zimbra version:** zcs-8.0.3_GA_5664.UBUNTU12_64.20130305090204
- **MTA server name:** mta
- **MTA hostname:** mta.zimbra-essentials.com
- **Internet domain:** zimbra-essentials.com
- **MTA server IP address:** 172.16.126.141
- **MTA server IP subnet mask:** 255.255.255.0
- **MTA server IP gateway:** 172.16.126.1
- **Internal DNS server:** 172.16.126.11
- **External DNS server:** 8.8.8.8
- **MTA admin ID:** abdelmonam
- **MTA admin Password:** Z!mbra@dmln
- **Zimbra admin Password:** zimbrabook
- **MTA server name:** ldap

- **MTA hostname:** ldap.zimbra-essentials.com
- **LDAP server IP address:** 172.16.126.140
- **LDAP server IP subnet mask:** 255.255.255.0
- **LDAP server IP gateway:** 172.16.126.1
- **Internal DNS server:** 172.16.126.11
- **External DNS server:** 8.8.8.8
- **LDAP admin ID:** abdelmonam
- **LDAP admin password:** Z!mbra@dmln

To be able to follow the steps described in the next sections, especially each time we need to perform a configuration, the reader should know how to harness the *vi* editor. If not, you should develop your skill set for using the *vi* editor or use another editor instead.

You can find good basic training for the *vi* editor at <http://www.cs.colostate.edu/helpdocs/vi.html>

System requirements

For the various system requirements, please refer to the following link:

http://www.zimbra.com/docs/os/8.0.0/multi_server_install/wwhelp/wwhimpl/common/html/wwhelp.htm#href=ZCS_Multiserver_Open_8.0.System_Requirements_for_VMware_Zimbra_Collaboration_Server_8.0.html&single=true

If you are using another version of Zimbra, please check the correct requirements on the Zimbra website.

Installing the Ubuntu server

This section is the same as in the first chapter except for a few differences regarding the following points:

- Step 3: When the installation prompts you to provide a hostname, configure only a one-word hostname; in the *Assumptions* section, we've chosen ldap for the LDAP and mailstore server and mta for the MTA server – don't give the fully qualified domain name (for example, mta.zimbra-essentials.com). On the next screen that calls for the domain name, assign it zimbra-essentials.com (without the hostname).

- Step 5: On the **Software Selection** screen, you must select the **DNS Server** and the **OpenSSH Server** choices for installation; no other options. This will authorize remote administration (SSH) and mandatorily set up `bind9` for a split DNS. For `bind9`, you can install it on only one server, which is what we've done in this book.

Let's start installation; to do so, repeat the process explained in the first chapter for each server and make sure to mention specific values.

Preparing Ubuntu for Zimbra installation

On each server, follow the same instructions given in the *Preparing Ubuntu for Zimbra installation* section of the first chapter and pay attention when you set the static IP address (172.16.126.140 for the LDAP server and 172.16.126.141 for the MTA server).

DNS configuration

We make the choice to install `bind` on the same server with LDAP and mailbox; you can install it on another server if you like, but the most important thing is just that, in all servers, you should configure your `/etc/resolv.conf` file to point at it.

The following steps will be done only on the LDAP server until otherwise notified:

1. **Sanity check:** It allows you to be sure that the BIND server is running. Type the following command:

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

You should get:

```
* bind9 is running
```

This is because we installed it within the Ubuntu installation process; else, if you forgot to install it at this step, you should install it now via the following command:

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

2. Edit your `hosts` file using the following command:

```
sudo vi /etc/hosts
```

Then change the following settings:

```
127.0.0.1      localhost
127.0.1.1      ldap
```


To:

```
127.0.0.1      localhost.localdomain      localhost
172.16.126.140 ldap.zimbra-essentials.com  ldap
```

3. Set a hostname for the server. Later, this will become the name of your Zimbra e-mail server. Run the following command:

```
sudo vi /etc/hostname
```

And edit the default settings to:

```
ldap.zimbra-essentials.com
```

4. In general, we edit DNS servers using the following command:

```
sudo vi /etc/resolv.conf
```

But for Ubuntu 12.04, you should instead edit the following command:

```
sudo vi /etc/resolvconf/resolv.conf.d/base
```

And set it to the following:

```
nameserver 127.0.0.1
nameserver 172.16.126.11
nameserver 8.8.8.8
domain zimbra-essentials.com
search zimbra-essentials.com
```

5. Type the following commands:

```
sudo touch /var/cache/bind/db.zimbra-essentials.com
sudo touch /var/cache/bind/db.126.16.172.in-addr.arpa
sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options.backup
sudo cp /etc/bind/named.conf.local /etc/bind/named.conf.local.backup
sudo cp /etc/bind/named.conf.default-zones /etc/bind/named.conf.default-zones.backup
```

Note here that for the reverse DB, `db.126.16.172.in-addr.arpa`, we put only the first three octets of the IP address in reverse order.

6. Stop the DNS server using the following command:


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

7. Edit your DNS options using the following command:

```
sudo vi /etc/bind/named.conf.options
```

And set the following options:

```
options {
    directory "/var/cache/bind";
    query-source address * port 53;
    forwarders {
        8.8.8.8; # this is Google DNS
    };
    # we use forwarders to forward DNS queries for external
    # DNS names to DNS servers outside of that network.
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
```

 The query-source address entry is to allow your server to hit the DNS if the DNS ports for outgoing requests are blocked. If you do not need it, you may leave it commented.

8. Edit your local DNS file by typing the following command:

```
sudo vi /etc/bind/named.conf.local
```

And set the following:

```
acl internals {
    127.0.0.0/8; # for localhost access
    172.16.126.0/24; # for access from my LAN, set yours
    # you can add all internal networks you allow to
    # access your zimbra server in this section
};

view "internal" {
    match-clients { internals; };
    recursion yes;
    zone "zimbra-essentials.com" {
        type master;
    };
};
```

```
        file "/var/cache/bind/db.zimbra-essentials.com";
    };
    zone "126.16.172.in-addr.arpa" {
        type master;
        file "/var/cache/bind/db.126.16.172.in-addr.arpa";
    };
};
```

9. Edit your reverse zone file using the following command:

```
sudo vi /var/cache/bind/db.126.16.172.in-addr.arpa
```

And set the following:

```
$TTL 86400
@      IN      SOA      ldap.zimbra-essentials.com.  admin.zimbra-
essentials.com.  (
                201306181855    ; Serial (increment after edit)
                604800         ; Refresh
                86400          ; Retry
                2419200        ; Expire
                86400)         ; Negative Cache TTL
      NS      ldap.zimbra-essentials.com.
1     PTR     ldap.zimbra-essentials.com.
2     PTR     mta.zimbra-essentials.com.
```

10. Edit your zone file using the following command:

```
sudo vi /var/cache/bind/db.zimbra-essentials.com
```

And set the following:

```
; zimbra-essentials.com
$TTL      86400
@      IN      SOA      ldap.zimbra-essentials.com.  admin.zimbra-
essentials.com.  (
                201306181901    ; Serial (increment after edit)
                604800         ; Refresh
                86400          ; Retry
                2419200        ; Expire
```

```

        604800)          ; Negative Cache TTL
; Define the nameservers and the mail servers
@      IN      NS      172.16.126.140.
      IN      MX      10   mta.zimbra-essentials.com.
      IN      A       172.16.126.140
ldap   IN      A       172.16.126.140
mta    IN      A       172.16.126.141

```

11. Since views were used, they also need to be used in the default zone. Type the following command:

```
sudo vi /etc/bind/named.conf.default-zones
```

And set the following:

```

// prime the server with knowledge of the root servers

acl internals-default {
    127.0.0.0/8; // for access from localhost
    172.16.126.0/24; // for access from my LAN, set yours
};

view "internal-default" {
    match-clients { internals-default; };
    recursion yes;

    zone "." {
        type hint;
        file "/etc/bind/db.root";
    };

    // be authoritative for the localhost forward and reverse zones,
    and for
    // broadcast zones as per RFC 1912

    zone "localhost" {
        type master;

```

```
        file "/etc/bind/db.local";
    };

    zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
    };

    zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
    };

    zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
    };
};
```

12. Ensure that all config files have the correct ownership and permissions:

```
sudo chown root:bind /var/cache/bind/db.*
sudo chmod 0644 /var/cache/bind/db.*
```

13. Start your DNS server using the following commands:

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

14. Sanity check! Here, our DNS should be working well; to verify that, try to run:

```
nslookup ldap.zimbra-essentials.com
```

We should see that our internal DNS server (127.0.0.1) has returned the result of our internal IP address (172.16.126.140) for your FQDN `ldap.zimbra-essentials.com`; the same should occur for MTA.

```
abdelmonam@ldap:~$ nslookup ldap.zimbra-essentials.com
Server:          127.0.0.1
Address:         127.0.0.1#53
```

```
Name: ldap.zimbra-essentials.com
Address: 172.16.126.140
```

```
abdelmonam@ldap:~$ nslookup mta.zimbra-essentials.com
Server:          127.0.0.1
Address:         127.0.0.1#53
```

```
Name: mta.zimbra-essentials.com
Address: 172.16.126.141
```

15. Sanity check! Run the following command:

```
dig zimbra-essentials.com mx
```

Ensure that you get a NOERROR status along with the output of this command; verify that there is an MX record for your FQDN, an NS record for your internal IP, and an A record that links your FQDN to your internal IP.

```
abdelmonam@ldap:~$ dig zimbra-essentials.com mx
```

```
; <<>> DiG 9.8.1-P1 <<>> zimbra-essentials.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17702
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 1

;; QUESTION SECTION:
zimbra-essentials.com.      IN      MX

;; ANSWER SECTION:
zimbra-essentials.com. 86400  IN      MX      10 mta.zimbra-
essentials.com.

;; AUTHORITY SECTION:
zimbra-essentials.com. 86400  IN      NS      172.16.126.140.
```

```
;; ADDITIONAL SECTION:
mta.zimbra-essentials.com. 86400 IN   A    172.16.126.141

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53 (127.0.0.1)
;; WHEN: Sat Jun 15 02:12:44 2013
;; MSG SIZE rcvd: 103
```



Proper DNS configuration is FUNDAMENTAL! If your DNS is not working well, don't try to install Zimbra at this point; installing Zimbra with a DNS that isn't working properly may result in an install that can do everything except send mails, even from a Zimbra user to himself.

If you have some difficulties with configuring DNS, refer to the following three useful links:

1. <http://blog.zimbra.com/blog/archives/2007/06/making-zimbra-bind-work-together.html>
2. http://wiki.zimbra.com/wiki/Split_dns
3. www.zimbra.com/forums/administrators/585-solved-dns-nutshell.html

Additional network configuration on the MTA server

To run Zimbra correctly, we should configure the network on the MTA server; to do so, complete the following few steps on the MTA server:

1. Edit your hosts using the following command:

```
sudo vi /etc/hosts
```

Then change the following default settings:

```
127.0.0.1      localhost
127.0.1.1      mta
```

To:

```
127.0.0.1      localhost.localdomain  localhost
172.16.126.141 mta.zimbra-essentials.com mta
```

2. Set a hostname for the server; later, this will become the name of your Zimbra MTA server:

```
sudo vi /etc/hostname
```

Edit the hostname to:

```
mta.zimbra-essentials.com
```

3. In general, we edit DNS servers using the following command:

```
sudo vi /etc/resolv.conf
```

But with Ubuntu 12.04, we should instead edit the following command:

```
sudo vi /etc/resolvconf/resolv.conf.d/base
```

And set it to the following:

```
nameserver 172.16.126.140
nameserver 127.0.0.1
nameserver 172.16.126.11
nameserver 8.8.8.8
domain zimbra-essentials.com
search zimbra-essentials.com
```

We can verify that our configuration is working well via the following commands:

```
abdelmonam@mta:~$ nslookup mta.zimbra-essentials.com
```

```
Server:          172.16.126.140
```

```
Address:         172.16.126.140#53
```

```
Name: mta.zimbra-essentials.com
```

```
Address: 172.16.126.141
```

```
abdelmonam@mta:~$ nslookup ldap.zimbra-essentials.com
```

```
Server:          172.16.126.140
```

```
Address:         172.16.126.140#53
```

```
Name: ldap.zimbra-essentials.com
```

```
Address: 172.16.126.140
```



```
abdelmonam@mta:~$ dig zimbra-essentials.com mx

; <<>> DiG 9.8.1-P1 <<>> zimbra-essentials.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16347
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 1

;; QUESTION SECTION:
zimbra-essentials.com.      IN      MX

;; ANSWER SECTION:
zimbra-essentials.com. 86400  IN      MX      10 mta.zimbra-
essentials.com.

;; AUTHORITY SECTION:
zimbra-essentials.com. 86400  IN      NS      172.16.126.140.

;; ADDITIONAL SECTION:
mta.zimbra-essentials.com. 86400 IN      A      172.16.126.141

;; Query time: 2 msec
;; SERVER: 172.16.126.140#53(172.16.126.140)
;; WHEN: Sat Jun 15 02:33:11 2013
;; MSG SIZE rcvd: 103
```

Syncing servers

As we've said earlier, system clocks should be synced on all servers. We will explain how to do that here. The following actions should be carried out in every server:

1. Install the NTP server (if it is not installed yet) and run the following command:
`sudo apt-get install ntp`

- Configure it; to do that, you should edit this config file by using the following command:

```
sudo vi /etc/ntp.conf
```

This file will probably have the default Ubuntu server activated. Just comment all of the servers by adding a # symbol in front of it and add in the one you want to use.

- Activate the new changes using the following command:

```
abdelmonam@mta:~$ sudo service ntp restart
* Stopping NTP server ntpd          [ OK ]
* Starting NTP server ntpd         [ OK ]
```

- Check if it syncs the servers by using the following command:

```
sudo ntpq -c lpeer
```

The following command will show a list of all the servers and when they were last checked. A random example from the Web is as follows:

```
abdelmonam@mta:~$ sudo ntpq -c lpeer
      remote           refid      st t when poll reach  delay
offset jitter
=====
=====
  maisha-02.aptus .INIT.          16 u   - 64   0  0.000
0.000  0.000
  igubu.saix.net .INIT.          16 u   - 64   0  0.000
0.000  0.000
  stratum1.neolog .INIT.          16 u   - 64   0  0.000
0.000  0.000
  sabela.saix.net .INIT.          16 u   - 64   0  0.000
0.000  0.000
  europium.canoni .INIT.          16 u   - 64   0  0.000
0.000  0.000
```

Installing Zimbra

There are two stages for installing Zimbra:

Understanding the prerequisites

In this section of the chapter, we take care of some prerequisites for installing Zimbra.

For each server, download and unpack the Zimbra package as described in the first chapter.

Package installation

First of all, and to do things simply, let's rename the Zimbra package by using the following command:

```
mv zcs-8.0.3_GA_5664.UBUNTU12_64.20130305090204 zcs
cd zcs/
```

Then we launch the installation process as follows:

```
sudo ./install.sh
```

```
[sudo] password for abdelmonam:
```

```
Operations logged to /tmp/install.log.10489
```

```
Checking for existing installation...
```

For normal installation, you should have a new server with no Zimbra package installed yet, so you should get an output in this format: <PACKAGE_NAME>...NOT FOUND

Where <PACKAGE_NAME> can be: zimbra-ldap, zimbra-logger, zimbra-mta, zimbra-snmp, zimbra-store, zimbra-apache, zimbra-spell, zimbra-convertd, zimbra-memcached, zimbra-proxy, zimbra-archiving, zimbra-cluster, zimbra-core.

The next step is the acceptance of the license: you will be asked to accept the license agreement – answer with *y*:

```
Do you agree with the terms of the software license agreement? [N] y
```

Then, the process will check for prerequisites.

If there are dependencies lacking in your system, the installation process will abort. You should install the required dependencies before resuming installation.

If you pass this step successfully, the next one will be the selection of packages to install.

Installing the first Zimbra server – LDAP master server

You must configure the Zimbra Master LDAP server before you can install other Zimbra servers. You can set up LDAP replication, configuration of a master LDAP server, and replica LDAP servers, configuring all LDAP servers either now or after you set up the initial ZCS servers.

The `zimbra-store` package can be installed with the LDAP server, the MTA server, or as a separate mailbox server. You can have more than one mailbox server and new mailbox servers can be added at any time.

As we've said before, we made the choice of installing two servers – one for LDAP and mailbox and the other for MTA. Here, we will see how to install the first one.

After launching the installation process and accepting the license, type `Y` and press *Enter* to install the `zimbra-ldap`, `zimbra-logger` (optional and only on one mailbox server), `zimbra-store`, and `zimbra-spell` (optional) packages. When the `zimbra-spell` package is installed, the `zimbra-apache` package also gets installed. In the following output example, the packages to be installed are emphasized.

Note that if SNMP is being used, the SNMP package is installed on every Zimbra server. Mark `Y` as shown in the output given below:

You will get the following output; normally, if we don't make a choice, it means that we agree with the default value by hitting the *Enter* key:

```
Select the packages to install
Install zimbra-ldap [Y]
Install zimbra-logger [Y]
Install zimbra-mta [Y] N
Install zimbra-snmp [Y]
Install zimbra-store [Y]
Install zimbra-apache [Y]
Install zimbra-spell [Y]
Install zimbra-memcached [N]
Install zimbra-proxy [N]
```

To summarize, The following's what we will do:

1. Choose the packages to be installed.
2. Set the LDAP admin password (you need to write it down; it will be used in MTA installation).

3. Set the password for the administrator account.
4. Set the SMTP host. This is the mta-server hostname.
5. We should also set passwords for postfix and amavis, since we will need them for MTA installation, but we will not do that in this step; we will show you how to set these passwords after finishing the installation process.

After that, the installer checks the necessary space for installation:

```
Checking required space for zimbra-core
```

```
Checking space for zimbra-store
```

If there is insufficient space on your hard disk, the installation process will abort. You should free up the needed space before resuming installation.

The installer will ask you if you accept that the system will be modified – accept this by entering `y` as follows:

```
The system will be modified. Continue? [N] y
```

Then, a classic operation takes place to guarantee that the installation is completed: the installer does a cleanup operation to remove any old installation of Zimbra.

Once the cleanup operation is finished, the installation of the chosen packages starts.

After installing packages, the configuration steps start. The first step is to align the Zimbra configuration with the DNS one. Accept to change the domain name and then enter the one you want for yourself. The following is what we do:

```
DNS ERROR resolving MX for ldap.zimbra-essentials.com
```

```
It is suggested that the domain name have an MX record configured in DNS
```

```
Change domain name? [Yes]
```

```
Create domain: [ldap.zimbra-essentials.com] zimbra-essentials.com
```

```
done.
```

```
Checking for port conflicts
```

Finally, you will get the final configuration menu. Values that need to be set are indicated by stars *, but, of course, you can modify any value you want.

```
Main menu
```

- 1) Common Configuration:
- 2) zimbra-ldap: **Enabled**
- 3) zimbra-store: **Enabled**

```

+Create Admin User:                yes
+Admin user to create:             admin@zimbra-essentials.
com
***** +Admin Password              UNSET
+Anti-virus quarantine user:       virus-quarantine.
thmglky8p@zimbra-essentials.com
+Enable automated spam training:   yes
+Spam training user:              spam.brgef_4xa@zimbra-
essentials.com
+Non-spam(Ham) training user:     ham.cclnkdtng@zimbra-
essentials.com
***** +SMTP host:                  UNSET
+Web server HTTP port:            80
+Web server HTTPS port:           443
+Web server mode:                 https
+IMAP server port:                143
+IMAP server SSL port:            993
+POP server port:                 110
+POP server SSL port:             995
+Use spell check server:          yes
+Spell server URL:                http://ldap.zimbra-
essentials.com:7780/aspell.php
+Configure for use with mail proxy: FALSE
+Configure for use with web proxy: FALSE
+Enable version update checks:    TRUE
+Enable version update notifications: TRUE
+Version update notification email: admin@zimbra-essentials.
com
+Version update source email:     admin@zimbra-essentials.
com
4) zimbra-snmpp:                  Enabled
5) zimbra-logger:                 Enabled
6) zimbra-spell:                  Enabled
7) Default Class of Service Configuration:
r) Start servers after configuration  yes
s) Save config to file
x) Expand menu
q) Quit

```

Address unconfigured (**) items (? - help) 1

As you can see, we choose to start the server configuration by modifying Common configuration (menu number 1). We get the following submenu:

Common configuration

- 1) Hostname: ldap.zimbra-essentials.com
- 2) Ldap master host: ldap.zimbra-essentials.com
- 3) Ldap port: 389
- 4) Ldap Admin password: set
- 5) Secure interprocess communications: yes
- 6) TimeZone: Africa/Algiers
- 7) IP Mode: ipv4

Select, or 'r' for previous menu [r] 4

By choosing number 1 in the submenu, we set the LDAP admin password as follows:

Password for ldap admin user (min 6 characters): [Y3uOf0Ry] ldapadmin

Common configuration

- 1) Hostname: ldap.zimbra-essentials.com
- 2) Ldap master host: ldap.zimbra-essentials.com
- 3) Ldap port: 389
- 4) Ldap Admin password: set
- 5) Secure interprocess communications: yes
- 6) TimeZone: Africa/Algiers
- 7) IP Mode: ipv4

Select, or 'r' for previous menu [r] r

By entering the letter *r*, we will go to the previous menu (the Main menu).

Then, we choose to configure zimbra-store (menu number 3). We get the following submenu:

Store configuration

- 1) Status: Enabled
- 2) Create Admin User: yes
- 3) Admin user to create: admin@zimbra-essentials.com
- ** 4) Admin Password UNSET
- 5) Anti-virus quarantine user: virus-quarantine.
thmg1ky8p@zimbra-essentials.com

```

6) Enable automated spam training:      yes
7) Spam training user:                  spam.brgef_4xa@zimbra-
essentials.com
8) Non-spam(Ham) training user:        ham.cclnkdtng@zimbra-
essentials.com
** 9) SMTP host:                        UNSET
10) Web server HTTP port:               80
11) Web server HTTPS port:             443
12) Web server mode:                   https
13) IMAP server port:                  143
14) IMAP server SSL port:              993
15) POP server port:                   110
16) POP server SSL port:               995
17) Use spell check server:            yes
18) Spell server URL:                  http://ldap.zimbra-
essentials.com:7780/aspell.php
19) Configure for use with mail proxy:  FALSE
20) Configure for use with web proxy:  FALSE
21) Enable version update checks:      TRUE
22) Enable version update notifications: TRUE
23) Version update notification email:  admin@zimbra-essentials.
com
24) Version update source email:       admin@zimbra-essentials.
com

```

Select, or 'r' for previous menu [r] 4

By choosing the submenu number 4, we set the Zimbra admin password as follows:

```

Password for admin@zimbra-essentials.com (min 6 characters): [wIthDGK9TT]
zimbrabook

```

Store configuration

```

1) Status:                             Enabled
2) Create Admin User:                   yes
3) Admin user to create:                admin@zimbra-essentials.com
4) Admin Password                       set

```



```
5) Anti-virus quarantine user:          virus-quarantine.
thmglky8p@zimbra-essentials.com

6) Enable automated spam training:      yes

7) Spam training user:                  spam.brgef_4xa@zimbra-
essentials.com

8) Non-spam(Ham) training user:         ham.cclnkdtng@zimbra-
essentials.com

** 9) SMTP host:                        UNSET

10) Web server HTTP port:               80

11) Web server HTTPS port:             443

12) Web server mode:                    https

13) IMAP server port:                   143

14) IMAP server SSL port:               993

15) POP server port:                    110

16) POP server SSL port:                995

17) Use spell check server:             yes

18) Spell server URL:                   http://ldap.zimbra-
essentials.com:7780/aspell.php

19) Configure for use with mail proxy:   FALSE

20) Configure for use with web proxy:    FALSE

21) Enable version update checks:       TRUE

22) Enable version update notifications: TRUE

23) Version update notification email:   admin@zimbra-essentials.
com

24) Version update source email:         admin@zimbra-essentials.
com
```

Select, or 'r' for previous menu [r] 9

Finally, we set the MTA host by selecting the submenu number 9 shown as follows:

Please enter the SMTP server hostname: mta.zimbra-essentials.com

Store configuration

```
1) Status:                               Enabled
2) Create Admin User:                     yes
3) Admin user to create:                  admin@zimbra-essentials.com
4) Admin Password                          set
```

```

5) Anti-virus quarantine user:          virus-quarantine.
thmglky8p@zimbra-essentials.com

6) Enable automated spam training:      yes

7) Spam training user:                  spam.brgef_4xa@zimbra-
essentials.com

8) Non-spam(Ham) training user:         ham.cclnkdtng@zimbra-
essentials.com

9) SMTP host:                           mta.zimbra-essentials.com

10) Web server HTTP port:                80

11) Web server HTTPS port:              443

12) Web server mode:                     https

13) IMAP server port:                    143

14) IMAP server SSL port:                993

15) POP server port:                     110

16) POP server SSL port:                 995

17) Use spell check server:              yes

18) Spell server URL:                    http://ldap.zimbra-
essentials.com:7780/aspell.php

19) Configure for use with mail proxy:    FALSE

20) Configure for use with web proxy:     FALSE

21) Enable version update checks:        TRUE

22) Enable version update notifications:  TRUE

23) Version update notification email:    admin@zimbra-essentials.
com

24) Version update source email:          admin@zimbra-essentials.
com

```

Select, or 'r' for previous menu [r] r

By entering the letter *r*, we will go to the previous menu shown as follows:

Main menu

```

1) Common Configuration:
2) zimbra-ldap:           Enabled
3) zimbra-store:         Enabled
4) zimbra-snmp:           Enabled
5) zimbra-logger:        Enabled
6) zimbra-spell:         Enabled
7) Default Class of Service Configuration:

```

- r) Start servers after configuration yes
- s) Save config to file
- x) Expand menu
- q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply

Select from menu, or press 'a' to apply config (? - help) a

Then, on the principal menu, by choosing the letter a, we apply the changes that we performed.

The installer will ask you to save the configuration to a file – accept it by pressing *Enter*; you will get the config file path, which then informs you that the system will be modified – agree with *y* and then the installation process will finish the remaining steps automatically.

As we've mentioned before, we should set passwords for postfix and amavis because we need them for MTA installation. If we forget this step or we do it, but forget the passwords that we set, it is not the end of the world; we can fix that as follows:

```
abdelmonam@ldap:~/zcs$ sudo -s
[sudo] password for abdelmonam:
root@ldap:~/zcs# su - zimbra
zimbra@ldap:~$ zmldappasswd -h
Usage: /opt/zimbra/bin/zmldappasswd [-h] [-r] [-p] [[-c]-l] newpassword
-h: display this help message
-a: change ldap_amavis_password
-b: change ldap_bes_searcher_password
-l: change ldap_replication_password
-c: Update ldap_replication_password on replica. Requires -l
-n: change ldap_nginx_password
-p: change ldap_postfix_password
-r: change ldap_root_passwd
Only one of a, l, n, p, or r may be specified
Without options zimbra_ldap_password is changed
```

Option -c requires -l and must be run on a replica after changing the password on the master (using -l by itself).

```
zimbra@ldap:~$ zmldappasswd -p postfixadmin
Updating local config and LDAP
zimbra@ldap:~$ zmldappasswd -a amavisadmin
Updating local config and LDAP
```

Now you can check if services are running; you should do that as a Zimbra user:

```
zimbra@ldap:~$ zmcontrol status
Host ldap.zimbra-essentials.com
ldap                Running
logger              Running
mailbox              Running
snmp                 Running
spell                Running
stats                Running
zmconfigd           Running
```

Installing Zimbra MTA on a server

When the `zimbra-mta` package is installed, the LDAP hostname and the Zimbra LDAP password must be known to the MTA server. If not, the MTA cannot contact the LDAP server and is not able to complete the installation.

After launching the installation process and accepting the license, type `Y` and press *Enter* to install the `zimbra-mta` package. The other packages should be marked `N`. In the output example mentioned in this section, the package to be installed is emphasized.

Note that if SNMP is used, it is installed on every server.

To summarize, the following's what we will do:

1. Choose the packages to be installed.
2. Configure the LDAP master host and the LDAP admin password with values set in the LDAP installation process.
3. Set the MTA auth host – this is the MTA authentication server hostname – to one of the Zimbra mailbox servers' hostnames. In our case, it is the LDAP server that we previously installed.
4. Configure postfix and amavis admin passwords with the values set in the LDAP installation step.

You will get the following output; normally, if we don't make a choice, it means that we agree with the default value by hitting the *Enter* key.

Select the packages to install

```
Install zimbra-ldap [Y] n
Install zimbra-logger [Y] n
Install zimbra-mta [Y]
Install zimbra-snmp [Y]
Install zimbra-store [Y] n
Install zimbra-apache [Y] n
Install zimbra-spell [Y] n
Install zimbra-memcached [N]
Install zimbra-proxy [N]
Checking required space for zimbra-core
```

Installing:

```
zimbra-core
zimbra-mta
zimbra-snmp
```

The system will be modified. Continue? [N] y

Removing /opt/zimbra

```
Removing zimbra crontab entry...done.
Cleaning up zimbra init scripts...done.
Cleaning up /etc/ld.so.conf...done.
Cleaning up /etc/security/limits.conf...done.
Finished removing Zimbra Collaboration Server.
Installing packages
```

```
zimbra-core.....zimbra-core_8.0.3.GA.5664.UBUNTU12.64_amd64.deb...
done
zimbra-mta.....zimbra-mta_8.0.3.GA.5664.UBUNTU12.64_amd64.deb...done
zimbra-snmp.....zimbra-snmp_8.0.3.GA.5664.UBUNTU12.64_amd64.deb...
done
```

```
Operations logged to /tmp/zmsetup.06152013-055329.log
Setting defaults...done.
```

```
Checking for port conflicts
```

Finally, you will get the final configuration menu. Values that need to be set are indicated by stars *, but, of course, you can modify any value you want as follows:

```
Main menu
```

```
  1) Common Configuration:
      +Hostname:                               mta.zimbra-essentials.com
***** +Ldap master host:                     UNSET
      +Ldap port:                             389
***** +Ldap Admin password:                 UNSET
      +LDAP Base DN:                          cn=zimbra
      +Secure interprocess communications:     yes
      +TimeZone:                              Africa/Algiers
      +IP Mode:                               ipv4
  2) zimbra-mta:                               Enabled
***** +MTA Auth host:                       UNSET
      +Enable Spamassassin:                   yes
      +Enable Clam AV:                        yes
      +Notification address for AV alerts:    admin@mta.zimbra-
essentials.com
***** +Bind password for postfix ldap user: UNSET
***** +Bind password for amavis ldap user:  UNSET
  3) zimbra-snmp:                             Enabled
  r) Start servers after configuration        yes
  s) Save config to file
  x) Expand menu
  q) Quit
```

```
Address unconfigured (**) items (? - help) 1
```

As you can see, we choose to start the configuration of the server by modifying Common configuration (menu number 1). We get the following submenu:

Common configuration

```
1) Hostname: mta.zimbra-essentials.com
** 2) Ldap master host: UNSET
3) Ldap port: 389
** 4) Ldap Admin password: UNSET
5) LDAP Base DN: cn=zimbra
6) Secure interprocess communications: yes
7) TimeZone: Africa/Algiers
8) IP Mode: ipv4
```

Select, or 'r' for previous menu [r] 2

First of all, we should set our ldap server hostname previously installed; to do that, choose submenu number 2:

Please enter the ldap server hostname: ldap.zimbra-essentials.com

Common configuration

```
1) Hostname: mta.zimbra-essentials.com
2) Ldap master host: ldap.zimbra-essentials.com
3) Ldap port: 389
** 4) Ldap Admin password: UNSET
5) LDAP Base DN: cn=zimbra
6) Secure interprocess communications: yes
7) TimeZone: Africa/Algiers
8) IP Mode: ipv4
```

Select, or 'r' for previous menu [r] 4

Then, we should set the ldap password that we've chosen while configuring our LDAP server; to do that, we need to choose submenu number 4, shown as follows:

Password for ldap admin user (min 6 characters): ldapadmin

Setting defaults from ldap...done.

Common configuration

```
1) Hostname: mta.zimbra-essentials.com
2) Ldap master host: ldap.zimbra-essentials.com
```

```
3) Ldap port:                389
4) Ldap Admin password:     set
5) LDAP Base DN:           cn=zimbra
6) Secure interprocess communications:  yes
7) TimeZone:                Africa/Algiers
8) IP Mode:                  ipv4
```

Select, or 'r' for previous menu [r] r

By entering the letter *r*, we will go to the previous menu (the Main menu).

Now we move on to MTA configuration by choosing menu number 2 as follows:

Mta configuration

```
1) Status:                    Enabled
** 2) MTA Auth host:          UNSET
3) Enable Spamassassin:      yes
4) Enable Clam AV:           yes
5) Notification address for AV alerts:  admin@mta.zimbra-
essentials.com
** 6) Bind password for postfix ldap user:  UNSET
** 7) Bind password for amavis ldap user:  UNSET
```

Select, or 'r' for previous menu [r] 2

For MTA configuration, we start by selecting submenu number 2, where we configure the MTA authentication server hostname (which is, by the way, our LDAP server):

Please enter the mta authentication server hostname: ldap.zimbra-essentials.com

Mta configuration

```
1) Status:                    Enabled
2) MTA Auth host:              ldap.zimbra-essentials.com
3) Enable Spamassassin:      yes
4) Enable Clam AV:           yes
```



```
5) Notification address for AV alerts:      admin@mta.zimbra-essentials.com
** 6) Bind password for postfix ldap user:  UNSET
** 7) Bind password for amavis ldap user:   UNSET
```

Select, or 'r' for previous menu [r] 5

Then, we move on to submenu number 5, where we correct the AV mail notification address as follows:

```
Notification address for AV alerts: [admin@mta.zimbra-essentials.com]
admin@zimbra-essentials.com
```

Mta configuration

```
1) Status:                                Enabled
2) MTA Auth host:                          ldap.zimbra-essentials.com
3) Enable Spamassassin:                    yes
4) Enable Clam AV:                          yes
5) Notification address for AV alerts:      admin@zimbra-essentials.com
** 6) Bind password for postfix ldap user:  UNSET
** 7) Bind password for amavis ldap user:   UNSET
```

Select, or 'r' for previous menu [r] 6

Before finishing this step, we should set the postfix admin password via submenu number 6; if you forget this password, come back to the *Installing first Zimbra server – LDAP master server* section to find out how to set it:

```
Password for ldap Postfix user (min 6 characters): postfixadmin
```

Mta configuration

```
1) Status:                                Enabled
2) MTA Auth host:                          ldap.zimbra-essentials.com
3) Enable Spamassassin:                    yes
4) Enable Clam AV:                          yes
5) Notification address for AV alerts:      admin@zimbra-essentials.com
6) Bind password for postfix ldap user:    set
** 7) Bind password for amavis ldap user:   UNSET
```

Select, or 'r' for previous menu [r] 7

Finally, we must set the amavis admin password via submenu number 7; if you forget this password, come back to the *Installing first Zimbra server – LDAP master server* section to find out how to set it:

```
Password for ldap Amavis user (min 6 characters): amavisadmin
```

Mta configuration

```
1) Status: Enabled
2) MTA Auth host: ldap.zimbra-essentials.com
3) Enable Spamassassin: yes
4) Enable Clam AV: yes
5) Notification address for AV alerts: admin@zimbra-essentials.
com
6) Bind password for postfix ldap user: set
7) Bind password for amavis ldap user: set
```

Select, or 'r' for previous menu [r] r

By entering the letter r, we will go to the previous menu:

Main menu

```
1) Common Configuration:
2) zimbra-mta: Enabled
3) zimbra-snmp: Enabled
r) Start servers after configuration yes
s) Save config to file
x) Expand menu
q) Quit
```

*** CONFIGURATION COMPLETE - press 'a' to apply

Select from menu, or press 'a' to apply config (? - help) a

Then, in the principal menu, by choosing the letter a, we apply the changes we performed.

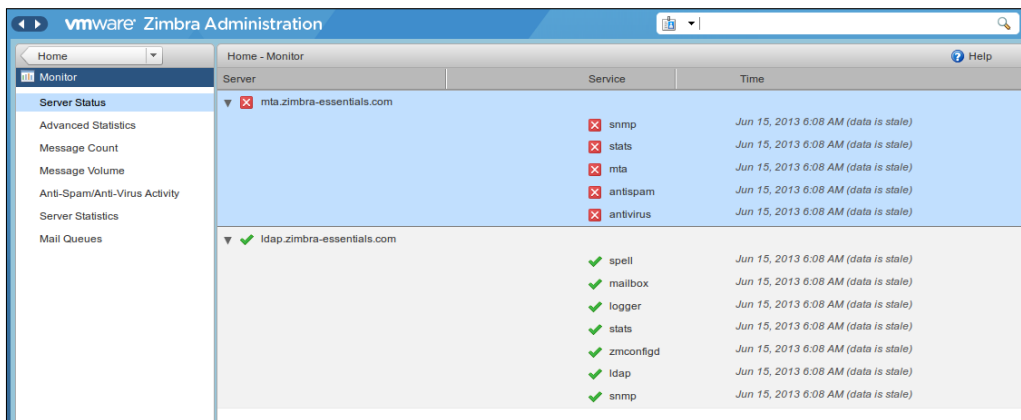
The installer will ask you to save the configuration to a file – accept it by pressing *Enter*; you will get the config file path which then informs you that the system will be modified – agree with *y*, and then the installation process will finish the remaining steps automatically.

Here you can also check if services are up via the following command:

```
zimbra@mta:~$ zmcontrol status
Host mta.zimbra-essentials.com
antispam           Running
antivirus          Running
mta                Running
snmp               Running
stats              Running
zmconfigd         Running
```

Post installation

Is that all? Can we start using Zimbra now? Well not yet; if we try to connect to the admin console now, we will get the following:



To solve this problem, we should perform the following actions:

- **Set up the ssh keys:** For remote management and postfix queue management, the ssh keys must be manually populated on each server. To populate the ssh keys on each server as the Zimbra user, type `zmupdateauthkeys` and press *Enter*. The key is updated on `/opt/zimbra/.ssh/authorized_keys`.

For example:

```
zimbra@ldap:~$ zmupdateauthkeys
Updating keys for ldap.zimbra-essentials.com
Fetching key for ldap.zimbra-essentials.com
Updating keys for ldap.zimbra-essentials.com
Updating keys for mta.zimbra-essentials.com
Fetching key for mta.zimbra-essentials.com
Updating keys for mta.zimbra-essentials.com
Updating /opt/zimbra/.ssh/authorized_keys
```

- **Enabling server statistics display:** In order for the server statistics to display on the administration console, the syslog configuration files must be modified. On each server, as the root user, type `/opt/zimbra/libexec/zmsyslogsetup`. This enables the server to display statistics.

For example:

```
root@mta:~/zcs# /opt/zimbra/libexec/zmsyslogsetup
updateRsyslogd: Updating /etc/rsyslog.d/50-default.conf...done.
```

Then, on the LDAP server, you have to edit `/etc/rsyslog.conf` and uncomment the following:

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

- Finally, restart syslog:

```
service rsyslog restart
```

Now you can start using your Zimbra server.

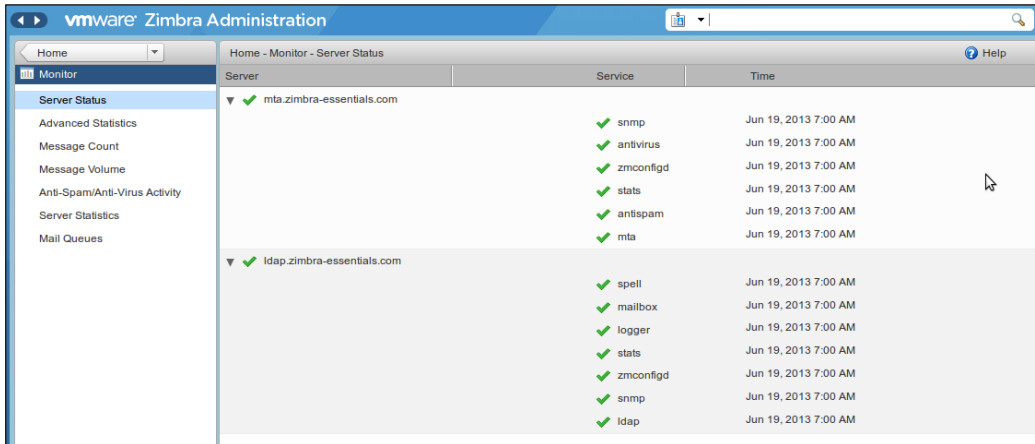
Running Zimbra for the first time

When running Zimbra for the first time, you need to go to the admin console to configure it. To do that, all you need is to go to the following address:

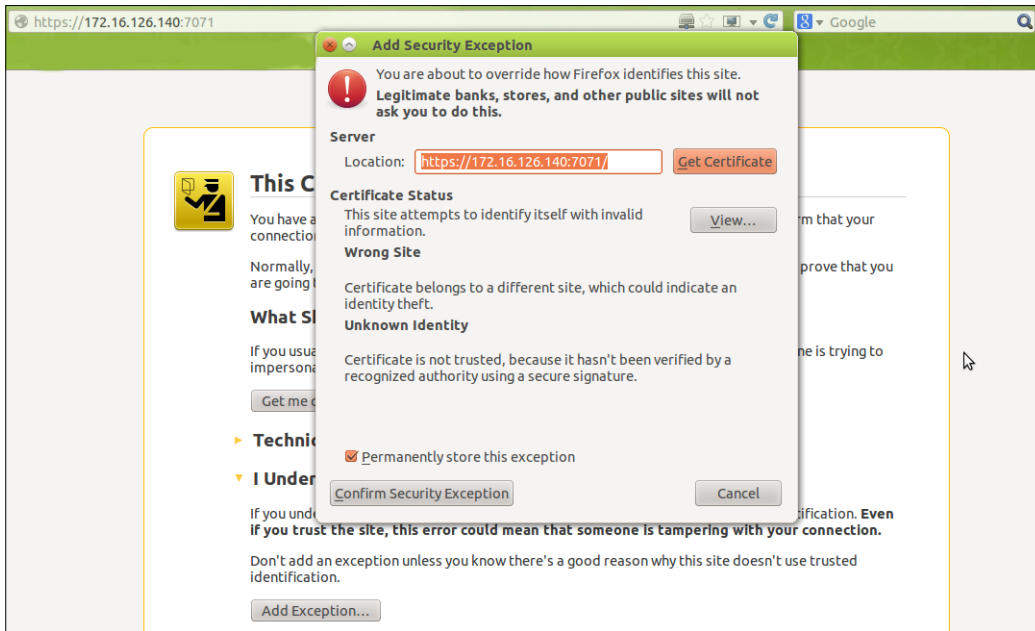
<https://172.16.126.140:7071/zimbraAdmin>

Multiserver Installation

You can now check that all services are running well (this may take some minutes after restarting the servers), as shown in the following screenshot:



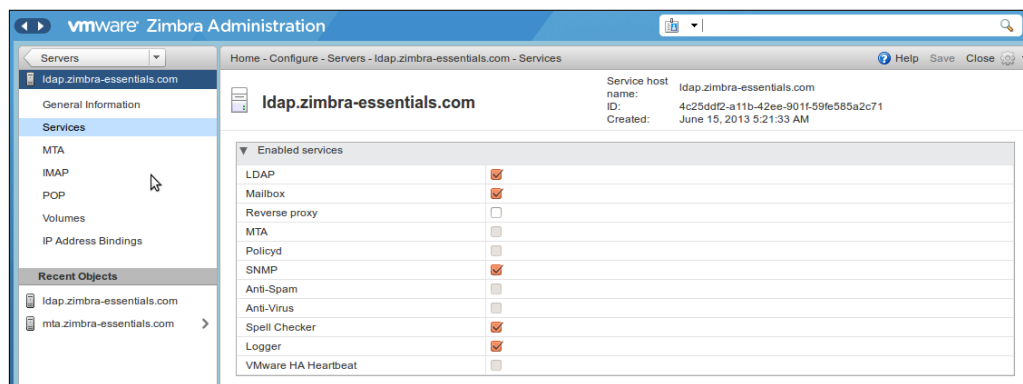
Note that, when you do this for the first time you will receive an SSL certification exception:



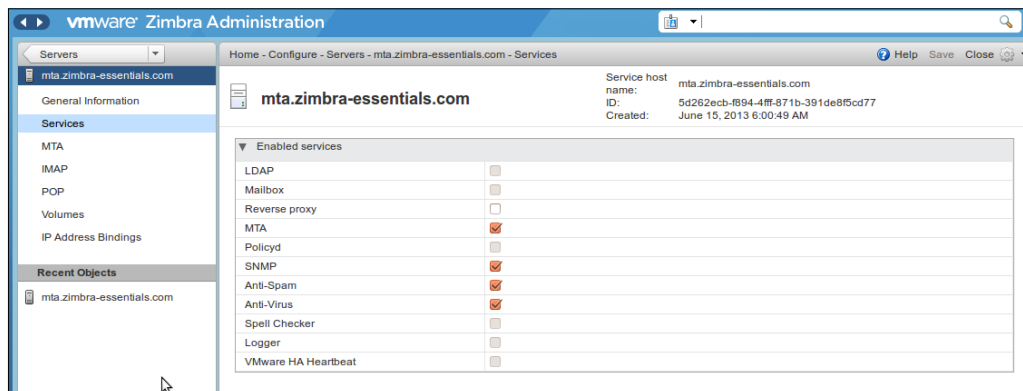
Don't worry; accept it. As we explained before, the Zimbra installation process generates a local certificate, which is not signed by any certification authority; that's why some browsers show this warning. In a professional context, you should get a professional certification signed by a trusted certificate authority; in this manner, you will avoid that warning. We will see this point in a later chapter of this book.

After login, you can start managing your Zimbra servers via the admin console by going to **Configure | Servers**; then double-click on the server you want to manage and you will get the following screenshot for each server, in our case:

The LDAP server:



The MTA server:



To access the mail account for the administrator (or any other created user), you should go to the address: `https://172.16.126.140/`

(The same as for the admin console, you will get an SSL exception the first time – accept it.)

Summary

In this chapter, we saw, step-by-step, how to install Zimbra in a multiserver environment. We started by describing the prerequisites, then preparing the environment for multiserver installation; next, we ran through all the installation steps for each server until we finally ran Zimbra and tested it.

Now, after seeing how to install Zimbra in both single and multiserver environments, it is time to start looking for something to protect our installation, which is how we can improve security inside Zimbra, especially antivirus/antispam tools. That is the subject of the next chapter.

3

Securing Zimbra

This chapter serves as an administration guide to secure Zimbra.

The topics covered in this chapter are:

- Internal solutions (updating the ClamAV antivirus, using DSPAM and ASSP as other antispam solutions, improving the main SpamAssassin antispam, and so on)
- External solutions (Barracuda, MailCleaner, and so on)

By the end of this chapter, the user should be able to increase the security inside Zimbra.

Problems and issues

Zimbra has a high-level security system, but it has some problems, especially in antivirus/antispam integrated solutions, which are:

- Zimbra integrates only one antivirus solution by default, which is a weakness.
- Zimbra updates the ClamAV package to the latest version with every Zimbra release. This means that the user must wait for the next release of Zimbra to have the latest version of ClamAV, even if the actual version contains a bug! (here there is always a solution to upgrade ClamAV without waiting for the new release of Zimbra, but it contains a lot of problems; I will explain that later).
- The second antispam solution integrated with Zimbra (DSPAM) is not activated by default.

- The user cannot modify the postfix configuration files directly. Some of the postfix files are rewritten when changes are made in the administration console. Any changes the user makes will be overwritten.
- The same problem exists for upgrading SpamAssassin/DSPAM: the user can only upgrade them with the new release of Zimbra.
- **Sender Policy Framework (SPF)** is not enabled in the Zimbra SpamAssassin package; neither are Razor nor Pyzor.
- The **Distributed Checksum Clearinghouses (DCC)** plugin is not installed.

To solve most of these problems and to improve Zimbra security, after a deep search we find that we may use the following two types of solutions:

- Internal solutions (we will cover these in detail just after this paragraph)
- External solution: Having a frontal antispam/antivirus gateway e-mail server; the choice of the best external solution will be the subject of a major part of this chapter in detail later.

Internal solutions

In this chapter, we will present the best solutions that we can implement inside the Zimbra environment; that's why we call them internal solutions.

Enabling DSPAM

The way Zimbra handles spam is not very effective and it doesn't resolve most users' needs. In fact, it relies on SpamAssassin to filter spam/ham mails, and this heuristics-based method, in my opinion, is very old and inadequate, though it does catch a lot of spam. Besides, rules should be added/updated on a regular basis in order to face a spammer's new methods.

On the other hand, DSPAM has another approach to filter spam: a statistical method that "learns" better how to detect spam. This learning is simply done when you repeatedly show DSPAM examples of spam by marking them as junk. With time, DSPAM learns patterns (words and combinations of words) that exist mostly in your spam and ham mails. In terms of that knowledge, it can define what you should regard as spam and what you shouldn't. This is what keeps DSPAM up to date with the latest trends in spam. Besides, the language in which DSPAM is written is C, and compared to Perl (the language in which SpamAssassin is written), C is much faster.

Zimbra disabled DSPAM quite some time ago because of stability issues, and in our case the mileage varies; therefore, we have to enable DSPAM.

To enable DSPAM inside Zimbra, we need to act as the Zimbra user by running the following command:

```
abdelmonam@mail:~$ sudo -i
[sudo] password for abdelmonam:
root@mail:~# su - zimbra
zimbra@mail:~$
```

Now we need to go to the `amavisd.conf.in` directory first:

```
zimbra@mail:~$ cd /opt/zimbra/conf/
```

You will see the `dspam` config by doing this:

```
zimbra@mail:~$ more amavisd.conf.in | grep dspam
%%uncomment LOCAL:amavis_dspam_enabled%%$dspam = '/opt/zimbra/dspam/bin/
dspam';
```

You can see `dspam` commented:

```
zimbra@mail:~$ more amavisd.conf | grep dspam
#$dspam = '/opt/zimbra/dspam/bin/dspam';
```

Now you need to enable DSPAM using the command:

```
$ zmlocalconfig -e amavis_dspam_enabled=TRUE
```

The `zmmtaconfig` command will automatically reload Amavis within 2 minutes, or you can run the following command for an immediate effect:

```
$ zmamavisdctl reload
```

If you check the different parameters in the `amavisd.conf` file, you will see it is uncommented:

```
$ more amavisd.conf | grep dspam
$dspam = '/opt/zimbra/dspam/bin/dspam';
```

Updating ClamAV independently of Zimbra updates

With each update of Zimbra comes the latest release of the ClamAV engine.

But sometimes you may need the latest package of ClamAV without waiting for Zimbra updates, especially for urgent security purposes, such as alerts of detection of critical bugs in the ClamAV release, so that the ClamAV community can correct it in the following release.

In this section, we will show you how to do that in a safe way.



The update of the ClamAV virus definitions base happens automatically every two hours by default, but you can configure it using the attribute: `zimbraVirusDefinitionsUpdateFrequency`

You can perform all the following actions either as a Zimbra user or any other user having `sudo` rights. If you do it all as a user other than a Zimbra user, remember to modify the ownership of the resulting `clamav-X.Y.Z` folder in `/opt/zimbra` to `zimbra:zimbra`.

If upgrading from anything below 0.90.x, please refer to:
http://wiki.zimbra.com/wiki/ClamAV_-_Updating_from_versions_lower_than_0.90.0

Step 1 – backing up your existing release

To avoid tricky situations, we should guarantee a rollback plan by preparing a backup for the existing release. To do that, all you need is to run the following command, making sure to replace the release version with yours:

```
cp -a /opt/zimbra/clamav-X.Y.Z ~/clamav-X.Y.Z.backup
```

Step 2 – updating

This is the main update step; we should start by getting the latest ClamAV source code from <http://www.clamav.net/download> (at the time of the writing of this book, the current stable version is 0.97.8).

Extract it to where you want; just don't forget our note about ownership if you are not logged in as a Zimbra user.

Assuming that the new ClamAV version is in the `/home/abdelmonam` directory:

```
tar -xvf clamav-0.97.8.tar.gz
cd clamav-0.97.8
```

Next, run `configure` inside the `clamav` extract as following:

```
./configure --prefix=/opt/zimbra/clamav-0.97.8 --with-user=zimbra --with-group=zimbra
```



In some cases, depending on your system configuration, you may have to install some other packages, which are dependencies, to be able to run the `configure` command.

If this step is completed successfully, I mean the output of your `configure` doesn't contain any errors, we can move to the next step: running the `make` command. However, if you get errors in your `configure` output, you should fix them before continuing. After fixing the errors, make sure to run `configure` again and then would go well.

Now run:

```
make
```

If the `make` output goes well, we can move to the next step; else, we should fix the errors in the `make` output. Note that we should switch to the root user to be able to run the following commands; to do that under Ubuntu, you need to run this command:

```
sudo -i
```

Now run:

```
make check
```

After that, run:

```
make install
```

If you have no errors, we can say that you now have the new version installed into the `/opt/zimbra/clamav-0.97.8` directory.

Before copying the `clamav` config file from the old release to the new one, you can compare your old `clamd.conf` and `freshclam.conf` files with the new ones:

```
cd /opt/zimbra/clamav-0.97.8/etc/
diff clamd.conf ../../clamav/etc/clamd.conf
diff freshclam.conf ../../clamav/etc/freshclam.conf
```

Then, you can copy these config files from the previous version to the new version directory:

```
mv clamd.conf clamd.conf.org
mv freshclam.conf freshclam.conf.org
cd /opt/zimbra/conf
cp clamd.conf /opt/zimbra/clamav-0.97.8/etc/
cp freshclam.conf /opt/zimbra/clamav-0.97.8/etc/
```

As a Zimbra user, run the following command to stop Zimbra:

```
zmcontrol stop
```

Now, delete the symbolic link and re-link it to the new install. As a root user, use the following command:

```
cd /opt/zimbra
ls -la | grep clamav
```

(You should see clamav -> /path/to/previous clamAV)

If so:

```
rm -rf clamav
```

If you want to keep the old install and link around, you can easily exit; just use the following command:

```
mv clamav clamav.old
```

Then:

```
ln -s /opt/zimbra/clamav-0.97.8 /opt/zimbra/clamav
```

Create the directory /opt/zimbra/clamav/db:

```
mkdir /opt/zimbra/clamav/db
```

Now, you should make sure the Zimbra user owns all of clamav:

```
chown -R zimbra:zimbra /opt/zimbra/clamav-0.97.8
```

The Zimbra user also needs access to the freshclam.conf file:

```
chmod a+r /opt/zimbra/clamav/etc/freshclam.conf
```

Next, we need to update the virus database:

```
abdelmonam@mail:~$ sudo -i
[sudo] password for abdelmonam:
root@mail:~# su - zimbra
zimbra@mail:~$
```

Run:

```
/opt/zimbra/clamav/bin/freshclam
```

If you get any warning, just run the command again to confirm that everything was successfully updated.

To start Zimbra, run:

```
zmcontrol start
```

Note that you may not need to stop Zimbra during this update. If you don't stop Zimbra, at this point just run:

```
zmantivirusctl restart
```

Run the following command to make sure the antivirus is running. If it is, you're good to go:

```
zmcontrol status
```

You should check `/opt/zimbra/log/clamd.log`, and `freshclam.log`, in the same directory, and also `/var/log/zimbra.log` for errors.

Using ASSP with Zimbra

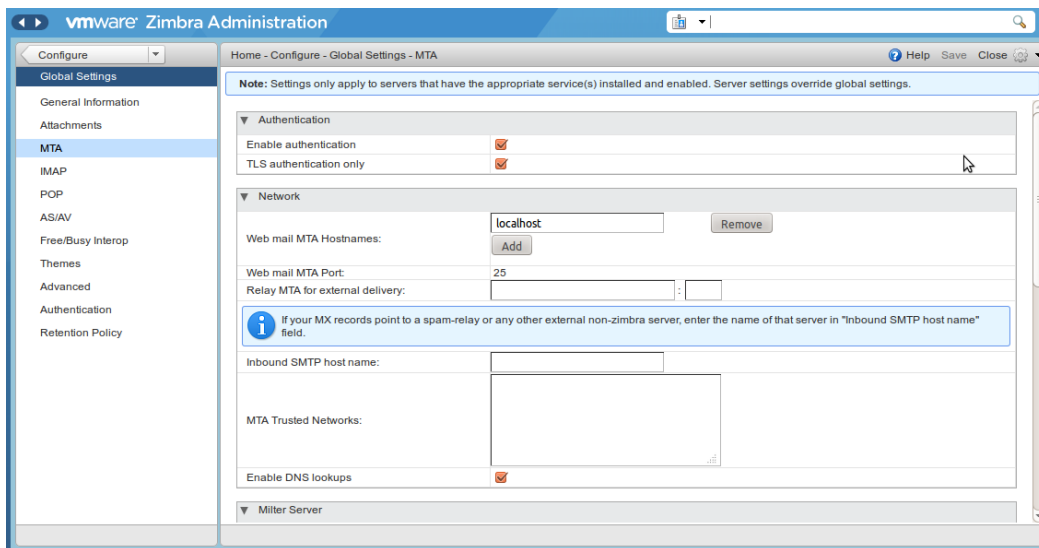
You can easily implement **Anti-Spam SMTP Proxy (ASSP)** with Zimbra as a separate appliance. All you need is a Linux distribution either on a simple machine or even a virtual machine; just configure ASSP to point to the Zimbra machine. You can either disable the antispam provided with Zimbra by default via admin console and use only ASSP, or keep it and use both internal and external antispam solutions to get better results.

You can also install ASSP on the same machine side by side with Zimbra; this implementation is a little bit more complex and can generate issues, especially when upgrading. The idea behind it is to change the receiving SMTP port inside Zimbra to a custom one that you choose, then install ASSP and configure it, firstly, to listen on the default port 25 and secondly, to forward mails to localhost at the customized Zimbra specified port number.

Despite its complexity and the upgrade issues that can occur, this method allows us to have both services on the same machine, which in turn reduces the amount of hardware or virtual instances to be maintained.

Independently of the method chosen to handle incoming e-mails, we must also configure all outgoing e-mails to be forwarded to the ASSP instance if you would like ASSP to maintain its automatic whitelist. Doing that is quite easy; all you need to do is specify the port and address of the ASSP instance in the Zimbra administration console:

1. Navigate to **Configure | Global Settings | MTA**.
2. Configure the **Relay MTA for external delivery** field from the administration console as shown in the following screenshot:



You will also need to ensure that the ASSP administrators and users can send e-mails to ASSP. The slickest way to do this, I think, is to create distribution lists in Zimbra with a single address similar to the desired ASSP reporting address. For example, create a distribution list named `ASSP.Spam@zimbra-essentials.com` and enter a single list member — `asspspam@your-assp-host.com`. Make the display name something like "ASSP: Forward Spam Here".

The whole point of this exercise is to get the ASSP reporting addresses into Zimbra's **Global Address List (GAL)**. Use a naming convention for these addresses, so they all sort together in the GAL. In this example, each display name would begin with "ASSP:".

One should also put the prefix – in this case "ASSP" – in the first name blank and the function – "Forward Spam" – in the last name when creating the distribution list. Then, users can easily look up all the appropriate addresses in the GAL if they forget what they are.

Improving SpamAssassin

There is more than one level to improve SpamAssassin; here is a list of them:

salocal.cf.in

The best way to configure the SpamAssassin filtering rules is to edit the `/opt/zimbra/conf/salocal.cf.in` file. Just keep in mind to back up this file before each Zimbra upgrade, because it will be replaced during this operation.

Blacklists and whitelists

This is the simplest way to add filtering rules for SpamAssassin, in fact to block all mails going from an address or domain. You just have to add the address or the domain into a blacklist entry, and vice versa if you want that mails from a specific address or domain should bypass all filtering rules, we just need to add this address or domain into a whitelist entry.

The following example shows how to add blacklist or whitelist entries to the `salocal.cf.in` file:

```
blacklist_from sales@abcde.com
whitelist_from bill@xyz.net
blacklist_from *@abc-xyz.net
```

Note that `*` is a wildcard. In this example, `*@ abc-xyz.net` indicates all e-mails from any user at `abc-xyz.net`.

Zimbra SpamAssassin needs to be restarted for each modification on the `salocal.cf.in` file; to do that, we have to run the following command as a Zimbra user:

```
zmmactl restart && zmamavisdctl restart
```

Basic rules

As we saw, blacklists and whitelists are used to filter addresses and domain names; however, this is not sufficient to filter spam mails, which is why there is another way based on content filtering that SpamAssassin uses to detect spam via reading headers, content of mails, and applying rules to that content.

Rules can be in the form of a particular word or phrase, as well as a variety of built-in functions. When a rule is "hit" while evaluating an e-mail, a point score is added to that e-mail's total score. When an e-mail's total score exceeds a certain threshold (typically 5 on a Zimbra system), the e-mail is either marked as spam, or deleted automatically if the score is high enough.

Rules are in the form of a test followed by a score. The rule mechanism typically uses Perl regular expressions to search for specific content within an e-mail. Custom rules should be added to the `saLocal.cf.in` file in the following format:

```
body LOCAL_RULE /sale/  
score LOCAL_RULE 0.5
```

The preceding code creates a rule called `LOCAL_RULE` that searches the body of the message for the word "sale" in lower case. If it finds the word "sale" anywhere in the body, it adds 0.5 to the total score of the e-mail. Note that the score is only applied once—multiple instances of the word "sale" in the same e-mail will not be scored separately. Also note that you should always precede the name added by the user in his/her defined rules with the word `LOCAL` as in the given example, to distinguish them from built-in SpamAssassin rules and prevent accidental duplicate names.

Perl regular expressions are quite powerful mechanisms for locating text. The following are some additional examples of Perl regular expression-based rules:

Performs a case-insensitive search for the word "sale":

```
body LOCAL_SALE /sale/i
```

Searches for a line that starts with the words "hot stock tip" in any case:

```
body LOCAL_STOCK1 /^hot stock tip/i
```

Searches for any four capital letters in a row (generally a stock symbol):

```
body LOCAL_4CAPS /[A-Z] [A-Z] [A-Z] [A-Z]/
```

Searches for three digits, a decimal point, and two more digits, and treats it as a word:

```
body LOCAL_MONEY /\d?\d?\d?.\d\d\b/
```

Meta rules

We can also search for a combination of rules and apply a score to that combination by creating a "meta" rule in the following format:

```
body LOCAL_FOUR_CAPS /[A-Z] [A-Z] [A-Z] [A-Z] /
body LOCAL_MONEY /\d?\d?\d?.\d\d\b/
meta LOCAL_STOCK (LOCAL_MONEY && LOCAL_FOUR_CAPS)
score LOCAL_STOCK 1
```

The given rule would add 1 to an e-mail's score only if both `LOCAL_FOUR_CAPS` and `LOCAL_MONEY` were hits. Be careful when creating meta rules, as it is easy to "over-score" an e-mail, as in the following code:

```
body LOCAL_FOUR_CAPS /[A-Z] [A-Z] [A-Z] [A-Z] /
score LOCAL_FOUR_CAPS 1
body LOCAL_MONEY /\d?\d?\d?.\d\d\b/
score LOCAL_MONEY 1
meta LOCAL_STOCK (LOCAL_MONEY && LOCAL_FOUR_CAPS)
score LOCAL_STOCK 1
```

The given example could add 3 points to the e-mail score, if the meta rule hits.

After editing the `salocal.cf.in` file, restart Zimbra SpamAssassin by issuing the following command at the server prompt (as a Zimbra user):

```
zmmactl restart && zmamavisdctl restart
```

Sender Policy Framework (SPF)

The **Sender Policy Framework (SPF)** is an open standard specifying a technical method to prevent forgery of the sender address. More precisely, the current version of SPF—called SPFv1 or SPF Classic—protects the envelope sender address, which is used for the delivery of messages.

Read more about SPF and how to configure it for any domain at <http://www.openspf.org/>

Also, read about tools for testing your SPF settings at <http://www.openspf.org/Tools>

First of all, Zimbra SpamAssassin has no SPF enabled. Since the Perl environment is system-way-integrated, adding SPF support is fairly simple.

We can install it on Debian/Ubuntu-like systems via the following command:

```
sudo apt-get install libmail-spf-query-perl
```

For every other platform, you can install SPF by opening and configuring it; if you didn't, use the cpan command line utility and execute the following commands:

```
perl -MCPAN -eshell
install Mail::SPF::Query
```

Razor2

Razor is a collaborative spam filtering network allowing users to report and filter out matching spam. After adding SPF, we can add Razor2 to enhance scores.

To install Razor2, we should first of all get the `razor-agents-sdk` package from `razor.sourceforge.net`, then untar it and run the following commands as a root user (that will compile and then install it):

```
perl Makefile.PL
make
make install
```

Repeat the preceding action with the `razor-agents` package that you get from `razor.sourceforge.net`:

```
perl Makefile.PL
make
make install
```

Don't forget to open the firewall ports for Razor2 (TCP/2703 outgoing).

Configuring Razor2

To configure Razor2, start by creating a `.razor` folder under `/opt/zimbra/amavisd` and, of course, don't forget to give Zimbra user permissions; follow this:

```
mkdir /opt/zimbra/amavisd/.razor; chown -Rf zimbra:zimbra /opt/zimbra/
amavisd/.razor
```

Then, as the Zimbra user, create your Razor account:

```
razor-admin -home=/opt/zimbra/amavisd/.razor -create
razor-admin -home=/opt/zimbra/amavisd/.razor -discover
razor-admin -home=/opt/zimbra/amavisd/.razor -register
```

Finally, enable Razor (if it is not done already). To do that, edit `/opt/zimbra/conf/spamassassin/v310.pre` and uncomment the line:

```
loadplugin Mail::SpamAssassin::Plugin::Razor2
```

Pyzor

Like Razor, Pyzor too serves to increase spam scores. Now, we are going to add Pyzor support to increase (again) spam scores. We can install it to improve spam filtering inside Zimbra.

Installing Pyzor

As we are using Ubuntu, to install Pyzor, we need to just run the following command:

```
sudo apt-get install pyzor
```

Configuring Pyzor

To configure Pyzor, start by creating the `.pyzor` folder into `zimbra-amavisd` home and, of course, don't forget to give Zimbra user permissions; follow this:

```
mkdir /opt/zimbra/amavisd/.pyzor; chown zimbra:zimbra /opt/zimbra/amavisd/.pyzor
```

Don't forget to open your firewall ports for Pyzor (UDP/24441 outgoing).

Finally, as a Zimbra user, run the following command:

```
pyzor --homedir /opt/zimbra/amavisd/.pyzor discover
```

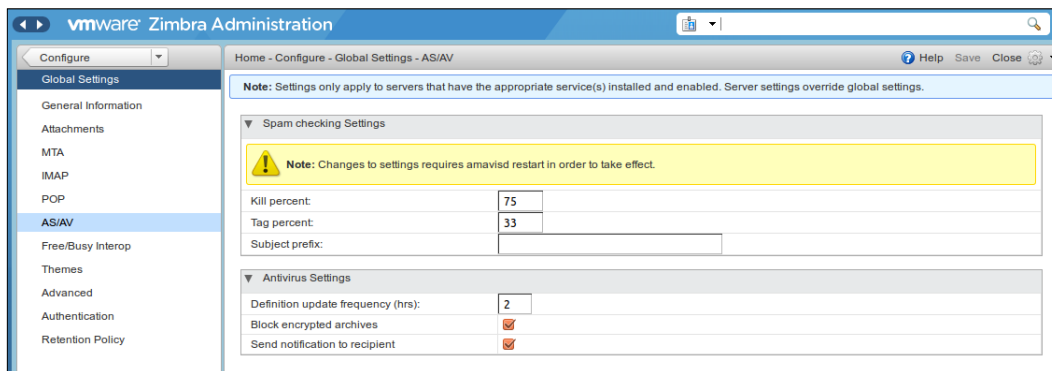
How to configure SpamAssassin

At this point, we have all three filters: Pyzor, Razor, and SPF. However, to gain the advantages of these tools, we should enable them and set rules for them inside the SpamAssassin configuration. To do that, edit the `/opt/zimbra/conf/spamassassin/local.cf` file and add the following rules at the end; of course, you can change values as you want and customize rules to suit your needs:

```
ok_languages en fr
ok_locales en fr
trusted_networks 127. 172.16.
use_bayes 1
skip_rbl_checks 0
```

```
use_razor2 1
#use_dcc 1 <<< WORK IN PROGRESS - SEE NEXT STEP
use_pyzor 1
dns_available yes
## Optional Score Increases
## Choose your preferred values...
score DCC_CHECK 4.000
score SPF_FAIL 10.000
score SPF_HELO_FAIL 10.000
score RAZOR2_CHECK 2.500
score PYZOR_CHECK 2.500
score BAYES_99 4.300
score BAYES_90 3.500
score BAYES_80 3.000
bayes_ignore_header Received: from mail.zimbra-essentials.com
bayes_ignore_header Received: from localhost
```

To get the required `score` parameter in Zimbra, we don't need to edit any config file. This value is calculated from a setting in the Zimbra admin page. Enter administration, and go to **Global Settings | AS/AV**. The required `score` parameter is `tag percent x 0.2`. So a **Tag percent** value of 33 will result in a required score of 6.6 ($33 \times 0.2=6.6$).



Adding DCC

We can also enable **Distributed Checksum Clearinghouses (DCC)** to enhance antispam content filtering.

The basic logic in DCC is that most spam mails are sent to many recipients. The same message body appears many times; therefore, it creates bulk e-mail. DCC identifies bulk e-mail by taking a checksum and sending that checksum to a Clearinghouse (server). The server responds with the number of times it has received that checksum. An individual e-mail will create a score of 1 each time it is processed. Bulk mail can be identified because the response number is high. The content is not examined.

To set up DCC, start by downloading it from <http://www.rhyolite.com/dcc/>.

Compile and install it, then change `/etc/dcc/dcc_conf` to read:

```
DCCUID=zimbra
DCCD_ENABLE=off
```

After that, change `/opt/zimbra/conf/spamassassin/v310.pre` to enable the DCC plugin:

```
loadplugin Mail::SpamAssassin::Plugin::DCC
```

Finally, enable DCC on the firewall (UDP/6277 outgoing).

External solutions

In this section, I will show you the best external solution to enhance security for any mailing server in general, and for Zimbra in particular. It is up to you to choose the solution/mixed solutions you want depending on your need.

Barracuda spam and virus firewall

This is a powerful mail security turnkey solution that provides filtering for incoming and outgoing mails. It is composed of a lot of security components, such as antivirus, antispam, antispymware (for attachments), anti-phishing, anti-spoofing, data leak prevention, DDoS, and a cloud protection layer.

This solution is compatible with all e-mail servers; it can also fit into most corporate types and dimensions. It can handle the traffic of a small company with less than 10 employees as well as the traffic of a huge organization with more than 200,000 employees. A single server handles around 100,000 active e-mail accounts. And for scalability and high availability, Barracuda supports the clustering of many units.

This solution protects your e-mail server with 12 defence layers, such as IP reputation analysis, rate control, network denial-of-service protection, sender authentication, recipient verification, spam fingerprint check, virus scanning, policy (user-specified rules), intent analysis, Bayesian analysis, image analysis, and rule-based scoring.

MailCleaner

This is a full-security mail-filtering gateway. It is based on a GNU/Linux OS and it comes in the form of an ISO image that contains a fully automated installer. So, we can say that it is a complete Linux distribution, it contains a graphical web interface for both frontend and backend access.

MailCleaner forms a filtering layer between your mail server (in our case, it is the Zimbra server) and the Internet; you can set it up as the new MX record for your domain(s) or you can get mails from your frontend gateways. After finishing the filtering operation, the messages will be forwarded to your destination mail server(s) or the next gateway(s).

MailCleaner is built on popular and very efficient free software:

- **OS:** Debian
- **MTA:** Exim
- **Filtering:** MailScanner
- **Antispam:** SpamAssassin
- **Antivirus:** ClamAV
- **Web GUI:** Apache/PHP/MySQL

The advantage of MailCleaner is that the usage of these tools is almost transparent for the users and administrators, as configuration and settings are done through a unified and intuitive interface.

A specific merit is that any user (either an administrator, or a simple user) can access the system, so any user can check his quarantine in real time and customize his preferences.

Some key features are filtering unsolicited messages, filtering any potentially dangerous e-mails, and managing any number of domains with independent configurations, policies, and templates, clustering capabilities for large volumes, and a web-based user interface for quarantine and personal settings.

IronPort

IronPort mail security is a solution provided by Cisco; it helps organizations of different sizes to:

- Minimize the downtime associated with e-mail-borne malware
- Simplify the administration of corporate mail systems
- Reduce the burden on technical staff, while offering insight into mail-system operations

Its main capabilities are:

- Anitspam
- **Data loss prevention (DLP)**
- Antivirus
- E-mail encryption
- Tracking and reporting tools

Cisco offers a choice of features and functionalities available on appliance-based, cloud-based, hybrid, or managed solutions.

Maia Mailguard

Maia Mailguard is a web-based interface and management system based on the popular amavisd-new e-mail scanner and SpamAssassin. Written in Perl and PHP, Maia Mailguard gives end users control over how their mail is processed by virus scanners and spam filters, while giving mail administrators the power to configure sitewide defaults and limits.

Its features are user-oriented quarantine management, a user-friendly web interface, flexible user authentication, powerful administration tools, effective spam and virus management tools, a scalable design, data security and integrity, and statistics tracking.

Untangle

This is a well-known open source security solution; most people know it as a firewall, but it is more than a firewall. Untangle provides three different packages: Lite, Standard, and Premium.

The Lite package is free, but the Standard and Premium packages are paid for by subscription. Each comprises a collection of Untangle network software applications.

Untangle applications include antispam, web content filtering, antivirus, anti-phishing, anti-spyware, intrusion prevention, firewall, openVPN, router, protocol control, attack blocker, reporting, policy manager, Kaspersky virus blocker, Commtouch spam booster, ESoft web filter, directory connector, captive portal, AdBlocker, WAN balancer, WAN failover, bandwidth control, web cache, and Branding Manager on the Untangle gateway platform.

The Untangle Lite package offers a collection of free, open source software applications to run on the Untangle Server. It provides an entry-level multifunctional firewall, with 12 products among which we can find what we need to fulfill our objective of improving Zimbra security with open source software: virus blocker, spam blocker, phish blocker, and spyware blocker.

Summary

In this chapter, we saw different mechanisms that enhanced the security for a Zimbra server. We started with internal solutions, where we learned how to enhance security inside Zimbra. Then we took a look at the best external solutions that we can use side by side with Zimbra, to ameliorate security of our mail traffic.

At this point, we have installed and secured our Zimbra Server. In the next chapter, we will move to another level: how to manage Zimbra configuration. See you there.

4

Managing Configuration

This chapter serves as an administration guide to configure Zimbra.

The topics covered in this chapter are:

- Managing global configuration
- Managing server settings
- Managing SSL certificates

By the end of this chapter, the user should be able to administrate Zimbra.

During the initial installation step, all Zimbra components are configured. And you can, of course, modify this configuration after installation, either by using the administration console or via the CLI utility.

This chapter will focus on managing Zimbra via the administration console; it will cover the most-used items but not all of them. You can get help from the administration console about how to perform tasks from it; you can refer to it for items not covered here.

If the task is only available from CLI, go to the following link for a description of how to use the CLI tool: http://www.zimbra.com/docs/os/6.0.8/administration_guide/A_app-command-line.13.01.html

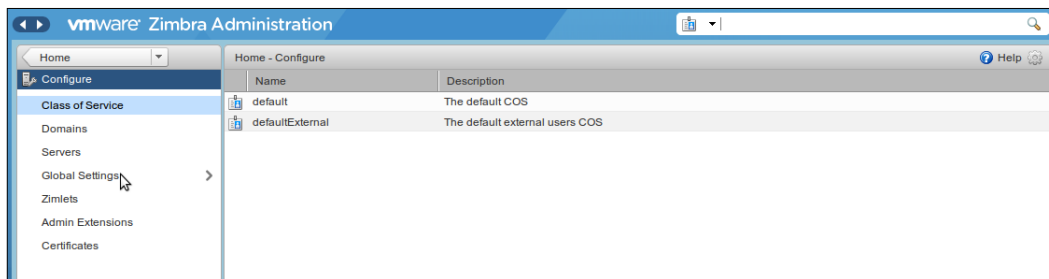
Understanding global configuration management

Global settings are initially set during the installation process, and we can modify them at any time using the administration console. Any modification in global settings is applied to all accounts inside the Zimbra servers.

The configurations set in the global settings cover the inherited default values for the following objects: server, account, **Class of Service (COS)**, and domain. If these attributes are configured in the server, the server settings override the global settings.

For the configuration of global settings, go to the administration console at <https://172.16.126.14:7071/zimbraAdmin>.

Then go to **Configure | Global Settings** as shown in the following screenshot:



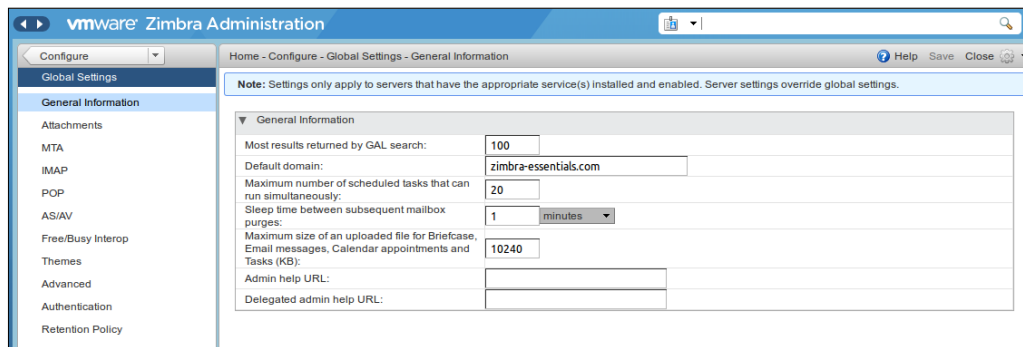
This page contains the following items:

- **General Information**
- **Attachments**
- **MTA**
- **IMAP**
- **POP**
- **AS/AV**
- **Free/Busy Interop**
- **Themes**
- **Advanced**
- **Authentication**
- **Retention Policy**

General global settings

This page includes the following items:

- **Most results returned by GAL search**
- **Default domain**
- **Maximum number of scheduled tasks that can run simultaneously**
- **Sleep time between subsequent mailbox purges**
- **Maximum size of an uploaded file for Briefcase, Email messages, Calendar appointments and Tasks (KB)**
- **Admin help URL**
- **Delegated admin help URL**

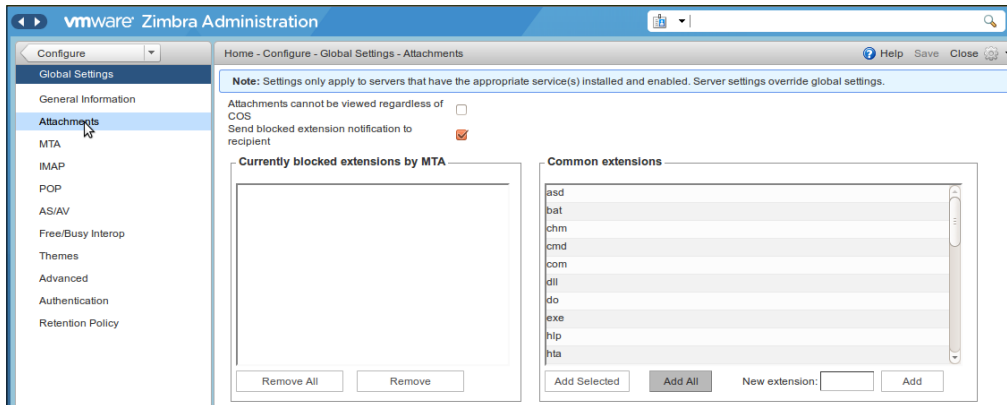


Attachments

With global e-mail attachment settings, you can specify global rules for handling attachments to an e-mail message. Besides these global settings, you can also set different rules by class of service and for individual accounts.

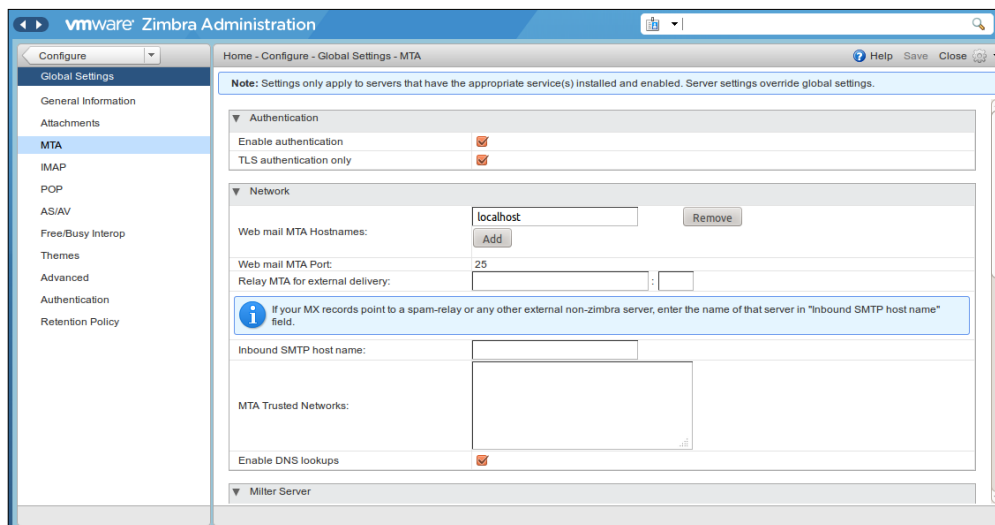
You can also filter on some types of file attachments and reject messages with these types (for example, *.mp3). You can define which files types are authorized and which are not, and you can add new extension types to the list.

By default, if a message is rejected because of its attachment's file type, the sender and the recipient are notified that the message was blocked. But if you would like to disable this default option, you can do it either via an external e-mail security gateway as explained in *Chapter 3, Securing Zimbra*, or by navigating to **Global Settings | Attachments** as shown in the following screenshot:



Global MTA settings

To configure the mail transfer agent settings inside Zimbra, go to **Global Settings | MTA**. From this page you can enable/disable authentication and configure a relay hostname (it was useful, for example, for *Chapter 3, Securing Zimbra*, when we proposed to configure a frontal security server). In this page, you can also set the maximum message size, enable DNS lookups, and perform protocol and DNS checks.

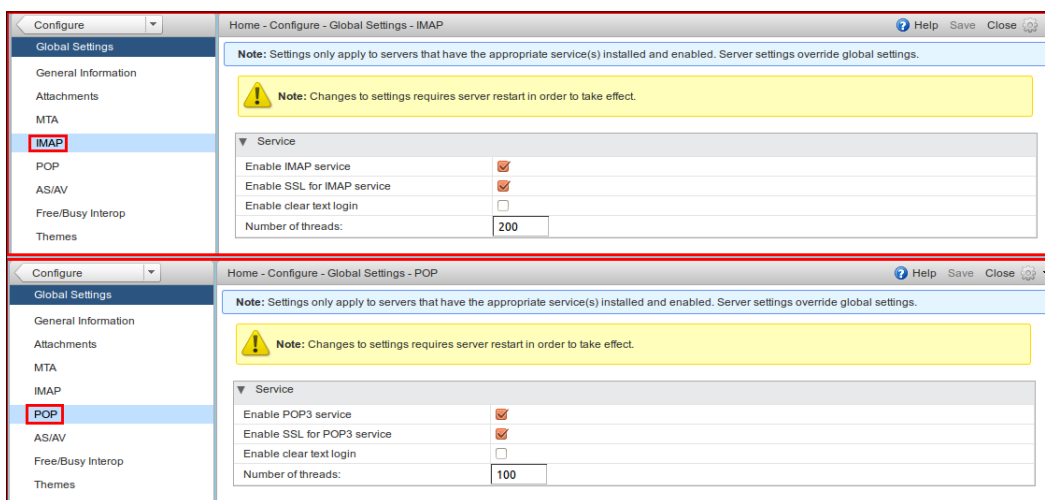


Global IMAP and POP settings

For IMAP and POP access, we have more than one method to configure them: we can enable them either by editing a server's IMAP or POP pages or as a global setting by navigating to **Global Settings | IMAP** or **POP**.

In order to perform any changes in the IMAP or POP settings we need to restart Zimbra. The changes do not take effect unless we restart Zimbra.

To set IMAP and POP polling intervals from the administration console, you should go to the **COS Advanced** page. The default option is to not set the polling interval.

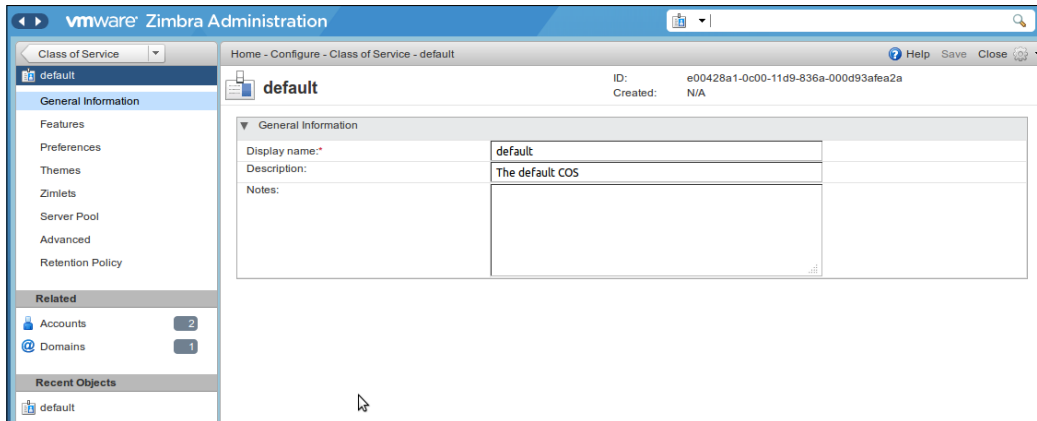


Configuration per COS

COS is a specific concept in Zimbra that defines default attributes related to users' accounts and the features that are enabled or disabled. The COS supervises mailbox quotas, attachment policy, password policy, message lifetime, and server pool.

During Zimbra installation, a default COS is automatically created. We can modify this default COS as well as create new ones.

To set a specific configuration for the default COS or any specific COS go to **Configure | Class of Service**, choose the COS you want to configure, then update the settings with your own, as shown in the following screenshot:



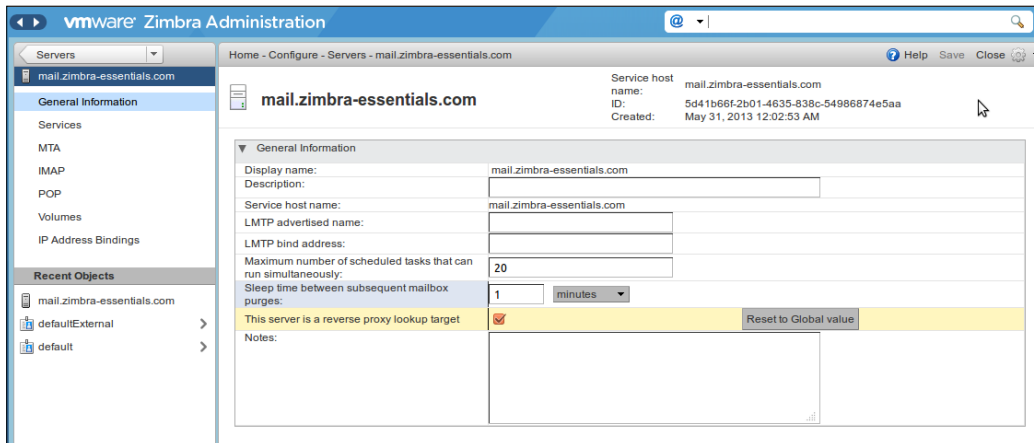
Managing server settings

From the administration console, you can perform a lot of tasks on your server's settings, but not all of them. For example, you can view the current status of all your servers configured with Zimbra, you can also edit or delete the existing server records, but you cannot add any server directly to LDAP, since the Zimbra installation program is the only way to add new servers because it is designed to register the new host during the installation process.

The server settings that can be viewed from the admin console are discussed next.

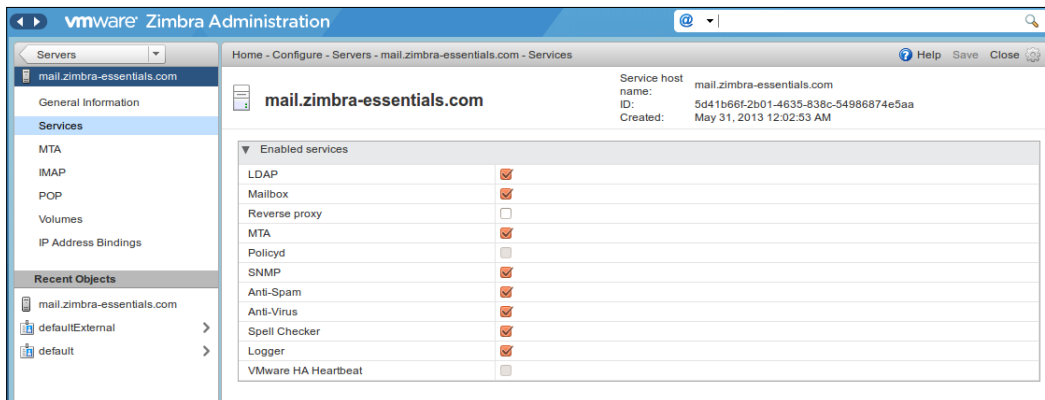
General information

The **General information** page allows you to view/edit some generic information about the selected server such as the service hostname, LMTP advertised name and bind address, and the number of threads that can simultaneously process data source imports.



Services

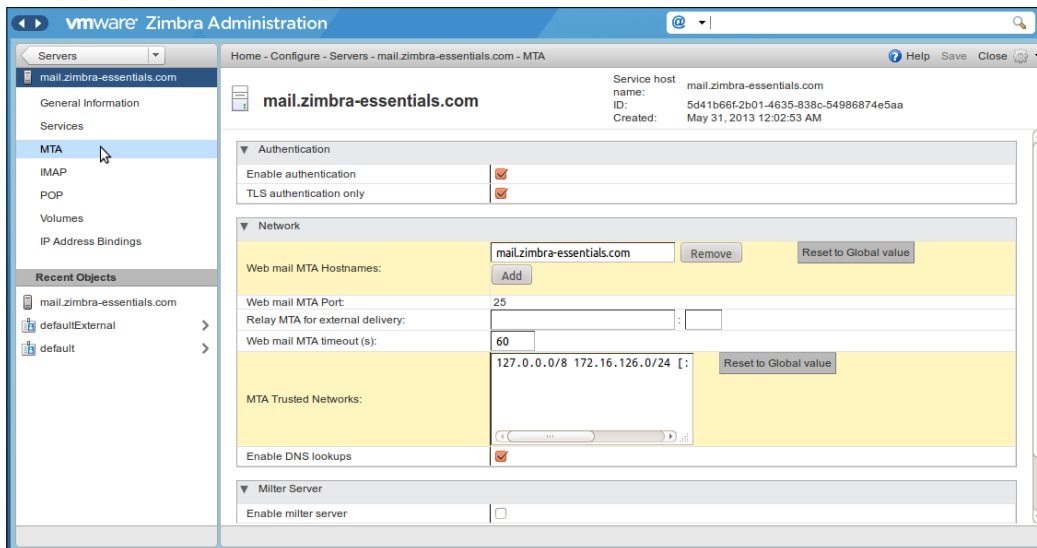
This page contains the list of existing services under the selected server. You can disable or enable the service you want by checking it in/checking it out in this list, as shown in the following screenshot:



MTA

This page contains several settings related to the **Mail Transfer Agent (MTA)** such as:

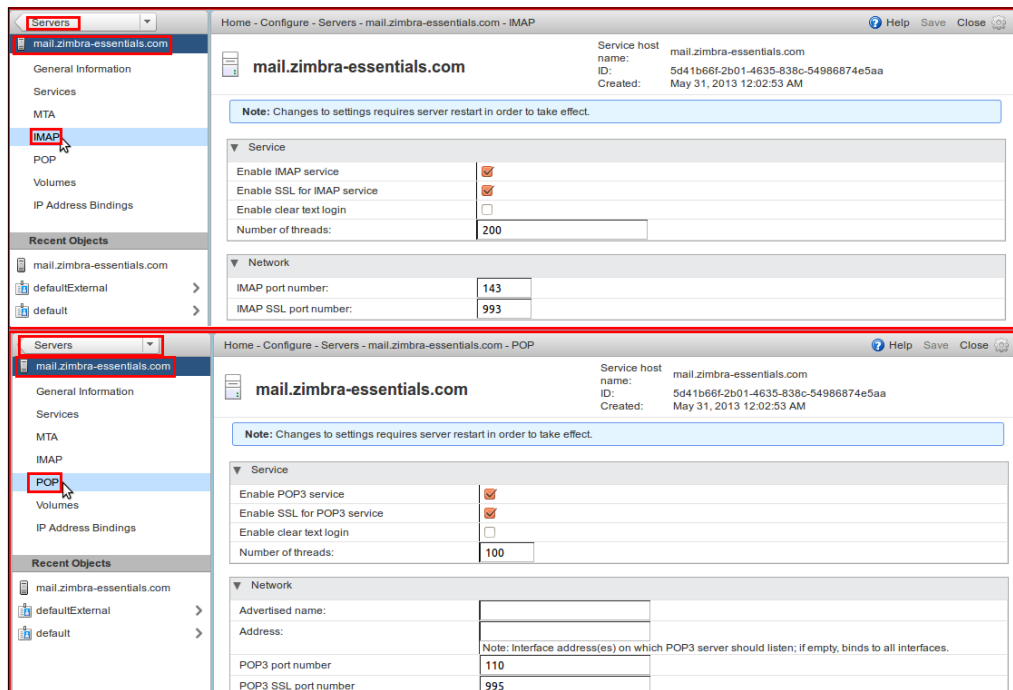
- Authentication (whether it is enabled or not, whether we are using TLS only or not, and so on).
- Settings of the Web mail MTA that Zimbra uses to send mails.
- Settings of the relay MTA for external delivery (nonlocal e-mail) when using an external MTA relay.
- Enabling DNS lookup if required. If it is disabled, you should set an MTA relay.



IMAP/POP

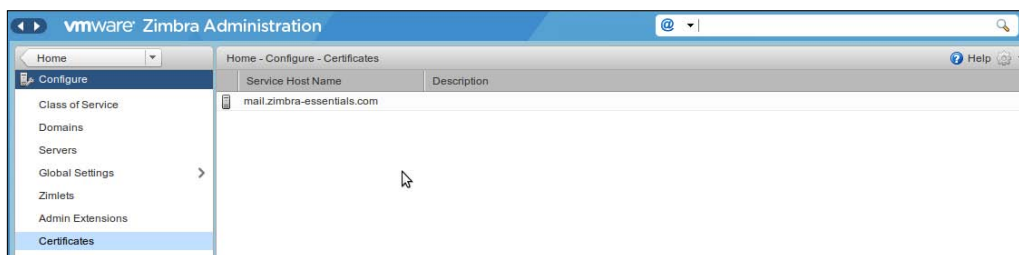
This page allows you to configure POP and IMAP settings such as enabling/disabling these services, setting the port numbers for a server, and enabling/disabling SSL.

Note here that if the IMAP/POP proxy is set up, you should make sure that the port numbers are configured correctly.



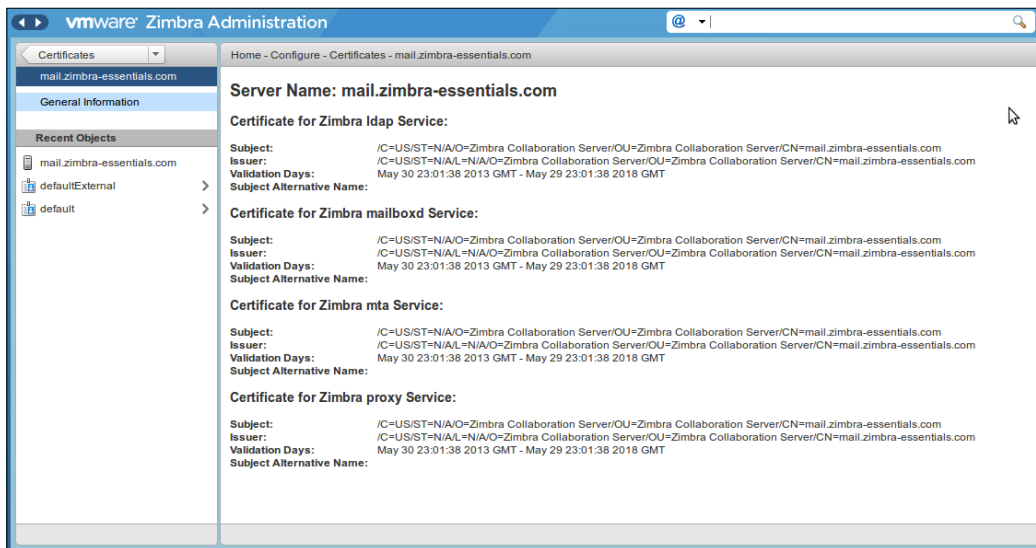
Managing SSL certificates

During the Zimbra installation process, and exactly at the final steps, the installer automatically generates and installs a self-signed certificate to be used for testing purposes. But in the production environment, you should generate and install a commercial certificate.



Checking installed certificates

With the Zimbra administration console, you can view the details of the certificates that are currently deployed. These details include the certificate subject, issuer, validation days, and subject alternative name. To do that, go to **Home | Configure | Certificates**, then select a service hostname. Certificates will display for different Zimbra services such as LDAP, mailboxd, MTA, and proxy as shown in the following screenshot:

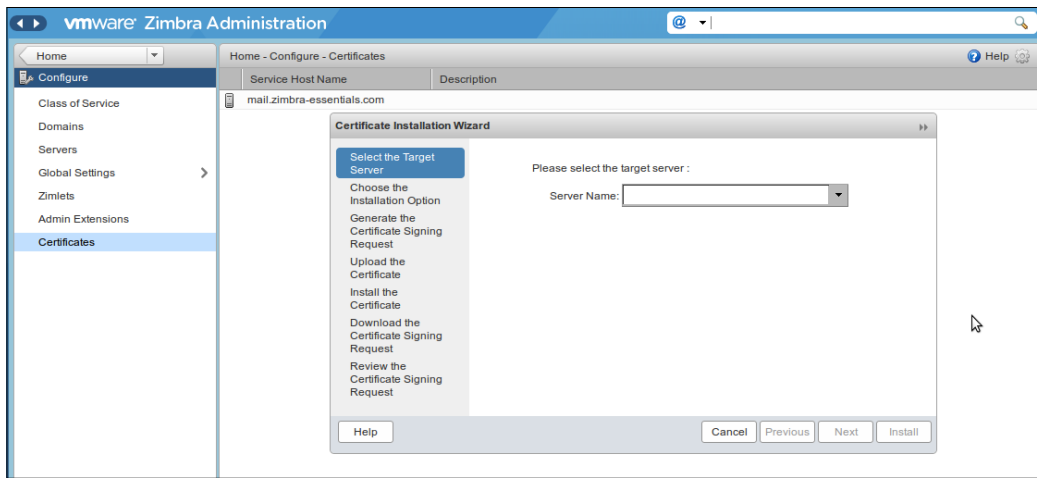


Installing certificates

In the following steps, we will see how to install certificates for the Zimbra server:

1. First of all you must generate the **Certificate Signing Request (CSR)**. To do that, you should complete a form with details about the domain, company, and country. After that, generate a CSR using the RSA private key. Next, save this file on your computer and then submit it to your commercial certificate authorizer. This is the general process; later, we will detail it step by step for Zimbra context. For obtaining the commercially signed certificate you need, use the Zimbra certificates wizard from the administration console to generate the RSA private key and CSR. To do that, go to **Home | Configure | Certificates** and after clicking on the gear icon select **Install Certificates**. This will display the **Certificate Installation Wizard** dialog box.

2. Enter the required information, then download the CSR from the Zimbra server, and before finishing, submit it to a certificate authority, such as VeriSign or GoDaddy. They issue a digitally signed certificate, and this is what we need.
3. When you receive your certificate, use the certificates wizard again to install the certificate on your Zimbra server. After installing the certificate, you must restart the server to finally apply the certificate.



Summary

In this chapter, we saw a general overview of the Zimbra management tasks. We also saw how to manage the global configuration, server settings, and SSL certifications. In the same manner, we will see how to manage user accounts in the next chapter.

5

Configuring User Accounts

This chapter serves as an administration guide to configure user accounts.

The topics covered in this chapter are:

- Managing user accounts
- Customizing accounts

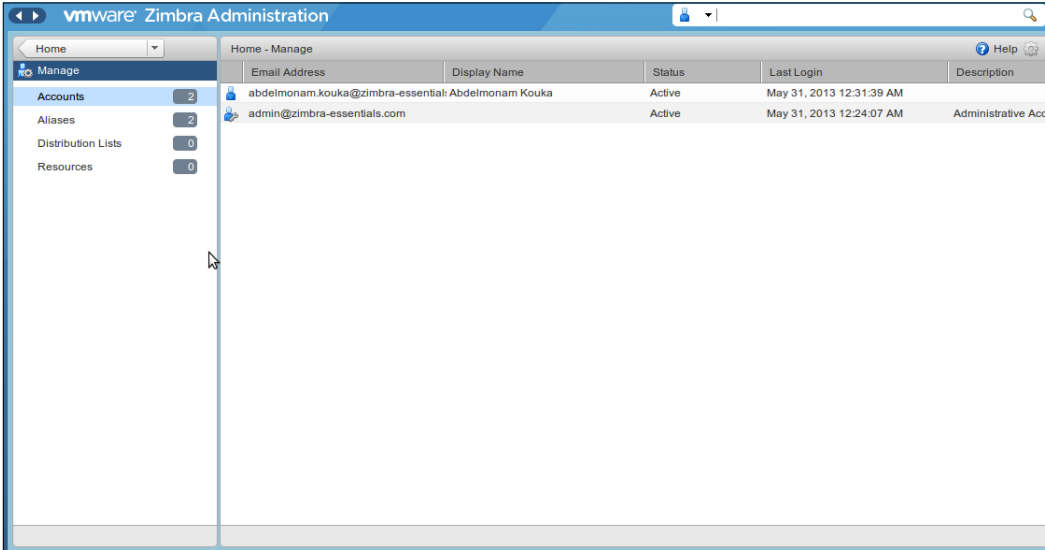
By the end of this chapter, the user should be able to manage and customize Zimbra accounts.

Managing user accounts

As other administration tasks, managing users' accounts can be done either via CLI or the management console. In this section, we will cover only the management console part.

Configuring User Accounts

First of all you need to go to **Home | Manage | Accounts** as shown in the following screenshot:



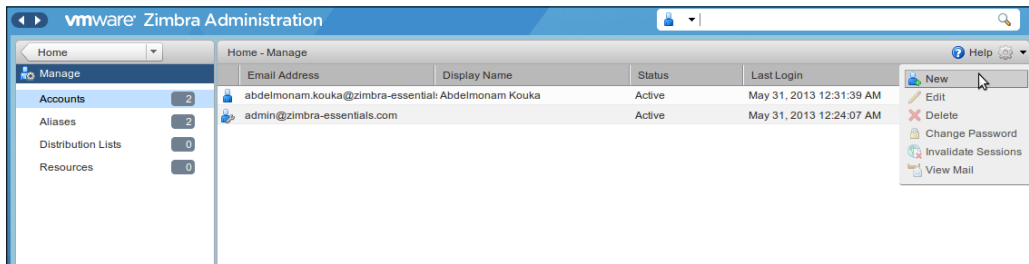
In this interface, you can see a list of existing accounts with some information such as name, status, and last login.

From this interface, you can add/edit/delete the user account via the gear button in the top-right corner of the central frame.

In the next section, we will see an example of creating an account.

Creating user accounts

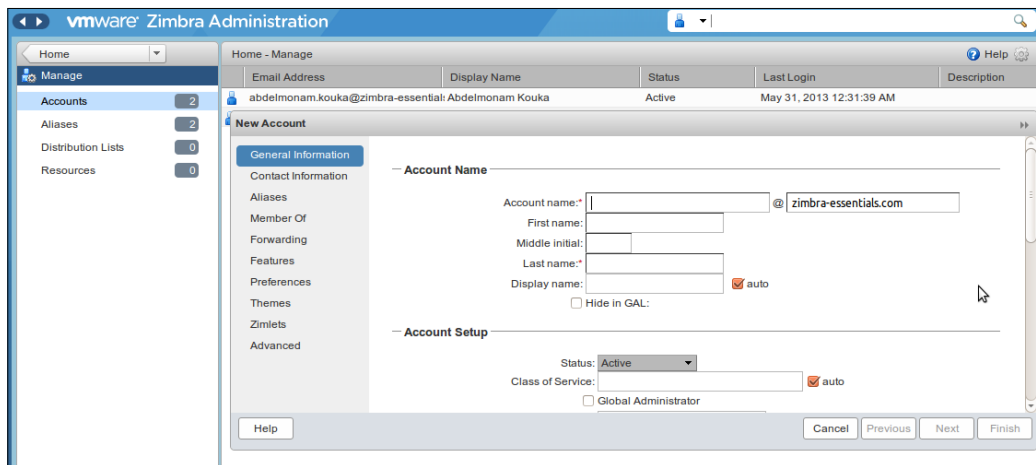
To create a new user account, you should go to **Home | Manage | Accounts** as we saw earlier, then click on the gear button in the top-right corner of the central frame, and finally select **New** as shown in the following screenshot:



After that you will get a frame containing the "create user wizard"; using this wizard you can create and customize the new user. All you need to create the new user is to enter the mandatory information such as the account name and password. For customization, you have a lot of options such as themes and mailing list memberships.

Note that for customization, you can do/change it later also.

The following is how the wizard looks:

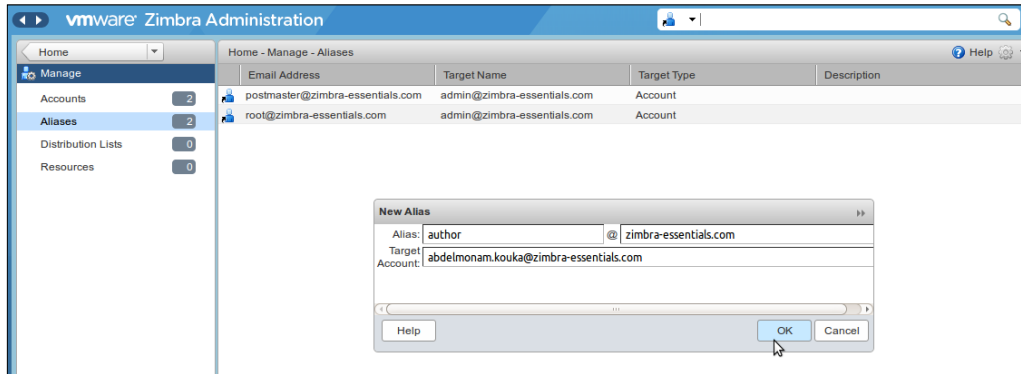


Creating aliases

You can also create an alias for the user account. An e-mail alias is an e-mail address that redirects all mails to a specified mail account. An alias is not an e-mail account. Each account can have unlimited numbers of aliases. You can create an alias for the user account with the help of following steps:

1. From the administration console, go to **Manage | Aliases**.
2. Go to the gear icon and click on it, then click on **New**.

3. On the pop-up window, add the alias you want, the target user account you would like to point to, and then confirm by clicking on the **OK** button.



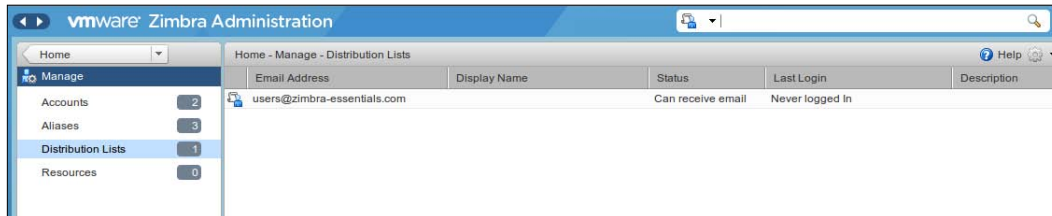
Creating distribution lists

You can also create mailing lists or distribution lists. A **distribution list** is a group of e-mail addresses contained in a list with a common e-mail address. When a message is sent to the distribution list address, all members of this list (whose e-mail addresses are included in the list) will receive this message. The "To" field in the header of the mail displays only the distribution list address and none of the individual recipients' addresses can be viewed. As a real example here, members of a specific team in a company could be part of a distribution list so that they all receive e-mails sent to the group address, for instance, `support@mycompany.com`.

After adding the user e-mail address to a distribution list, the **Member Of** page related to the user's account is updated with the list name. In the same manner, when a distribution list is deleted or the user e-mail address is removed from this list, the **Member Of** page is updated and automatically the distribution list is removed from the user account. You can create and populate a distribution list with the help of following steps:

1. From the administration console, go to **Manage | Distribution Lists**.
2. Go to the gear icon and click on it, then click on **New**.
3. On the **Members** page, enter the distribution list name. The other fields are optional.
4. In the **Add Members to this list** section, you can search for names from the address book. You can also enter a complete e-mail address in the **Or enter addresses below** section.
5. Click on **Next** to continue the configuration of other pages.

- Finally, after adding all names to the list, click on the **Save** button. The distribution list is enabled and the distribution list address is created. In the following screenshot, we can see the result of creation of the `users@zimbra-essentials.com` distribution list:

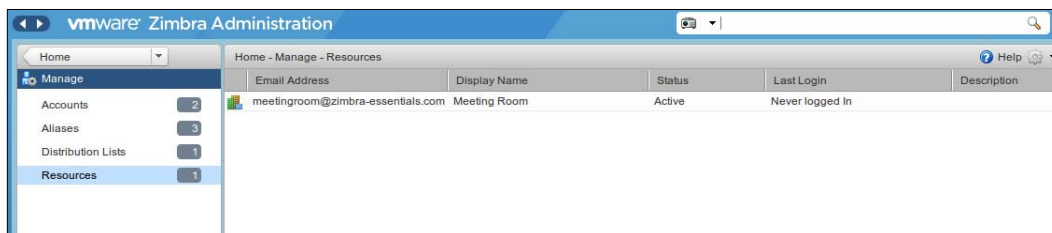


Creating resources

Resources such as locations and equipments can also be created and used via Zimbra. Why do we need to create such a resource on Zimbra? Simply because it helps us to avoid booking a resource twice for the same period. For example, if the user X creates an event and invites the user Y to it, and plans it in the meeting room Z between fourteenth hour and fifteenth hour, by using the concept of resource account inside Zimbra, no other user can book meeting room Z for the same period, since it is already booked as a resource in another calendar event. We can create a resource with the help of following steps:

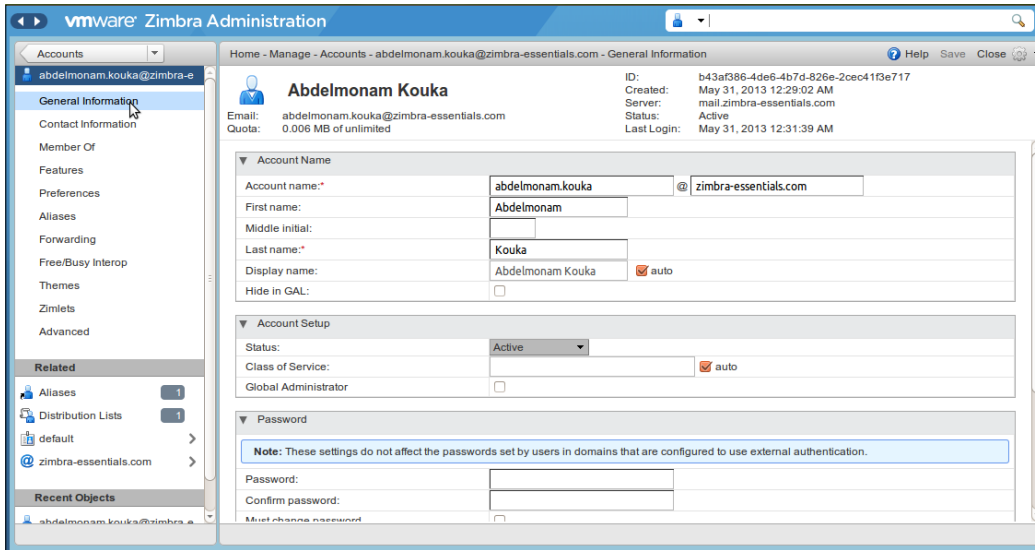
- From the administration console, go to **Manage | Resources**.
- Go to the gear icon and click on it, then click on **New**.
- Introduce the information that is requested.

In the following screenshot, I created a new resource, **Meeting Room**, as a location resource:

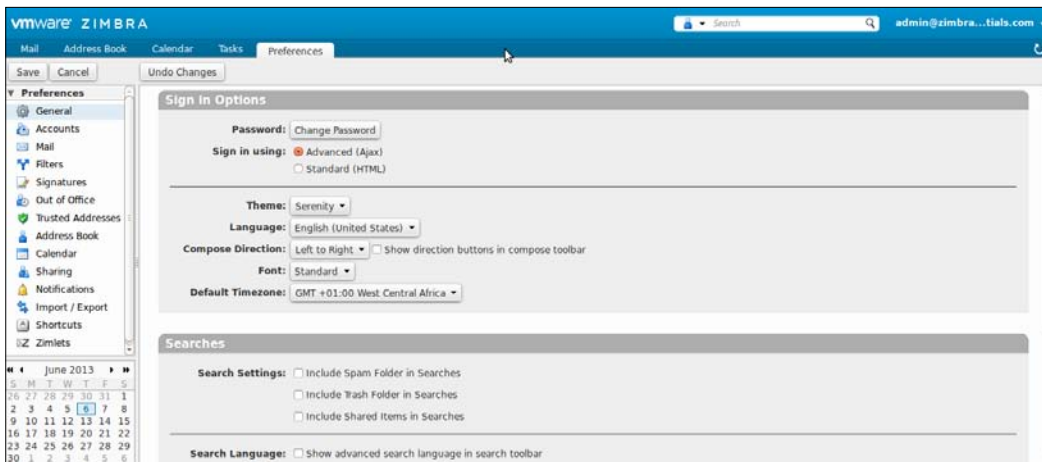


Customizing accounts

To customize an account via the management console, go to **Manage | Accounts**, select an account and start customization. There are a lot of submenus such as **Features, Preferences, Forwarding**, within which you can configure very useful functionalities such as creating an away message (auto-reply).



Of course, each user can customize his/her own account directly from the **Preferences** menu in his mailbox:



Summary

In this chapter, we saw how to manage the user account configuration inside Zimbra. We browsed different management tasks, and also saw how to customize the user account.

After finishing this chapter, you should have a Zimbra server that you can administrate easily. What you need now is to monitor that everything is going well. To do that, you need to use monitoring facilities and tools provided by Zimbra; we will develop this part in the next chapter.

6

Monitoring the Zimbra Server

This chapter serves as an IT guide for the Zimbra server.

The topics covered in this chapter are:

- Monitoring servers
- Monitoring mailbox quotas
- Monitoring authentication

By the end of this chapter, the user should be able to monitor the Zimbra server.

Prerequisites

The **Zimbra Logger** package includes different tools for syslog aggregation and reporting. Installing the Logger package is optional, but if you do not install it you cannot get server statistics and server status information.

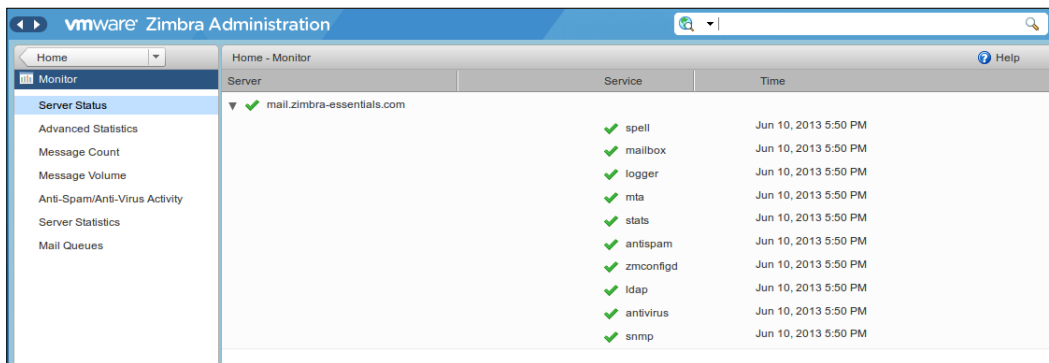
In Zimbra multiserver environments, Logger is enabled on only one mailbox server. This server is the monitor host. The Zimbra monitor host is responsible for checking the status of all the other ZCS servers and presenting this information on the Zimbra administration console. Real-time service status, MTA, spam, virus traffic, and performance statistics can be displayed. The Logger creates a daily report about mail activity, such as the number of messages, average delivery delay, and errors generated.

Monitoring servers

We can monitor Zimbra servers via CLI as well as the admin console. But with the admin console we can get more information with easy-to-understand graphical charts and a lot of facilities.

Review server status

Navigate to **Monitor | Server Status**, there you will get the page that lists all Zimbra servers and services, their status, and the last time when the server status was checked. The servers include your installed servers. In our case, in the single server installation we have only one server and in the multiserver installation we have two servers (one for LDAP and mailbox, and the other for MTA). The services include MTA, LDAP, mailbox, SNMP, antispam, antivirus, spellchecker, and Logger.



Server	Service	Time
mail.zimbra-essentials.com	spell	Jun 10, 2013 5:50 PM
mail.zimbra-essentials.com	mailbox	Jun 10, 2013 5:50 PM
mail.zimbra-essentials.com	logger	Jun 10, 2013 5:50 PM
mail.zimbra-essentials.com	mta	Jun 10, 2013 5:50 PM
mail.zimbra-essentials.com	stats	Jun 10, 2013 5:50 PM
mail.zimbra-essentials.com	antispam	Jun 10, 2013 5:50 PM
mail.zimbra-essentials.com	zmconfigd	Jun 10, 2013 5:50 PM
mail.zimbra-essentials.com	ldap	Jun 10, 2013 5:50 PM
mail.zimbra-essentials.com	antivirus	Jun 10, 2013 5:50 PM
mail.zimbra-essentials.com	snmp	Jun 10, 2013 5:50 PM

To start a non-running server, use the `zmcontrol` CLI command. You can also stop and start services via the administration console:

```
zimbra@mail:~$ zmcontrol
Release 8.0.3.GA.5664.UBUNTU12.64 UBUNTU12_64 FOSS edition.
/opt/zimbra/bin/zmcontrol [-v -h -H <host>] command [args]

-v:display version
-h:print usage statement
-H:Host name (localhost)
```

Command in:

```
restart                Restart services
shutdown              Stop services
start                 Start services
```

<code>startup</code>	<code>Start services</code>
<code>status</code>	<code>Display service status</code>
<code>stop</code>	<code>Stop services</code>

```
zimbra@mail:~$ zmcontrol status
Host mail.zimbra-essentials.com
antisppam           Running
antivirus           Running
ldap                Running
logger              Running
mailbox             Running
mta                  Running
snmp                 Running
spell               Running
stats               Running
zmconfigd           Running
zimbra@mail:~$
```

Enable or disable server services

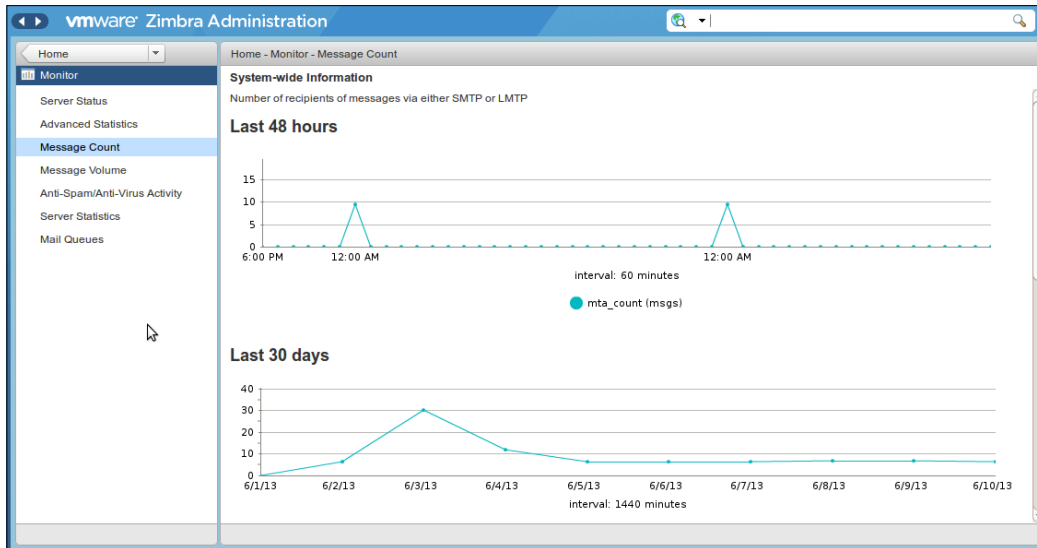
Server services are enabled or disabled by following steps:

1. Navigate to **Configure | Servers**.
2. Select **Services** in the navigation pane and select to enable or disable the services.

You can take a look at the screenshot in the *Managing server settings* section of *Chapter 4, Managing Configuration*.

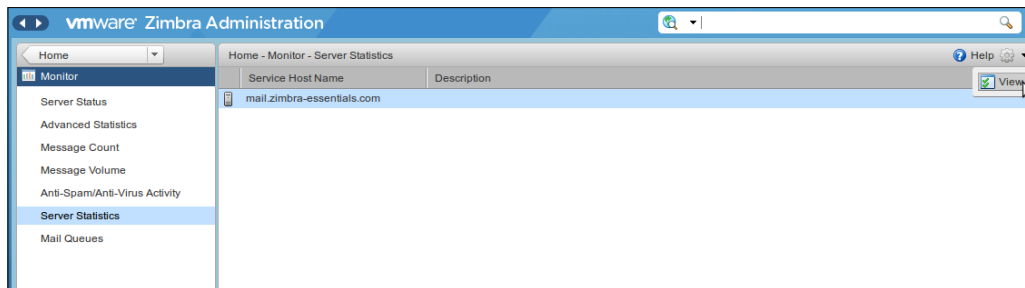
Server performance statistics

If you have installed the Logger package on a Zimbra mailbox server, you will get a lot of server statistics shown as bar graphs representing statistics of the message count, message volume, antispam, and antivirus activity. There is also a different chronological view of the information since it is displayed for the last 48 hours, 30 days, 60 days, and 365 days.

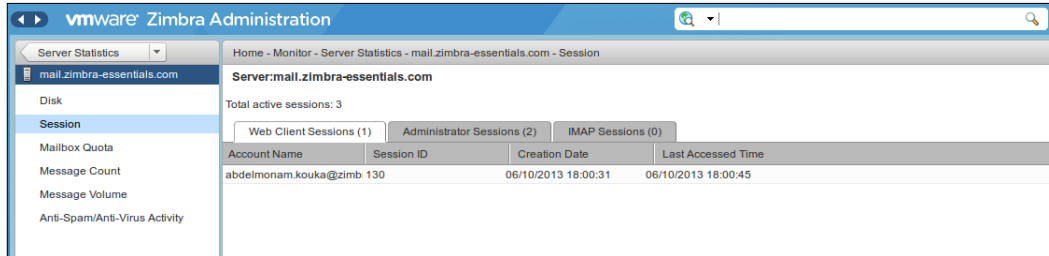


By selecting the **Message Count** tab or the **Message Volume** tab in the navigation pane, we will get merged statistics for all mailbox servers. But if you would like to get specific server information, you should go to the **Server Statistics** tab in the navigation pane and then select the server you require. Server-specific information also includes disk usage, session information, and mailbox quota details.

The following screenshot shows how to select a server to get its statistics:



And the following screenshot is a sample of one of these statistics (about sessions):

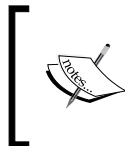


Configuring disk space notifications

A Zimbra administrator should regularly review his disk capacity and take preventative measures to maintain service when disks are getting full. An alert e-mail notification is sent to the administrator account when disk space is low. The default is to send a warning alert when the threshold reaches 85 percent and a critical alert when the threshold reaches 95 percent.

If you need to change these values, use `zmlocalconfig` to set the disk warning thresholds you want; the following are the parameters to which you should assign the value you want to perform this change:

Key	Parameter
Warning alerts key	<code>zmdisklog_warn_threshold</code>
Critical alerts key	<code>zmdisklog_critical_threshold</code>

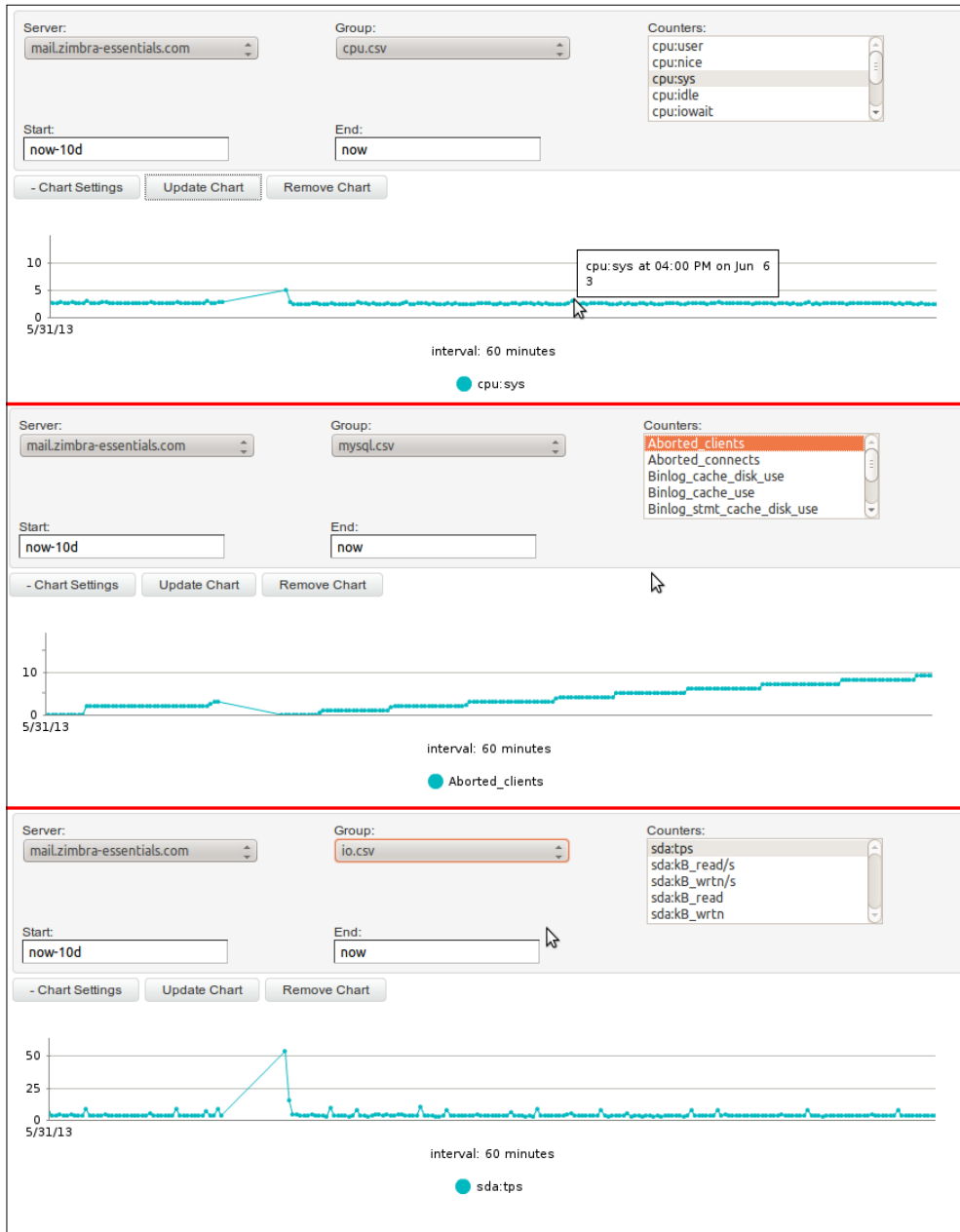


When you start services with the `zmcontrol` control, if the threshold is exceeded, you will get a warning displayed before the services are started. In this case, you should cleanup your disk to free up space to avoid service interruption.

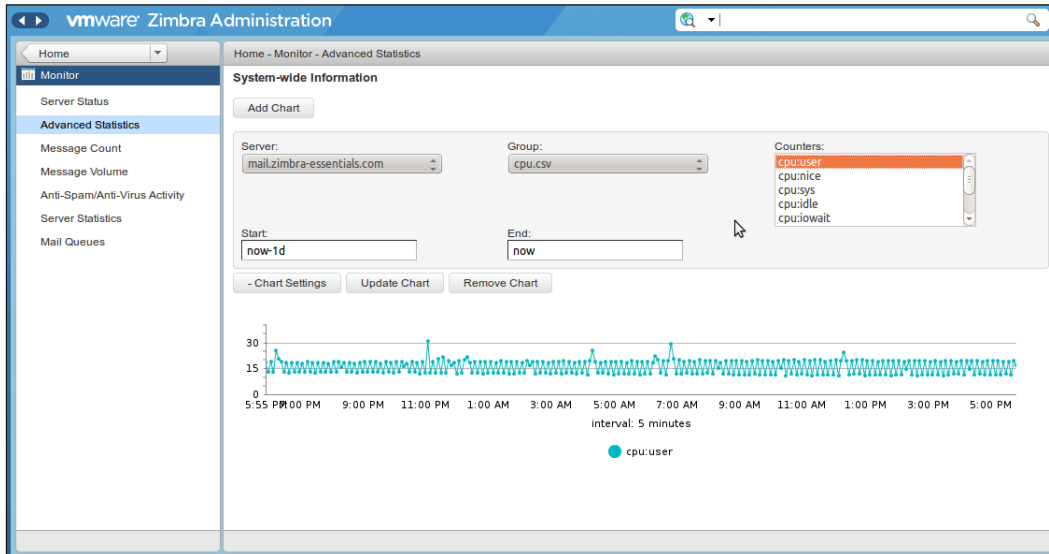
Monitoring servers

The Zimbra server collects many performance-related statistics that can help you to diagnose problems and load issues.

Go to **Monitor | Advanced Statistics**, there you will get the page that includes a lot of advanced and sophisticated graphing options that allow you to generate several charts based on statistical information for components such as CPU, IO, mailboxd, MTA queue, MySQL and others. The following screenshot gives some of the examples:



To chart the graphics in the **Advanced Statistics** tab, select one of these groups and then select from the list of specific counters for the type of information to display.



Information on counters covers a wide array of data grouped by themes is as follows:

- **cpu.csv:** This group contains counters to keep track of CPU usage (iowait time, idle time, system time, user time, and so on). This information can be tracked at both the server and process levels.
- **df.csv:** This group allows access to get disk usage information. Disk utilization (such as space used, percentage, and total space) is tracked for each disk partition.
- **fd.csv:** This is the file descriptor count. It captures file descriptor usage on the system. This is primarily used to track down "out-of-file descriptor" errors.
- **mailboxd.csv:** Zimbra server and **Java Virtual Machine (JVM)** statistics. This group contains counters of almost all of the mailboxd statistics.
- **mtaqueue.csv:** This measures the mail queue size in number of messages and the size in bytes.
- **proc.csv:** Zimbra processes statistics such as mailboxd/java, MySQL, and OpenLDAP.
- **soap.csv:** SOAP request processing time.
- **threads.csv:** Counts the number of JVM threads with a common name prefix.
- **vm.csv:** Shows Linux VM statistics.

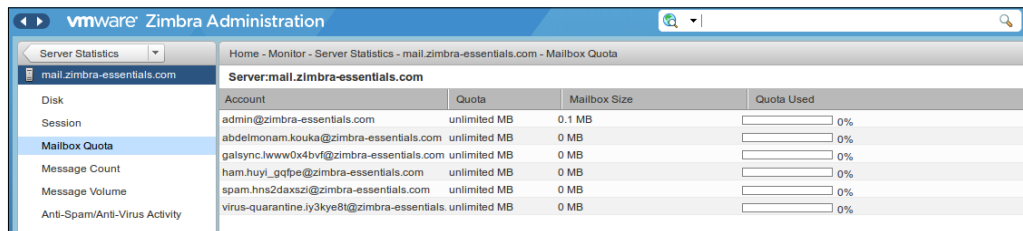
Monitoring mailbox quotas

A mailbox quota is a quota related to the user account and it applies to all account features from e-mail messages, to attachments, to calendar appointments, and tasks. The user should be careful about this value because when an account quota is reached all mail messages will be rejected. If this happens, the user can either delete some mails from his/her account to free some space so as to get below the quota limit (this action includes emptying the trash also), or can ask the administrator to increase his/her quota.

View quotas

Zimbra gives the administrator the option of checking mailbox quotas for individual accounts from the **Server Statistics** tab on the administration console. From the **Mailbox Quota** tab, you get an instant view of the following information for each account with the help of following steps:

1. On the administrator console, go to **Monitor | Server Statistics**.
2. Select the server for which you want to view statistics.
3. In the navigation pane, select the **Mailbox Quota** tab. The **Mailbox Quota** page displays the following information:
 - The **Quota** column announces the value of the mailbox quota allocated to the account. We can configure this value either in the COS or individually by account. If this value is 0, then it means unlimited quota.
 - The **Mailbox Size** column displays the used disk space.
 - The **Quota Used** column displays the used quota percentage.

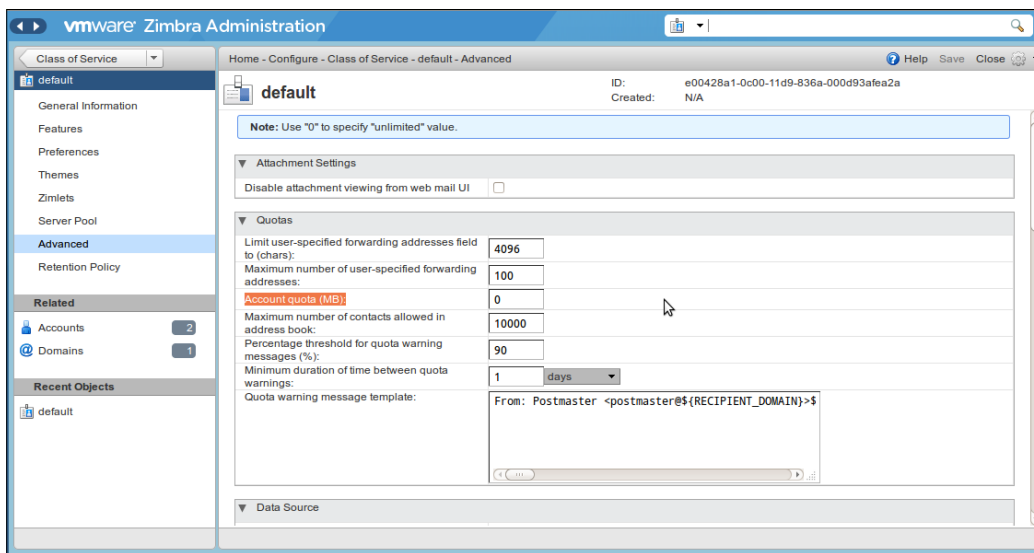


Account	Quota	Mailbox Size	Quota Used
admin@zimbra-essentials.com	unlimited MB	0.1 MB	<input type="text"/> 0%
abdelmonam.kouka@zimbra-essentials.com	unlimited MB	0 MB	<input type="text"/> 0%
galsync.lwww0x4bv6@zimbra-essentials.com	unlimited MB	0 MB	<input type="text"/> 0%
ham.huyl_gqfpe@zimbra-essentials.com	unlimited MB	0 MB	<input type="text"/> 0%
spam.hns2daxsz@zimbra-essentials.com	unlimited MB	0 MB	<input type="text"/> 0%
virus-quarantine.iy3kye8@zimbra-essentials.com	unlimited MB	0 MB	<input type="text"/> 0%

Increase or decrease quotas

We can configure a quota threshold either from a COS or from an account. When this quota is reached, the server sends a warning message to the user alerting him that he is about to reach his mailbox quota. The following steps show how to configure a quota threshold from the default COS:

1. On the administrator console, go to **Configure | Class of Service | default | Advanced**. Scroll down to the **Quotas** section.
2. Modify the quota settings. 0 means unlimited quota.
3. Click on the **Save** button.



Monitoring authentication

This section explains of how to monitor the authentication process in Zimbra. It covers monitoring authentication failures and viewing logfiles.

Monitoring authentication failures

This is a security mechanism that allows protection against dictionary-based and distributed attacks; to take advantage of it you should configure the `zmauditwatch` script. By looking at where the authentication failures are coming from and the frequency at which they are happening, this script tries to detect the most advanced attacks, for all accounts on a Zimbra mailbox server.

There are many types of authentication failures checked, such as:

- **IP/Account hash check:** It sends an alert e-mail if X authentication failures occur from a unique IP/account combination during Y period. The default values are 10 for X and 60 seconds for Y.
- **Account check:** This check is similar to the previous one; the difference is that it checks authentication failures from any IP address. The default values here are 15 for X and 60 seconds for Y. This check attempts to detect a distributed hijack-based attack on a single account.
- **IP check:** This check deals with authentication failures that occur to any account. The default values here are 20 for X and 60 seconds for Y. This check attempts to detect a single host-based attack across multiple accounts.
- **Total authentication failure check:** The default is to send an e-mail alert if 1,000 authentication failures occur from any IP address to any account within 60 seconds. The default should be modified to be 1 percent of the active accounts on the mailbox server.

To change the default values that trigger an e-mail alert, use the `zmlocalconfig` command with the following parameters:

- `zimbra_swatch_ipacct_threshold`: This allows you to change the IP/Account value
- `zimbra_swatch_acct_threshold`: This allows you to change the account check value
- `zimbra_swatch_ip_threshold`: This allows you to change the IP check value
- `zimbra_swatch_total_threshold`: This allows you to change the total authentication failure check value

And to finish, we should configure a mail address that should receive these alerts. We do that via `zmlocalconfig` and also with the `zimbra_swatch_notice_user` parameter.

The following is an example of how to configure these parameters:

```
zmlocalconfig -e zimbra_swatch_notice_user=admin@zimbra-essentials.com
```

Viewing logfiles

Zimbra has a dual logging system: it logs the list of its activities and errors at the same time through the system `syslog` daemon as well as Zimbra-specific logs on the local file system. In case of analysis and troubleshooting, these logs are used first of all.

Zimbra puts its local logs in the `/opt/zimbra/log` directory; it contains the following files:

- `audit.log`: This logfile contains authentication activities of both the users and administrators. It also records admin activity order aim to track configuration modifications.
- `clamd.log`: This logfile registers the antivirus daemon `clamd` activity.
- `freshclam.log`: This logfile contains information collected during the `clamd` virus definition's updating process.
- `mailbox.log`: This is a special log: it is a `mailboxd log4j` server log that contains the mailbox server logs. It includes the mailbox store, LMTP server, IMAP and POP servers, and the Index server.
- `myslow.log`: As its name suggests, this log tracks all SQL statements from the mailbox server that took more than `long_query_time` seconds to execute. Note that the `long_query_time` parameter is defined in `/opt/zimbra/my.cnf`.
- `spamtrain.log`: This logfile contains the `zmtrainsa` output during regularly scheduled executions from the cron.
- `sync.log`: This logfile contains information related to Zimbra mobile synchronisation operations.

We can also find other logs such as:

- `/opt/zimbra/jetty/logs/`: This is where Jetty-specific activity is logged.
- `/opt/zimbra/db/data.<hostname>.err`: This is the message store database error log.
- `/opt/zimbra/logger/db/data.<hostname>.err`: This is the Logger database error log.

As we saw, Zimbra activity is logged to System `syslog` also and the related logfile is `/var/log/zimbra.log`. The Zimbra `syslog` details the activities of the Zimbra MTA (Postfix, `amavisd`, `antispam`, `antivirus`), Logger, Authentication (`cyrussasl`), and Directory (OpenLDAP). By default, LDAP activity is logged to the `zimbra.log` file.

Summary

In this chapter, we learned how to monitor a Zimbra server with the aim of keeping it secure and reliable. We saw in detail how to monitor servers, mailbox quotas, and authentication.

Index

A

- aliases, user accounts**
 - creating 101
- Anti-Spam SMTP Proxy (ASSP)**
 - about 75
 - installing 75
 - using, with Zimbra 75, 76
- authentication**
 - failures, monitoring 115
 - logfiles, viewing 117
 - monitoring 115
- authentication failures**
 - account check 116
 - IP/Account hash check 116
 - IP check 116
 - total authentication failure check 116
 - types 116

B

- Barracuda spam and virus firewall 83**

C

- Certificate Signing Request (CSR) 96**
- ClamAV**
 - existing release, backing up 72
 - updating 72-75
- configuration management**
 - global configuration management 87
- COS 91**

D

- DeMilitarized Zone (DMZ) 7**
- Distributed Checksum Clearinghouses (DCC)**
 - about 83
 - enabling 83
 - setting up 83
- distribution lists, user accounts**
 - creating 102
- DNAT 7**
- DNS configuration, Zimbra**
 - performing 10-16
- DNS configuration, Zimbra multiserver installation**
 - performing 37-44
- DSPAM**
 - enabling 70, 71

E

- external solutions, security system**
 - about 83
 - Barracuda spam and virus firewall 83
 - IronPort 85
 - Maia Mailguard 85
 - MailCleaner 84
 - Untangle 86

G

- Global Address List (GAL)** 76
- global configuration management**
 - about 87
 - attachment settings 89
 - COS 91, 92
 - general global settings 89
 - global MTA settings 90
 - IMAP and POP settings 91
 - settings 88
- global e-mail attachment settings** 89
- global MTA settings**
 - configuring 90

I

- IMAP or POP settings**
 - configuring 91
- installation**
 - Zimbra 17
- internal solutions, security system**
 - ASSP, using 75
 - ClamAV, updating 72
 - DSPAM, enabling 70, 71
 - SpamAssassin, improving 77
- IronPort**
 - about 85
 - capabilities 85
 - features 85

J

- Java Virtual Machine (JVM) statistics** 113

L

- LDAP master server**
 - installing 49-57
- log files**
 - audit.log 117
 - clamd.log 117
 - freshclam.log 117
 - mailbox.log 117
 - myslow.log 117
 - spamtrain.log 117
 - sync.log 117

M

- Maia Mailguard** 85
- mailbox quotas**
 - decreasing 115
 - increasing 115
 - monitoring 114
 - viewing 114
- MailCleaner**
 - about 84
 - advantages 84
 - features 85
- multiserver configuration options**
 - large configuration 34
 - medium configuration 34
 - small configuration 34
 - very large configuration 34

P

- package installation, Zimbra multiserver installation**
 - performing 48
 - Zimbra Master LDAP server, installing 49-57
 - Zimbra MTA, installing 57-63
- post installation, Zimbra multiserver installation**
 - performing 64
 - server statistics display, enabling 65
 - ssh keys, setting up 64
- prerequisites, Zimbra**
 - about 5
 - assumptions 6
 - DNS configuration 10-15
 - environment, preparing 6
 - OS, preparing 9
 - system requisites 7
 - Ubuntu server installation 7-9
- prerequisites, Zimbra multiserver installation** 33
- Pyzor**
 - about 81
 - configuring 81
 - installing 81

R

Razor2

- about 80
- configuring 80
- installing 80

resources, user accounts

- creating 103

S

salocal.cf.in file

- about 77
- basic rules 77
- blacklist, adding 77
- meta rules 79
- whitelist, adding 77

security system, Zimbra

- external solutions 83
- internal solutions 70
- issues 69
- solutions 70

Sender policy framework (SPF) 79

servers

- disk space notifications, configuring 111
- monitoring 107, 111, 113
- review server status 108
- server performance statistics 110
- server services, disabling 109
- server services, enabling 109

server settings

- general information page 92
- IMAP/POP 94
- managing 92
- MTA 94
- services 93

SpamAssassin

- configuring 81, 82
- DCC, adding 83
- improving 77
- Pyzor 81
- Razor2 80
- salocal.cf.in 77
- Sender Policy Framework (SPF) 79

SSL certificates

- installed certificates, checking 96
- installing 96, 97
- managing 95

U

Ubuntu server

- preparing, for Zimbra 9

Ubuntu server installation

- about 7, 8
- steps 8

Ubuntu server installation, Zimbra multiserver installation

- performing 36

Untangle

- about 86
- Lite package 86
- Premium package 86
- Standard package 86

user accounts

- aliases, creating 101
- creating 100, 101
- customizing 104
- distribution lists, creating 102
- managing 99, 100
- resources, creating 103

V

vi Editor

- about 6
- URL, for basic training 6

Z

Zimbra

- authentication, monitoring 115
- configuration management 87
- downloading 17
- mailbox quotas, monitoring 114
- prerequisites 5, 107
- running 28-31
- security 69
- servers, monitoring 107
- user accounts, customizing 104
- user accounts, managing 99, 100

Zimbra installation

- installation step 18
- performing 18-25
- preinstallation 17
- steps 17

Zimbra Logger package 107

Zimbra MTA

installing 57-64

Zimbra multiserver installation

assumptions 35

DNS configuration 37-44

environment, preparing 34

multiserver configuration examples 34

network configuration, on MTA

server 44, 45

package installation 48

post installation 64

prerequisites 33

running 65-67

servers, syncing 46, 47

system requisites 36

Ubuntu, preparing 37

Ubuntu server installation 36

zmcontrol CLI command 108

zmlocalconfig command

parameters 116

zmmtaconfig command 71



**Thank you for buying
Learning Zimbra Server Essentials**

About Packt Publishing

Packt, pronounced 'packed', published its first book "*Mastering phpMyAdmin for Effective MySQL Management*" in April 2004 and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

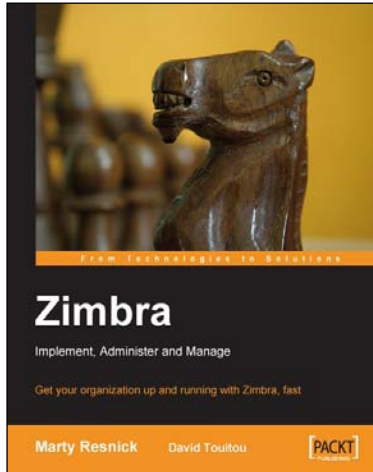
Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern, yet unique publishing company, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: www.packtpub.com.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to author@packtpub.com. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.

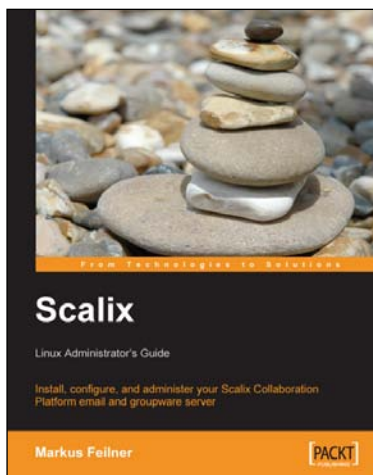


Zimbra: Implement, Administer and Manage

ISBN: 978-1-847192-08-0 Paperback: 220 pages

Get your organization up and running with Zimbra, fast

1. Get your organization up and running with Zimbra, fast
2. Administer the Zimbra server and work with the Zimbra web client
3. Protect your Zimbra installation from hackers, spammers, and viruses



Scalix: Linux Administrator's Guide

ISBN: 978-1-847192-76-9 Paperback: 276 pages

Install, configure, and administer your Scalix Collaboration Platform email and groupware server

1. Install, upgrade, and configure Scalix
2. Build a robust and reliable system
3. Detailed walkthroughs and expert advice on best practices

Please check www.PacktPub.com for information on our titles

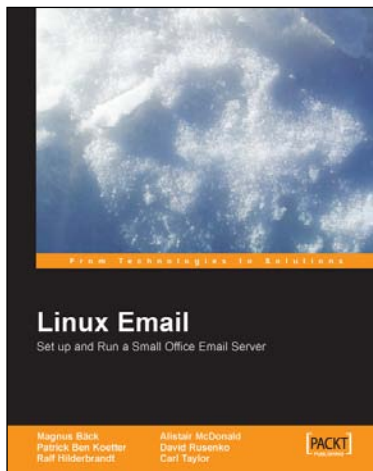


Qmail Quickstarter: Install, Set Up and Run your own Email Server

ISBN: 978-1-847191-15-1 Paperback: 152 pages

A fast-paced and easy-to-follow, step-by-step guide that gets you up and running quickly

1. Qmail Basics
2. Storing and retrieving of emails
3. Virtualisation
4. Hosting Multiple Domains, Encryption, and Mailing Lists



Linux Email: Set up and Run a Small Office Email Server

ISBN: 978-1-904811-37-4 Paperback: 316 pages

Your step-by-step guide to using free open source email in small businesses

1. All the information you need to easily set up your own Linux email server
2. Shows how to provide web access to email, virus and spam protection, and more
3. Techniques to backup and protect your data

Please check www.PacktPub.com for information on our titles