



Zimbra™ Collaboration Suite Multi-Server Installation Guide

**ZCS 4.0
Network Edition
August 2006**

Copyright Zimbra, Inc. 2006. All rights reserved. Zimbra and the Zimbra logo are trademarks of Zimbra, Inc.

No part of this document may be reproduced, in whole or in part, without the express written permission of Zimbra Inc.

Trademark and Licensing

MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Postfix is copyright © 1999 International Business Machines Corporation and others and it was created by Wietse Venema <wietse@porcupine.org>.

SpamAssassin is a trademark of Deersoft, Inc.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

All other marks are the property of their respective owners.

Building Better Products within the Open Source Community

Zimbra Collaboration Suite leverages many great technologies from the open source community: MySQL, OpenLDAP, Postfix, SpamAssassin, and Apache. Zimbra believes that great products come from contributing to and leveraging open source technologies. We are thankful for the great contributions that led to the creation of MySQL, OpenLDAP, Postfix, SpamAssassin, and Apache software.

Zimbra, Inc.
1500 Fashion Island Boulevard, Suite 100
San Mateo, California 94404 USA
650. 212.0505
www.zimbra.com

Revised September 2006

Table of Content

Chapter 1 Introduction	5
Audience	5
Zimbra Collaboration Suite License	5
For More Information	5
Support and Contact Information	6
Chapter 2 Preparing Your Server Environment	7
System Requirements	7
Installation Modifications for Red Hat Enterprise Linux	8
Installation Modification for Mac Servers	10
DNS Configuration Requirement	10
Chapter 3 Planning for the Installation	11
Zimbra Packages	11
Configuration Examples	12
Downloading the Zimbra Software	12
Zimbra License	13
Menu-Driven Configuration	13
Configuring IMAP and POP Proxy Server	17
Configuring for Virtual Hosting	18
Load Balancing on ZCS	18
Chapter 4 Multiple-Server Installation	21
Starting the Installation Process	21
Starting the Installation Process on the Mac Server	23
Installing Zimbra LDAP Master Server	24
Installing Zimbra Mailbox Server	26
Installing Zimbra MTA on a Server	29
Installing the Zimbra-SNMP package	31
Final Set-Up	31
Verifying Server Configuration	32
Post Installation Tasks	32
Logging on to the Administration Console	33
Defining Classes of Service	33
Provisioning Accounts	33
Uninstalling Zimbra Collaboration Suite	34
Chapter 5 LDAP Replication Installation	35
Installing Zimbra LDAP Master Server	35
Installing a LDAP Replica Server	37
Setting Up Zimbra LDAP Servers for Replication	39

Configuring Zimbra Servers to use LDAP Replica 40

**Chapter 6 Zimbra Cluster Installation - Multi-Node Configuration
For Red Hat Cluster Suite Integration . . . 41**

Pre-configuration Requirements 41

 Hardware for the Cluster Environment 41

 Software Requirements For Clustering 41

Preparing the SAN 42

Overview of Cluster Installation 42

 Cluster Scenario 43

Installing and Configuring the Software 43

 Install the Active Mailbox Nodes 43

 Mounting Volumes for Cluster Service 48

 Running Zimbra Cluster Post Install Script 48

 Configuring the Standby Mailbox Server Node 51

 Running the Cluster Post Install Script 54

Modify Zimbra LDAP and Zimbra MTA Servers for Logger Service 55

Configuring Red Hat Cluster for Zimbra Collaboration Suite 55

Start the Red Hat Cluster Suite Daemons 61

Testing the Cluster Set up 63

View Zimbra Cluster Status 63

System Requirements for Zimbra Collaboration Suite 4.0

Index 7

Chapter 1 Introduction

Information in this guide is intended for persons responsible for installing the Zimbra Collaboration Suite. This guide will help you plan and perform all installation procedures necessary to deploy a fully functioning email system based on Zimbra's messaging technology.

This guide covers the installation of Zimbra Collaboration Suite Network Edition 4.0.x.

Audience

This installation guide assumes you have a thorough understanding of system administration concepts and tasks and are familiar with email communication standards, security concepts, directory services, and database management.

Zimbra Collaboration Suite License

A Zimbra license is required in order to create accounts in the Network Edition Zimbra Collaboration Suite servers. You can install ZCS without a license but only one account, the administrator account, can be created.

The license types available are

- **Trial.** You can obtain the trial license from the Zimbra license portal for free. The trial license allows you to create up to 50 users. It expires in 60 days.
- **Regular.** You must purchase the Zimbra Regular license. This license is valid for a specific Zimbra Collaboration Suite system and is encrypted with the number of Zimbra accounts (seats) you have purchased, the effective date and expiration date of the regular license.

If do not have a license, go to Zimbra's website to obtain a license from the Network Downloads area.

For More Information

Zimbra documentation, including a readme text file, release notes, the administration guide, and other Zimbra guides are copied to the servers during the installation. They are also available from www.zimbra.com and from the administration console.

- **Administrator's Guide.** This guide describes product architecture, server functionality, administration tasks, configuration options, and backup and restore procedures. The guide is available in pdf format from the administrator's console.
- **Administrator Help.** The administrator Help provides instructions about how to add and maintain your servers, domains, and user accounts from the admin console.
- **Web Client Help.** The Web Client Help provides instructions about how to use the Zimbra Web Client features.
- **Migration Wizard Guide.** This guide describes how to migrate Microsoft® Exchange users to the Zimbra Collaboration Suite.
- **Clustering Guide.** This guide describes how to setup clustering for either a single server, multiple servers, or an LDAP server.

Support and Contact Information

Visit www.zimbra.com to join the community and to be a part of building the best open source messaging solution. We appreciate your feedback and suggestions.

- Contact sales@zimbra.com to purchase Zimbra Collaboration Suite
- Network Edition customers can contact support at support@zimbra.com
- Explore the Zimbra Forums for answers to installation or configurations problems
- Join the [Zimbra Community Forum](#), to participate and learn more about the Zimbra Collaboration Suite.
- Send an email to feedback@zimbra.com to let us know what you like about the product and what you would like to see in the product. Or, if you prefer, post your ideas to the Zimbra Forum.

If you encounter problems with this software, visit Zimbra.com and submit a bug report. Make sure you provide enough detail so that the bug can be easily duplicated.

Chapter 2 Preparing Your Server Environment

In order to successfully install and run Zimbra Collaboration Suite, ensure your system meets the requirements described in this section. This section includes:

- System requirements
- Operating system modifications
- DNS Configuration requirements

Important: Do not manually create the user 'zimbra' before running the ZCS installation. The installation automatically creates this user and sets up its environment.

System Requirements

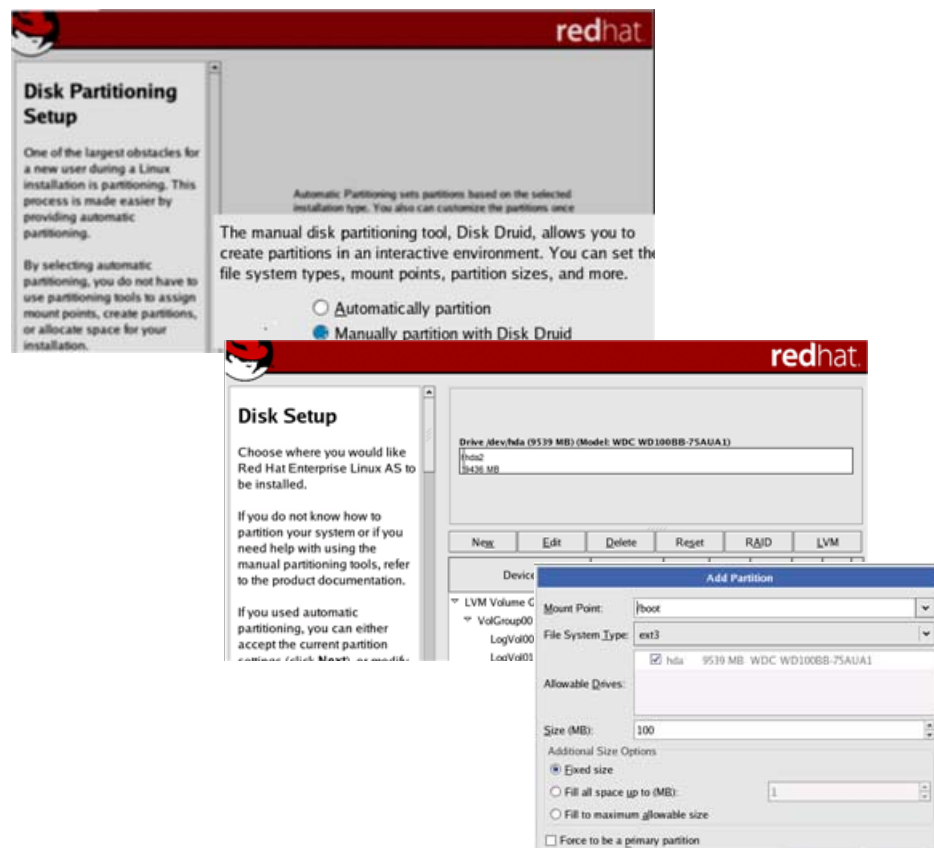
For the ZCS system requirements see [System Requirements for Zimbra Collaboration Suite 4.0](#)

Installation Modifications for Red Hat Enterprise Linux

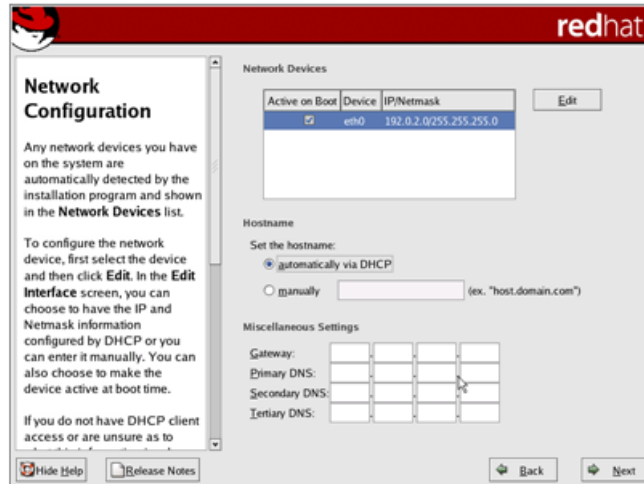
The Zimbra Collaboration Suite runs on the Red Hat Enterprise Linux, 4 operating system. When you install the Red Hat software for the Zimbra Collaboration Suite, you should accept the default setup answers to install the minimum configuration, except the following steps must be modified.

Refer to the Red Hat Enterprise Linux installation guide for detailed documentation about installing their software.

- **Disk Partitioning Setup.** Check **Manually partition with DiskDruid**. The disk partition should be set up as follows:
 - The **Mount Point/RAID Volume** size for the **/boot** partition should be 100 MB.
 - The **Swap** partition should be set to twice the size of the RAM on your machine.
 - The **Root** partition (/) should be set with the remaining disk space size.



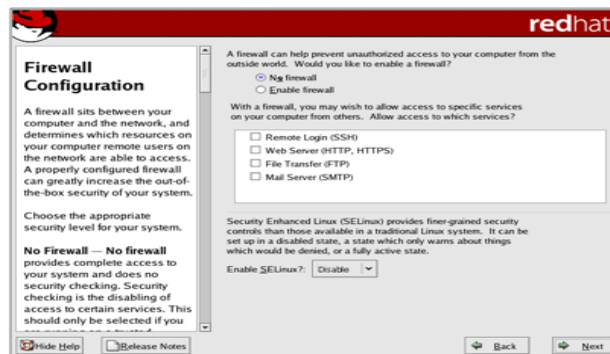
- **Network Configuration>Network Devices>Hostname** should be configured manually with the hostname [*mailhost.example.com*] of the Zimbra server.



- Enter the **Gateway** and **Primary DNS** addresses.
- In the **Edit Interface** pop-up screen, check **Activate on Boot**. Enter the **IP Address** and **Netmask** of the device. This allows the interface to start when you boot.



- **Firewall Configuration** should be set to **No firewall**, and the **Security Enhanced Linux (SELinux)** should be disabled.



Important: The following should also be considered before you install the Zimbra Collaboration Suite.

- You must disable Sendmail in order to run the Zimbra Collaboration Suite. Disable the Sendmail service with these commands, **chkconfig sendmail off, service sendmail stop**.
- A fully qualified domain name is required. Make sure that the FQDN entry in `/etc/hosts` appear before the hostnames. If this is missing, the creation of the Zimbra certificate fails. The FQDN entry should look like this example.

127.0.0.1	localhost.localdomain localhost
your.ip.address	FQDN yourhostname

Installation Modification for Mac Servers

No modifications are required to the MAC server operating system, but Java 1.5 should be set as the default Java.

To set Java 1.5 as the default:

- **su - root**
- **cd /System/Library/Frameworks/JavaVM.Framework/Versions**
- **rm CurrentJDK**
- **ln -s 1.5.0 CurrentJDK**

DNS Configuration Requirement

In order to send and receive email, the Zimbra MTA must be configured in DNS with both A and MX records. For sending mail, the MTA uses DNS to resolve hostnames and email-routing information. To receive mail the MX record must be configured correctly to route the message to the mail server.

During the installation process ZCS checks to see if you have an MX record correctly configured. If it is not, an error is displayed suggesting that the domain name have an MX record configured in DNS.

You must configure a relay host if you do not enable DNS. After ZCS is installed, go to the **Global Settings>MTA** tab on the administration console and uncheck **Enable DNS lookups**. Enter the relay MTA address to use for external delivery.

Note: Even if a relay host is configured, an MX record is still required if the ZCS server is going to receive email from the internet.

Chapter 3 Planning for the Installation

This chapter describes the components that are installed and reviews the configuration options that can be made when you install the Zimbra Collaboration Suite.

Zimbra Packages

Zimbra architecture includes open-source integrations using industry standard protocols. The third-party software has been tested and configured to work with the Zimbra software. The following describes the Zimbra packages that are installed.

- **Zimbra Core.** This package includes the libraries, utilities, monitoring tools, and basic configuration files. Zimbra Core is automatically installed on each server.
- **Zimbra LDAP.** User authentication is provided through OpenLDAP® software. Each account on the Zimbra server has a unique mailbox ID that is the primary point of reference to identify the account. The OpenLDAP schema has been customized for the Zimbra Collaboration Suite. The Zimbra LDAP server must be configured before the other servers. You can set up LDAP replication, configuring a master LDAP server and replica LDAP servers.
- **Zimbra MTA.** Postfix is the open source mail transfer agent (MTA) that receives email via SMTP and routes each message to the appropriate Zimbra mailbox server using Local Mail Transfer Protocol (LMTP). The Zimbra MTA also includes the anti-virus and anti-spam components.
- **Zimbra Store.** The Zimbra store includes the components for the mailbox server, including Apache Tomcat, which is the servlet container the Zimbra software runs within. The Zimbra mailbox server includes the following components:
 - **Data store.** The data store is a MySQL® database.
 - **Message store.** The message store is where all email messages and file attachments reside.
 - **Index store.** Index and search technology is provided through Lucene. Index files are maintained for each mailbox.

- **Zimbra SNMP.** Installing the Zimbra SNMP package is optional. If you choose to install Zimbra-SNMP for monitoring, this package should be installed on every Zimbra server.
- **Zimbra Logger.** Installing the Zimbra Logger package is optional*. If you install the Logger package, it must be installed on the first mailbox server. The Zimbra logger installs tools for syslog aggregation, reporting, and message tracing. If you do not install Logger, you cannot use the message trace feature. In addition, the server statistics are not captured, and the server statistics section of the administration console will not display.
*The Logger package must be installed at the same time as the mailbox server.
- **Zimbra Spell.** Installing the Zimbra Spell package is optional. Aspell is the open source spell checker used on the Zimbra Web Client. When Zimbra-spell is installed, the Zimbra-apache package is also installed.

The Zimbra server configuration is menu driven. The installation menu displays the default configuration values. The menu displays the logical host name and email domain name [example.com] as configured for the computer.

Configuration Examples

Zimbra Collaboration Suite can be easily scaled for any size of email environment, from very small businesses with fewer than 25 email accounts to large businesses with thousands of email accounts. The following table shows examples of different configuration options.

Table 1 Zimbra Collaboration Suite Configuration Options

Small	Medium	Large	Very Large
All ZCS components installed on one server. See the Zimbra Installation Quick Start for installation instructions.	<ul style="list-style-type: none"> • Zimbra LDAP and Zimbra message store on one server • Zimbra MTA on a separate server. • Possibly include additional Zimbra MTA servers configured 	<ul style="list-style-type: none"> • Zimbra LDAP on one server • Multiple Zimbra mailbox servers • Multiple Zimbra MTA servers 	<ul style="list-style-type: none"> • Zimbra LDAP server as master • LDAP replicas • Multiple Zimbra mailbox servers • Multiple Zimbra MTA servers

Downloading the Zimbra Software

For the latest Zimbra software download, go to [www. Zimbra.com](http://www.Zimbra.com). Save the Zimbra Collaboration Suite download file to the computer from which you will install the software.

When the Zimbra Collaboration Suite is installed, the following Zimbra applications are saved to the Zimbra server:

- **Zimbra Collaboration Suite Connector for Outlook®** .msi file. This is a MAPI service provider that is installed on users' computers.
- **Zimbra Collaboration Suite Migration Wizard for Exchange** .exe file to migrate Microsoft® Exchange server email accounts to the Zimbra server.
- **Zimbra Collaboration Suite Import Wizard for Outlook** .exe file to allow users to import their Outlook .pst files to the Zimbra server.
- ZCS documents, including administrator's guide, installation guides, Migration Wizard guide, and release notes.

See the Administrator's Guide for information about the ZCS Connector for Outlook and the ZCS Import Wizard. See the Migration Wizard Guide for information about the Migration Wizard file.

Zimbra License

A Zimbra license is required in order to create accounts. See "Zimbra Collaboration Suite License" on page 5 for a description of the license types.

The regular license can only be installed on the ZCS system for which it is purchased. Only one Zimbra license is required for your Zimbra Collaboration Suite environment. This license is installed on the Zimbra LDAP server.

When you purchase, renew, or change the Zimbra license, you must update the Zimbra server with the new license information. Use the **Update License Wizard** from the administration console's Global Settings to upload and install a new license and to update an existing license, or you can install or update the license using the **zmlicense** CLI command. See the Administration Guide, Appendix A, CLI Commands, "zmlicense" on page 142 to use the CLI command.

Current license information, including the number of accounts purchased, the number of accounts used, and the expiration date, can be viewed from the Global Settings in the administration console.

Menu-Driven Configuration

The menu driven installation displays the components and their existing default values. During the installation process you can modify the default values. Only those menu options associated with the package being installed are displayed.

The table below describes the Main menu options.

Table 2 Main Menu Options

Server Configured	Main Menu	Description
All	Hostname	The host name configured in the operating system installation
All	LDAP master host	The LDAP master host name. This LDAP host name is configured on every server.
All	LDAP port	The default port is 389.
All	LDAP password	The root LDAP password for the host. This LDAP password is configured on every server.
ZimbraLDAP Server	zimbra-ldap	Configuration includes the following: <ul style="list-style-type: none"> • Create Domain - Yes. You can create one domain during installation and additional domains can be created from the administration console. • Domain to create - The default domain is the fully qualified hostname of the server. If you created a valid mail domain on your DNS server, enter it n
Zimbra Mailbox Server	zimbra-store	Configuration includes the following. <ul style="list-style-type: none"> • Create Admin User - The administrator account is created during installation. This account is the first account provisioned on the Zimbra server and allows you to log on to the administration console. • Admin user to create - The default is admin@[mailhost.example.com]. • Admin Password - You must set the admin account password. The password is case sensitive and must be a minimum of six characters. The administrator name, mail address, and password are required to log in to the administration console.

Table 2 Main Menu Options

Server Configured	Main Menu	Description
Zimbra Mailbox Server	zimbra-store	<ul style="list-style-type: none"> • By default, the automated spam training filter is enabled and two mail accounts are created. <p><i>Spam Training User</i> to receive mail notification about mail that was not marked as junk, but should be.</p> <p><i>Non-spam (HAM) training user</i> to receive mail notification about mail that was marked as junk, but should not have been.</p> <p>These addresses are automatically configured to work with the spam training filter. The accounts created have a randomly selected name. To recognize what the account is used for you may want to change this name.</p> <p>The spam training filter is automatically added to the cron table and runs daily.</p> <p>These default port configurations are shown.</p> <ul style="list-style-type: none"> • SMTP host • Web server HTTP port: - 80 • Web server HTTPS port: - 443 • Web server mode - Can be http, https, mixed. Mixed mode uses HTTPS for logging in and HTTP for normal session traffic. All modes use SSL encryption for back-end administrative traffic. Note: selecting both will set it to mixed. • Enable POP/IMAP proxy, default No. See “Configuring IMAP and POP Proxy Server” on page 17. • IMAP server port: 143 • IMAP server SSL port: 993 • POP server port: 110 • POP server SSL port: 995 • Use spell checker server: yes (if installed) • Spell server URL: http://<example.com>:7780/aspell.php

Table 2 Main Menu Options

Server Configured	Main Menu	Description
Zimbra MTA Server	zimbra-mta	<p>The following options can be modified.</p> <ul style="list-style-type: none"> • MTA Auth host. This is configured automatically if the MTA authentication server host is on the same server, but must be configured if the authentication server is not on the MTA. The MTA Auth host must be one of the mailbox servers. • Enable Spamassassin. Default is enabled. • Enable ClamAV. Default is enabled. • Notification address for AV alerts. Sets the notification address for AV alerts. You can either accept the default or create a new address. If you create a new address, remember to provision this address from the admin console. Note: If the virus notification address does not exist and your host name is the same as the domain name on the Zimbra server, the virus notifications queue in the Zimbra MTA server and cannot be delivered. •
All servers, if installed	zimbra-snmpp Installing SNMP is optional, but if installed it must be on all servers.	<p>You can modify the following options</p> <ul style="list-style-type: none"> • Enable SNMP notifications. The default is No. If you enter yes, you must enter the SNMP Trap hostname. • SNMP Trap hostname • Enable SMTP notification - The default is No. • SMTP Source email address - If you enter yes for SMTP notification, you must enter the SMTP source email address and SMTP Destination email address - destination email address.

Table 2 Main Menu Options

Server Configured	Main Menu	Description
Installed on one mailbox server	zimbra-logger	If installed, it is automatically enabled. Logs from all the hosts are sent to the mailbox server where the logger package is installed. This data is used to generate the statistics graphs and is used for message tracing, and reporting.
	zimbra-spell	If installed, it is automatically enabled. When composing messages in the Zimbra Web Client, spell check can be run.
	Enable default backup schedule	Default is yes. Sets the schedule for Backup session to run as a full backup every Sunday at 1 a.m. and as incremental on the other days at 1 a.m.
	r) Start servers after configuration	When the installation and configuration is complete, if this is set to Yes, the Zimbra server is automatically started.
	s) Save config to file	At any time during the installation, you can save the configuration to a file.
	q) Quit	Quit can be used at any time to quit the installation.

Configuring IMAP and POP Proxy Server

Use of an IMAP/POP proxy server allows mail retrieval for a domain to be split across multiple Zimbra servers on a per user basis.

When ZCS is installed on a Zimbra server, the IMAP/POP Proxy server feature can be enabled so that IMAP and POP users connect to a proxy server and are redirected to a specific mail server. When you configure the Zimbra server, from the **Main menu** select **zimbra-store**. Then select **9) Enable POP/IMAP proxy**. This sets the feature to **yes**.

When the proxy server is configured, the default POP and IMAP ports are configured for the proxy server. ZCS designates the Zimbra server port numbers. These port numbers cannot be changed. When you enable a proxy server on any Zimbra server, servers that do not have the proxy server enabled, must be configured with appropriate *server* port number listed in Table 3.

Table 3 Zimbra IMAP/POP Proxy Server Port Mapping

	Port
IMAP Proxy port	143
IMAP SSL proxy port	993
POP proxy port	110
POP SSL proxy port	995
IMAP server port	7143
IMAP SSL server port	7993
POP server port	7110
POP SSL server port	7995

When an IMAP or POP user enters his email address and password, the IMAP/POP proxy server searches the LDAP directory server to find which Zimbra server host the account is created on and then passes the authenticating through to the appropriate mailbox server. The proxy server does not contain any data.

After the initial installation, you can edit the global and server configuration from the administration console.

Configuring for Virtual Hosting

You can configure multiple virtual hostnames to host more than one domain name on a server. When you create a virtual host, users can log in without have to specify the domain name as part of their user name.

Virtual hosts are configured from the administration console **Domains>Virtual Hosts** tab. The virtual host requires a valid DNS configuration with an A record.

When users log in, they enter the virtual host name in the browser. For example, **https://mail.example.com**. When the Zimbra logon screen displays, users enter only their user name and password. The authentication request searches for a domain with that virtual host name. When the virtual host is found, the authentication is completed against that domain.

Load Balancing on ZCS

You can deploy a load balancer for the Zimbra server so that all users can log in using the same address/name instead of having to remember which server their mailbox is on.

An example scenario for ZCS load balancing

You set up a virtual hostname of mail.example.com and configure four mail servers, mail1.example.com to mail4.example.com.

When users log on to mail.example.com, the load balancer directs the user to any one of the mail servers to verify the log on information. After successfully logging on, users are redirected to the actual server their mail is stored on. While they are logged on, all subsequent requests go directly to their server.

How to set up

In order to configure load balancing for ZCS,

1. Each Zimbra servers must have a routeable address/name.
2. You must configure the virtual hostname on the administration console.
3. You must turn on the following localconfig setting on each mail server,
zmlocalconfig -e zimbra_auth_always_send_refer=true

Chapter 4 Multiple-Server Installation

The installation is straight-forward and easy to run. You run the same install script on each server, select which component(s) to install, and use the menu to configure the system. After the installation is complete, two additional steps to fetch the ssh encryption keys and enable some logger functionality should be run. When the server installation is complete, the servers are started, and the status is displayed.

Important: *Install the servers in the following order*

1. LDAP server
2. Zimbra mailbox servers
3. Zimbra MTA servers

Important: *Do not manually create the user 'zimbra' before running the ZCS installation. The installation automatically creates this user and sets up its environment.*

Starting the Installation Process

For servers other than Mac servers, step 1 through step 4 are performed for each server to be installed.

For Mac servers, see “Starting the Installation Process on the Mac Server” on page 23.

1. Log in as **root** to the Zimbra server and **cd** to the directory where the Zimbra Collaboration Suite archive file is saved (**cd /var/<tmp>/var**). Type the following commands.
 - **tar xzvf [zcs.tgz]** to unpack the file
 - **cd zcs** to change to the correct directory
 - **./install.sh** to begin the installation

Note: *As the installation proceeds, press **Enter** to accept the defaults that are shown in brackets [] or enter the appropriate answer for your configuration.*

The screen shots are examples of the Zimbra installation script.

```
[root@mailhost tmp]# tar xzvf zcs.tgz
zcs/
zcs/install.sh
zcs/packages/
zcs/packages/zimbra-ldap-3.0.M2_316.RHEL4-20051007080249.i386.rpm
zcs/packages/zimbra-logger-3.0.M2_316.RHEL4-20051007080249.i386.rpm
zcs/packages/zimbra-snmp-3.0.M2_316.RHEL4-20051007080249.i386.rpm
zcs/packages/zimbra-mta-3.0.M2_316.RHEL4-20051007080249.i386.rpm
zcs/packages/zimbra-core-3.0.M2_316.RHEL4-20051007080249.i386.rpm
zcs/packages/zimbra-store-3.0.M2_316.RHEL4-20051007080249.i386.rpm
zcs/README.txt
zcs/readme_binary.txt
zcs/docs/
zcs/docs/quick_start.pdf
zcs/docs/RNZCSN.pdf
zcs/docs/admin.pdf
.
.
.
[root@ tmp]# cd zcs
[root@ zcs]# ./install.sh

Operations logged to /tmp/install.log.9496
Checking for existing installation...
zimbra-ldap...NOT FOUND
zimbra-logger...NOT FOUND
zimbra-mta...NOT FOUND
zimbra-snmp...NOT FOUND
zimbra-store...NOT FOUND
zimbra-apache...NOT FOUND
zimbra-spell...NOT FOUND
zimbra-core...NOT FOUND
```

2. The installation process checks to see if Sendmail, Postfix, and MySQL software are running. If any application is running, you are asked to disable it. The default is **Yes** to disable the applications. Disabling MySQL is optional, but highly recommended. Sendmail and Postfix must be disabled for the Zimbra Collaboration Suite to start correctly.
3. The installation process checks to see if a Zimbra license is already installed. If no license file is found, a warning displays stating that the ZCS Connector for Outlook, Zimbra Mobile, and Zimbra account creation will not work without a valid license file. When asked if you wish to continue, type **Y** to continue the installation.

Important: When the installation is complete, you will need to install the Zimbra license. See the *Post Installation Tasks* section.

4. The Zimbra software agreement is displayed and includes the link to the license terms for the Zimbra Collaboration Suite. Please read the agreement and to continue, press **Enter**.

```
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
ZIMBRA, INC. ("ZIMBRA") WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU
FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR
INSTALLING THE SOFTWARE, OR USING THE PRODUCT, YOU ARE CONSENTING TO
BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS
OF THIS AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.
```

```
License Terms for the Zimbra Collaboration Suite:
http://www.zimbra.com/license/index.html
```

```
Press Return to continue
```

5. Next, the installer checks to see that the prerequisite software is installed. If NPTL, sudo, libidn, cURL, fetchmail, GMP or compat-libstdc++ are not installed, the install process quits. You must fix the problem and start the installation over.

Note: Before the Main menu is displayed, the installer checks to see if the hostname is resolvable via DNS and if there is an error asks if you would like to change the hostname. The domain name should have a MX record configured in DNS.

Starting the Installation Process on the Mac Server

The following steps are performed on each Mac server to be installed.

1. Click on the dmg file to open the file and then click **ZCS.mpkg** to open the Zimbra install package. The Apple installer opens and verifies that the server is ready to install the Zimbra Collaboration Suite. Click **Continue**.
2. Welcome screen appears, click **Continue**.
3. The Zimbra Software License Agreement is displayed. Read the agreement and click **Continue**. A popup screen appears asking that to continue the install you must accept the terms of the license agreement. Click **Agree**.
4. Select the destination volume to install the software. Click **Continue**.
5. The **Easy Install ...** dialog displays. Now you select which services to be installed on this server.

To select which services to install, click **Customize**. Deselect those packages you do not want installed. See "Planning for the Installation" on page 11 for information about the packages. Click **Install** to proceed.

A progress bar shows the Zimbra packages being installed. When **The software was successfully installed** dialog displays, click **Close**.

6. Open the Apple Terminal and log on as **root**. Type **sudo /bin/bash**. Enter your root password, if asked.
7. Type **cd /opt/zimbra/libexec**.

8. Type `ls` to see the packages in the directory.
9. Type `./zmsetup.pl`. This starts the ZCS configuration. A temporary log file is created and the server port configurations are checked for conflicts. The installation process checks to see if Sendmail, Postfix, and MySQL software are running. If any of these applications are running, you are asked to disable them. Disabling MySQL is optional but highly recommended. Sendmail and Postfix must be disabled for the Zimbra Collaboration Suite to start correctly.
10. If no conflicts are found, the Main menu displays the default entries for the Zimbra component you are installing. To expand the menu to see the configuration values type `X` and press `Enter`. The main menu expands to display configuration details for the package being installed. Values that require further configuration are marked with asterisks (*).
11. To continue, follow the installation instructions for each server type, starting with Step 3.

Installing Zimbra LDAP Master Server

You must configure the Zimbra Master LDAP server before you can install the other Zimbra servers.

1. Follow steps 1 through 4 in **Starting the Installation Process** section to open a SSH session to the LDAP server, log on to the server as root, and unpack the Zimbra software.
2. The `zimbra-ldap` package should be marked `y`. The MTA, Store and Logger packages should be marked `n`. If you are using SNMP, SNMP package is marked `y`.

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

Installing:
  zimbra-core
  zimbra-ldap

This system will be modified. Continue [N] Y
Configuration section
```

3. Type `y`, and press `Enter` to modify the system. The selected packages are installed on the server.

The Main menu displays showing the default entries for the Zimbra component you are installing. To expand the menu to see the configuration values type **x** and press **Enter**. The main menu expands to display configuration details for the package being installed. Values that require further configuration are marked with asterisks (*).

To navigate the Main menu, select the menu item to change. You can modify any of the defaults. See [Table 2, "Main Menu Options," on page 14](#) for a description of the Main menu.

```

Main menu

 1) Hostname:                               ldap.example.com
 2) Ldap master host:                       ldap.example.com
 3) Ldap port:                               389
 4) Ldap password:                           set
 5) zimbra-ldap:                             Enabled
    +Create Domain:                           yes
    +Domain to create:                         ldap.example.com
r) Start servers after configuration         yes
s) Save config to file
x) Expand menu
q) Quit

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

```

Items with an asterisks must be configured.

4. Type **4** to display the automatically generated LDAP password. You can change this password.

Remember the LDAP password, the LDAP host name, and the LDAP port. You must configure this information, when you install the MTA server and the mailbox servers.

5. Type **5** to change the zimbra-ldap settings.
 - Type **3** to change the default domain name to the email domain name.

```

Ldap configuration

 1) Status:                               Enabled
 2) Create Domain:                         yes
 3) Domain to create:                       ldap.example.com

Select, or 'r' for previous menu [r] 3

Create Domain: [ldap.example.com] example.com

```

6. When the LDAP server is configured, type **a** to apply the configuration changes. Press **Enter** to save the configuration data.
7. When **Save Configuration data to a file** appears, press **Enter**.

8. When **The system will be modified - continue?** appears, type **y** and press **Enter**.

The server is modified. Installing all the components and configuring the server can take a few minutes.

9. When **Installation complete - press return to exit** displays, press **Enter**.

The installation of the LDAP server is complete.

```
Select, or press 'a' to apply config (? - help) a
Save configuration data? [Yes]
Save config in file: [/opt/zimbra/config.2843]
Saving config in /opt/zimbra/config.2843...Done
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.log.2843
Setting local config zimbra_server_hostname to [ldap.example.com]
.
Operations logged to /tmp/zmsetup.log.2843

Installation complete - press return to exit
```

Installing Zimbra Mailbox Server

The Zimbra-store 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 servers can be added at any time.

Note: *The Zimbra logger is installed on only one Zimbra mailbox server.*

1. Follow steps 1 through 4 in **Starting the Installation Process** section to log on to the server as root and unpack the Zimbra software.
2. Type **y** to install the **zimbra-store**, **zimbra-logger** (optional and only on one mailbox server), and **zimbra-spell** (optional) packages. When **zimbra-spell** is installed the **zimbra-apache** package is also installed.

```
Installing:
  zimbra-core
  zimbra-store
  zimbra-logger
  zimbra-apache
  zimbra-spell
```

3. Press **Enter** to modify the system. The selected packages are installed on the server.

At this point the Main menu displays the default entries for the Zimbra component you are installing. To expand the menu to see the configuration values type **x** and press **Enter**.

To navigate the Main menu, select the menu item to change. You can modify any of the defaults.

```

Main menu

  1) Hostname:                               mailhost.example.com
** 2) Ldap master host:                       UNSET
  3) Ldap port:                               389
** 4) Ldap password:                         UNSET
  5) zimbra-store:                           Enabled
      +Create Admin User:                    yes
      +Admin user to create:                 admin@mailhost.example.com
***** +Admin Password                       UNSET
      +Enable automated spam training:       yes
      +Spam training user:                  zqjeh@mailhost.example.com
      +Non-spam(Ham) training user:         logpu@mailhost.example.com
***** +SMTP host:                          UNSET
      +Web server HTTP port:                 80
      +Web server HTTPS port:                443
      +Web server mode:                      http
      +Enable POP/IMAP proxy:                no
      +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://
mailhost.example.com:7780/aspell.php

  6) zimbra-logger:                           Enabled
  7) zimbra-spell:                            Enabled
  8) Enable default backup schedule:          yes
  r) Start servers after configuration        yes
  s) Save config to file
  x) Expand menu
  q) Quit

Address unconfigured (**) items or correct ldap configuration (? - help)

Checking ldap on :389...FAILED

```

4. The Hostname is displayed. You must set the LDAP host and password configured on the LDAP server.

- Type **2** and then type the LDAP host name.
- Type **4** and then type the LDAP password.

The server immediately contacts the LDAP server. If it cannot contact the server, you cannot proceed.

5. Type **5** to configure the admin password, the SMTP host, and to set the web server mode, if your configuration is not http.

- Type **4** and set the password for the administrator account. The password is case sensitive and must be a minimum of six characters. The admin account is provisioned on the Zimbra server and allows you to log on to the administration console. The administrator name, mail address, and password are required to log in to the administration console.
- Type **8** to set the SMTP host.
- Type **9**, if you are changing the default. The communication protocol options are HTTP, HTTPS, or mixed. Mixed mode uses HTTPS for logging in and HTTP for normal session traffic. All modes use SSL encryption for back-end administrative traffic
- If you are setting up IMAP/POP proxy servers, type **12** to enable. When you enable these, IMAP and POP server port numbers and proxy port numbers are automatically changed. See the "Planning for the Installation" chapter, Configuring IMAP and POP Proxy Server.

```

Address unconfigured (**) items or correct ldap configuration (? - help)
5
Store configuration

    1) Status:                               Enabled
    2) Create Admin User:                     yes
    3) Admin user to create:                  admin@mailhost.example.com
** 4) Admin Password                         UNSET
    5) Enable automated spam training:        yes
    6) Spam training user:                   k7vb@mailhost.example.com
    7) Non-spam(Ham) training user:          tofx@mailhost.example.com
** 8) SMTP host:                             UNSET
    9) Web server HTTP port:                  80
   10) Web server HTTPS port:                443
   11) Web server mode:                      http
   12) Enable POP/IMAP proxy:                no
   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://
mailhost.example.com:7780/aspell.php

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

```

6. When the mailbox server is configured, type **a** to apply the configuration changes. Press **Enter** to save the configuration data.
7. When **Save Configuration data to a file** appears, press **Enter**.
8. When **The system will be modified - continue?** appears, type **y** and press **Enter**.

The server is modified. Installing all the components and configuring the server can take a few minutes.

9. When **Installation complete - press return to exit** displays, press **Enter**.

The installation of the mailbox server is complete.

```
Select, or press 'a' to apply config (? - help) a
Save configuration data? [Yes]
Save config in file: [/opt/zimbra/config.2843]
Saving config in /opt/zimbra/config.2843...Done
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.log.2843
Setting local config zimbra_server_hostname to [mailhost.example.com]
.
Operations logged to /tmp/zmsetup.log.2843

Installation complete - press return to exit
```

Installing Zimbra MTA on a Server

When the Zimbra MTA is being installed the root LDAP password and the Zimbra LDAP password must be known to the MTA server. If not, the MTA cannot contact the LDAP server and will not be able to complete the installation.

1. Follow steps 1 through 4 in **Starting the Installation Process** section to open a SSH session to the MTA server, log on to the server as root, and unpack the Zimbra software.
2. Enter **y** to install the **zimbra-mta** package. The other packages should be marked **n**. Note: If you installed the SNMP package on the LDAP server, install it here also.
3. Press **Enter** to modify the system. The selected packages are installed on the server.

At this point the Main menu displays the default entries for the Zimbra component you are installing. To expand the menu to see all the configuration values type **X** and press **Enter**.

To navigate the Main menu, select the menu item to change. You can modify any of the defaults.

```

Main menu

  1) Hostname:                               mta.example.com
** 2) Ldap host:                             UNSET
  3) Ldap port:                              389
** 4) Ldap password:                         UNSET
  5) zimbra-mta:                             Enabled
***** +MTA Auth host:                       UNSET
        +Enable Spamassassin:                yes
        +Enable Clam AV:                     yes
        +Notification address for AV alerts:  admin@example.com
r) Start servers after configuration         yes
s) Save config to file
x) Expand menu
q) Quit

Address unconfigured (**) items or correct ldap configuration (? -
help) 2

Please enter the ldap server hostname ldap.company.com
Checking ldap on ldap.company.com:389...FAILED

```

- The Main menu displays. The Hostname is displayed. You must set the LDAP host and password configured on the LDAP server.

- Type **2** and then type the LDAP host name.
- Type **4** and then type the LDAP password.

The server immediately contacts the LDAP server. If it cannot contact the server, you cannot proceed.

- Type **5** and then type **2** to set the **MTA Auth host**. This is the MTA authentication server host name and is set to one of the Zimbra mailbox server's hostname.

Note: *If configuring the MTA server for a cluster environment, the MTA Auth host is the cluster services hostname, not the physical hostname.*

You can change **5, AV alerts notification address**. The administrator's address is configured by default.

Note: *If you enter a new address, you will need to configure this address on the administration console.*

```

Select, or press 'a' to apply config (? - help) 5

Mta configuration

  1) Status:                                 Enabled
**2) MTA Auth host:                         mailhost.example.com
  3) Enable Spamassassin:                    yes
  4) Enable Clam AV:                         yes
  5) Notification address for AV alerts:     admin@mta.example.com

```

6. When the MTA server is configured, type **a** to apply the configuration changes. Press **Enter** to save the configuration data.
7. When **Save Configuration data to a file** appears, press **Enter**.
8. When **The system will be modified - continue?** appears, type **y** and press **Enter**.

The server is modified. Installing all the components and configuring the server can take a few minutes.

9. When **Installation complete - press return to exit** displays, press **Enter**.

The installation of the MTA server is complete.

Installing the Zimbra-SNMP package

Installing the Zimbra-SNMP package is optional, but if you use SNMP monitoring, this package should be installed on each Zimbra server.

In the Main menu select the zimbra-snmp to make changes to the default values.

The following questions are asked for SNMP configuration.

- Configure whether to be notified by SNMP or SMTP. The default is **No**. If you enter yes, you must enter additional information.
 - For SNMP type the SNMP Trap host name.
 - For SMTP type the SMTP source email address and destination email address.

```

8) zimbra-snmp:                               Enabled
   +Enable SNMP notifications:                 yes
   +SNMP Trap hostname:                       mailhost.example.com
   +Enable SMTP notifications:                 yes
   +SMTP Source email address:                 admin@example.com
   +SMTP Destination email address:           admin@example.com

```

Final Set-Up

After the Zimbra LDAP, mailbox, and MTA servers are configured in a multi-node configuration, the following two functions must be configured:

- In order for remote management and postfix queue management, the ssh keys must be manually populated on each server.
- If logger is installed, set up the syslog configuration files on each server to enable server statistics to display on the administration console, and then enable the logger monitor host. The server statistics includes information about the message count, message volume, and anti-spam and anti-virus activity.

Set up the ssh keys. To populate the ssh keys, on each server, as Zimbra user (`su-zimbra`). Type `zmupdateauthkeys` and press **Enter**. The key is updated on `/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.

***Note:** If you set up Zimbra in a cluster environment, the syslog configuration files for logger are automatically modified during the cluster configuration. In a cluster installation, you need only to perform step 1 on the LDAP and MTA servers to enable the syslog.*

1. On each server, as root, type `/opt/zimbra/bin/zmsyslogsetup`. This enables the server to display statistics.
2. On the logger monitor host, you must enable **syslog** to log statistics from remote machines.
 - a. Edit the `/etc/sysconfig/syslog` file, add `-r` to the `SYSLOGD_OPTIONS` setting, `SYSLOGD_options="-r -m 0"`
 - b. Stop the syslog daemon. Type `/etc/init.d/syslogd stop`.
 - c. Start the syslog daemon. Type `/etc/init.d/syslogd start`.

Verifying Server Configuration

When **Configuration complete - press return to exit** is displayed, the installation is finished and the server has been started. Before going to the next server, you should verify that the server is running.

Use the CLI command, **zmcontrol status**, to verify that each server is running.

1. For each server in the Zimbra Collaboration Suite environment, log on as a Zimbra administrator, from the root.
2. Type `su - zimbra`.
3. Type `zmcontrol status`. The services status information is displayed. All services should be running.

***Note:** If services are not started, you can type `zmcontrol start`. See the CLI command appendix in the Administration Guide for more `zmcontrol` commands.*

Post Installation Tasks

Once the Zimbra Collaboration Suite is installed, you should go to the administration console and install your Zimbra license. You can configure additional domains and create Classes of Service without the license but you cannot provision accounts. See “Zimbra License” on page 13 for more information about the Zimbra license.

Logging on to the Administration Console

To log on to the administration console, open your browser, type the administration console URL and log on to the console. The administration console URL is entered as

https://[example.com]:7071/zimbraAdmin.

Note: *The administration console address must be typed with “https”, even if you configured only “http”.*

The first time you log on, a certificate authority (CA) alert may be displayed. Click **Accept this certificate permanently** to accept the certificate and be able connect to the Zimbra administration console. Then click **OK**.

Enter the admin user name and password configured during the installation process. Enter the user name as **admin@[example.com]**

Defining Classes of Service

A default Class of Service (COS) is automatically created during the installation of Zimbra software. The COS controls mailbox quotas, message lifetime, password restrictions, attachment blocking and server pools. You can modify the default COS and create new COSs to assign to accounts according to your group management policies.

In an environment with multiple mailbox servers, COS is used to assign the new accounts to a mailbox server. The COS server pool tab lists the mailbox servers in your Zimbra environment. When you configure the COS, select which servers to add to the server pool. Within each pool of servers, a random algorithm assigns new mailboxes to any available server.

To create or modify a COS, from the administration console, click COS. If you have questions, refer to the Help.

Provisioning Accounts

From the administration console, you can quickly create accounts using the New Account Wizard that steps you through the account information to be completed.

To provision accounts:

1. From the admin console navigation pane, click **Accounts**.
2. Click **New**, page 1 of the **New Account Wizard** opens.
3. Enter the account name to be used as the email address. The only required information is the account name and last name.
4. You can click **Finish** at this point, and the account will be configured with the default COS and global features.

If you want to configure aliases, forwarding addresses, and specific features for this account, proceed through the dialog.

Accounts are now ready to send and receive mail.

Refer to the administration guide to learn more about provisioning accounts, including how to provision multiple accounts at once.

Uninstalling Zimbra Collaboration Suite

To uninstall servers, other than Mac servers, you run the install script `-u` and then delete the `zcs` directory and remove the ZCS `tgz` file on the servers.

1. `cd` to the original install directory for the `zcs` files.
2. Type `./install.sh -u`.
3. When **Completely remove existing installation?** is displayed, type **Yes**.
The Zimbra servers are stopped, the existing packages, the `webapp` directories, and the `/opt/zimbra` directory are removed.
4. Delete the `zcs` directory, type `rm -rf zcs`.
5. Delete the `zcs.tgz` file.
6. Additional files may need to be delete. See the Zimbra Wiki Installation section on http://wiki.zimbra.com/index.php?title=Main_Page.

To uninstall ZCS from a Mac server

1. Type `su - zimbra` to go to the Zimbra directory.
2. To stop the Zimbra services, type `zmcontrol stop`. To verify that the services are stopped, type `zmcontrol status`. The display should show all services stopped.
3. Type `Exit`, to return to the root.
4. Run the following commands to remove the Zimbra directories and log files

```
rm -rf /opt/zimbra
rm -rf /Library/Receipts/zimbra-*
rm -f /var/log/zimbra*
rm -f /tmp/install.*
```
5. If you want to remove the `zimbra` user, use the System Preferences, User pane.

Chapter 5 LDAP Replication Installation

LDAP replication lets you distribute Zimbra server queries to specific LDAP replica servers. The Zimbra install program is used to configure a master LDAP server and additional read-only replica servers. The master LDAP server is installed following the normal ZCS installation options. The LDAP replica server installation is modified to point the replica server to the LDAP master host and to set the replica LDAP status to **Disabled**.

After the LDAP servers are correctly installed and configured, the following additional configuration is required.

- SSH keys are set up on each LDAP server
- Trusted authentication between the master LDAP and the LDAP replica servers is set up
- The content of the master LDAP directory is copied to the LDAP replica server. LDAP replica servers are read-only.
- Zimbra servers are configured to query the LDAP replica server instead of the master LDAP server.

Note: *To install a LDAP replica on a previously existing Zimbra server, you run the install program again and perform an upgrade to the server to add the Zimbra LDAP package.*

Installing Zimbra LDAP Master Server

You must install the Zimbra Master LDAP server before you can install LDAP replica servers.

1. Follow steps 1 through 4 in **the Multiple-Server installation** chapter, **Starting the Installation Process** section to open a SSH session to the LDAP server, log on to the server as root, and unpack the Zimbra software.
2. The Zimbra packages to installed should be marked **Y**. Those packages that should not be installed mark **N**.

Note: *These directions and screen shots are for installing the zimbra-LDAP package.*

```

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

Installing:
  zimbra-core
  zimbra-ldap

This system will be modified. Continue [N] Y
Configuration section

```

3. Type **y**, and press **Enter** to modify the system. The selected packages are installed on the server.

The Main menu shows the default entries for the LDAP server. To expand the menu to see the configuration values type **x** and press **Enter**. The main menu expands to display configuration details for the LDAP server.

```

Main menu

1) Hostname:                ldap.example.com
2) Ldap Master host:       ldap.example.com
3) Ldap port:               389
4) Ldap password:          set
5) zimbra-ldap:            Enabled
   +Create Domain:         yes
   +Domain to create:      ldap.example.com
r) Start servers after configuration  yes
s) Save config to file
x) Expand menu
q) Quit

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

```

4. Type **4** to display the automatically generated LDAP password. You can change this password.

Note: Remember the LDAP password, the LDAP master host name, and the LDAP port. You must configure this information when you install the LDAP replica servers.

5. Type **5** to change the zimbra-ldap settings.
 - Type **3** to change the default domain name to the email domain name.

```
Ldap configuration

  1) Status:                               Enabled
  2) Create Domain:                         yes
  3) Domain to create:                      ldap.example.com
Select, or 'r' for previous menu [r] 3

Create Domain: [ldap.example.com] example.com
```

6. When the LDAP server is configured, type **a** to apply the configuration changes. Press **Enter** to save the configuration data.

```
Select, or press 'a' to apply config (? - help) a
Save configuration data? [Yes]
Save config in file: [/opt/zimbra/config.2843]
Saving config in /opt/zimbra/config.2843...Done
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.log.2843
Setting local config zimbra_server_hostname to [ldap.example.com]
.
Operations logged to /tmp/zmsetup.log.2843

Installation complete - press return to exit
```

7. When **Save Configuration data to a file** appears, press **Enter**.
8. When **The system will be modified - continue?** appears, type **y** and press **Enter**.

The server is modified. Installing all the components and configuring the server can take a few minutes.

9. When **Installation complete - press return to exit** displays, press **Enter**.

The installation of the master LDAP server is complete.

Installing a LDAP Replica Server

You run the ZCS install program on the replica server to install the LDAP package, but you make the following configuration changes.

- In the Zimbra LDAP menu, you must change the Status to **Disabled**.

Important: *If you do not disable the ldap replica servers, a new directory server is created and you will have separate mail systems.*

- On the Main menu, change LDAP master host name, port and LDAP password to be the same information as on the Master LDAP server.

Follow steps 1 through 4 in **Starting the Installation Process** section to open a SSH session to the LDAP server, log on to the server as root, and unpack the Zimbra software.

1. The **zimbra-ldap** package should be marked **y**.

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

Installing:
  zimbra-core
  zimbra-ldap

This system will be modified. Continue [N] Y
Configuration section
```

2. Type **y**, and press **Enter** to modify the system. The selected packages are installed.

The Main menu shows the default entries for the LDAP replica server. To expand the menu type **x** and press **Enter**.

```
Main menu

1) Hostname: ldapRep.example.com
2) Ldap Master host: ldapRep.example.com
3) Ldap port: 389
4) Ldap password: set
5) zimbra-ldap: Enabled
   +Create Domain: yes
   +Domain to create: ldapRep.example.com
r) Start servers after configuration yes
s) Save config to file
x) Expand menu
q) Quit

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

3. Type **5** to disable the zimbra-ldap settings.
 - Type **1** to change the Status to **Disabled**.
Important, if you do not disable the ldap replica servers, a new directory server is created and you will have separate mail systems.

```
Ldap configuration
  1) Status:                               Disabled
Select, or 'r' for previous menu [r]
```

4. Type **2** and change the LDAP Master host name to the Master LDAP host name that you configured earlier.
5. Type **3**, and change the port to the same port as configured for the Master LDAP server.
6. Type **4** and change the password to the Master LDAP server password.
7. When the LDAP server is configured, type **a** to apply the configuration changes. Press **Enter** to save the configuration data.

```
Select, or press 'a' to apply config (? - help) a
Save configuration data? [Yes]
Save config in file: [/opt/zimbra/config.2843]
Saving config in /opt/zimbra/config.2843...Done
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.log.2843
Setting local config zimbra_server_hostname to [ldap.example.com]
.
Operations logged to /tmp/zmsetup.log.2843

Installation complete - press return to exit
```

8. When **Save Configuration data to a file** appears, press **Enter**.
9. When **The system will be modified - continue?** appears, type **y** and press **Enter**.

The server is modified. Installing all the components and configuring the server can take a few minutes.

10. When **Installation complete - press return to exit** displays, press **Enter**.

The installation is complete.

Setting Up Zimbra LDAP Servers for Replication

After the master and replica LDAP servers are installed, before LDAP replication will work you must complete the following steps.

- Populate the ssh keys
- Set up replication
- Test the replica

CLI commands are run as Zimbra user.

To set up the LDAP servers

1. On the master LDAP server,
 - Type **zmupdateauthkeys** and press **Enter**.
 - Type **zmldapenablereplica**, and press **Enter**

The key is updated on **/opt/zimbra/.ssh/authorized_keys**.

2. On the LDAP replica server,
 - Type **zmupdateauthkeys** and press **Enter**
 - Type **zmldapenablereplica** and press **Enter**

This sets up the replication account in the directory and makes a copy of the master content to the replica LDAP server.

Note: If **zmupdateauthkeys** does not fetch the keys correctly, run **zmsshkeygen** on both servers and rerun **zmupdateauthkeys**.

To test the replica

1. Create several user accounts, either from the admin console or on the master LDAP server. The CLI command is **zmprov ca <name@domain.com> <password>**
2. To see if the accounts were correctly copied to the LDAP replica server, on the replica LDAP server, type **zmprov gaa**. The accounts created on the master LDAP should display on the LDAP replica.

Configuring Zimbra Servers to use LDAP Replica

To use the LDAP replica server instead of the master LDAP server, you must add the LDAP replica URL on each Zimbra server

1. Stop the Zimbra services on the server, **zmcontrol stop**.

2. Enter the LDAP replica server URL"

zmlocalconfig -e ldap_url="ldap://<replicahost>ldap://<masterhost>"

Enter more than one replica hostnames in the list typed as **"ldap://<replicahost1>ldap://<replicahost2>ldap://<masterhost>"**. The hosts are tried in the order listed.

3. Restart the Zimbra server, **zmcontrol start**.

Chapter 6 Zimbra Cluster Installation - Multi-Node Configuration

For Red Hat Cluster Suite Integration

Zimbra Collaboration Suite can be integrated with Red Hat® Enterprise Linux® Cluster Suite version 4, update 3 to provide high availability.

In a cluster implementation, all Zimbra mailbox servers are part of a cluster under the control of the Red Hat Cluster Manager.

Note: *Red Hat Cluster Suite consists of Red Hat Cluster Manager and Linux Virtual Server Cluster. For Zimbra, only Red Hat Cluster Manager is used. In this guide, Red Hat Cluster Suite refers only to Cluster Manager.*

Pre-configuration Requirements

All servers must meet the requirements described in the [installation prerequisites](#) chapter, in addition to the requirements described here.

Go to the Red Hat Cluster Suite website, <https://www.redhat.com/software/rha/cluster> to view specific system requirements for cluster configurations using Red Hat Cluster Suite. If you are not familiar with the Red Hat Cluster Suite, read the documentation to understand how each of the components work to provide high availability.

Hardware for the Cluster Environment

For Red Hat Cluster Suite integration, the following hardware is required.

- SAN (shared disk storage device) to store the data for each of the Zimbra mailbox servers. The size of the shared storage device depends on your expected site capacity.
- Network power control switch to connect cluster nodes. The power control switch is used as the fence device for I/O fencing during a failover. Use either a APC or a WTI network power switch.

Configure the network power control switch according to the manufacturer's requirements.

Software Requirements For Clustering

- The Red Hat Enterprise Linux 4, Update 3 operating system installed on each mailbox server node configured with the same netmask and broadcast address.

- To use the Red Hat Cluster Configuration Tool GUI, install X Window and a desktop environment such as GNOME or KDE .
- Red Hat Cluster Suite, Update 3 on each mailbox server node.

Preparing the SAN

Configure the SAN device and create the partitions for the volumes. Refer to the Red Hat Cluster Suite documentation for configuration requirements. The SAN device must be partitioned to provide the following volumes for each Zimbra mailbox server in the cluster.

- **conf** Volume for the service-specific configuration files
- **log** Volume for the local logs for Zimbra server
- **redolog** Volume for the redo logs for the Zimbra server
- **data (mysql)** Volume for the MySQL data files for the data store
- **store** Volume for the message files
- **index** Volume for the search index files
- **backup** Volume for the backup files
- **logger** Volume for the MySQL data files for logger service's MYSQL instance
- **logger/db/data** Volume for logger data
- **openldap -data** Volume for OpenLDAP data
- **postfix/spool** Volume for Postfix/spool

Overview of Cluster Installation

Red Hat Cluster Suite integration requires planning the cluster design and precisely executing the configuration. The Zimbra Cluster software automates the setup on the nodes. The scripts in the Zimbra Cluster software configure the Zimbra Collaboration Suite servers for Red Hat Cluster integration. In most cases, you may not need to use Red Hat's graphical Cluster Configuration Tool to configure the Zimbra cluster. If you do, refer to the Red Hat Cluster Suite documentation for detailed configuration and management instructions.

The Zimbra Cluster software includes:

- **Zimbra Cluster install script**, used before the Zimbra Collaboration Suite installer to create the mount points for the SAN volumes.
- **Zimbra Cluster post install script**, used after Zimbra Collaboration Suite is installed on the servers to move the data files from the local disk to the volumes created on the SAN.
- **Zimbra Cluster configurator script** that runs on one active node. The configurator script automates the Red Hat Cluster configuration process, taking you through the steps to create the `/etc/cluster/cluster.conf` file. In addition, the configurator script copies the `cluster.conf` file to each node.

Cluster Scenario

The screen-shots in this chapter describe configuring a cluster environment with two active nodes, one standby node, and two cluster services and separate LDAP and MTA servers that are not under the control of Red Hat Cluster Suite. The domain name is **example.com**.

The following Zimbra servers are configured:

- One Zimbra LDAP server, **ldap.example.com**
- One Zimbra MTA server, **mta.example.com** ()
- Three Zimbra mailbox nodes. Two mailbox nodes are active servers. One mailbox node is the standby server.
 - Active mailbox node 1, **node1.example.com**
 - Active mailbox node 2, **node2.example.com**
 - Standby mailbox node, **node3.example.com**
- Two cluster services, one for each of the active nodes
 - Cluster Service 1, **mail1.example.com**
 - Cluster Service 2, **mail2.example.com**

Sixteen volumes are configured on the SAN for this example cluster, eight for each of the two services.

Installing and Configuring the Software

You should install and configure ZCS servers in the following order:

1. Zimbra LDAP server
2. Active and standby mailbox nodes as the Zimbra mailbox servers in the cluster.
3. MTA servers. The MTA server is last because you need to configure one of the active cluster services' hostname as the MTA auth host.

See the [Multiple-Server Installation](#) chapter, for instructions about how to install the Zimbra LDAP and Zimbra MTA servers.

Install the Active Mailbox Nodes

For each active mailbox node, install and configure the following software:

- Red Hat Cluster Suite software
- Zimbra Cluster software
- Zimbra Collaboration Suite software

Installing the Red Hat Cluster Suite Software

On each node, install the required RPMs and the **rgmanager** RPM for *Red Hat Cluster Suite with DLM*. See the Red Hat Cluster Suite documentation, [Determining RPMs To Install Determining](#) section for descriptions and the installation instructions.

Installing the Zimbra Cluster Software

The Zimbra Cluster software consists of **install.pl**, **postinstall.pl**, and **configure-cluster.pl** scripts to automate the cluster configuration process and files that are used during the Zimbra cluster service operation.

The software is a standard compressed tar file. Save the file to the computer from which you will install the software.

1. Log in as **root** to the Zimbra server and **cd** to the directory where the Zimbra **zcs-cluster.tgz** file is saved. Type the following commands:
 - **tar xzvf zcs-cluster.tgz** to unpack the file
 - **cd zcs-cluster** to change to the correct directory
 - **./install.pl** to begin the installation

The necessary scripts, files, and Red Hat Cluster Suite patches are installed.

```
[root@node1 zcs-cluster]# ./install.pl

Each cluster node needs zimbra user and zimbra group. The same user ID
and group ID must be used on all cluster nodes to allow files on SAN
owned by zimbra user/group to be accessible on every node.

Enter zimbra group ID [500]:
... groupadd -g 500 zimbra

Enter zimbra user ID [500]:
... useradd -u 500 -g zimbra -G tty -d /opt/zimbra -s /bin/bash zimbra
... chown root:root /opt/zimbra

Creating root directory for mount points
... mkdir -p /opt/zimbra-cluster/mountpoints
```

2. Type the Zimbra group ID (GID) to be used. The same group ID number must be configured on every node. The default is 500. Change the default, if this group ID is not available on all the nodes in the cluster.
3. Type the Zimbra user ID (UID) to be used. The same user ID number must be configured on every node. The default is 500. Change the default, if this user ID is not available on all the nodes in the cluster.
4. Type the first cluster service name, press **Enter**. Type **mail1.example.com**. This is the public hostname. The eight volume mount points for the cluster service are created.

5. Type additional cluster service names until all services are configured.
6. Type **Done**, when finished.

On every mailbox server node you need to create mount points for all cluster services. Enter one service name per prompt.

```
Enter cluster service name ("done" to finish): mail1.example.com
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail1.example.com
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail1.example.com/conf
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail1.example.com/log
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail1.example.com/redolog
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail1.example.com/db/data
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail1.example.com/store
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail1.example.com/index
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail1.example.com/backup
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail1.example.com/logger/
db/data

Enter cluster service name ("done" to finish): mail2.example.com
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail2.example.com
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail2.example.com/conf
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail2.example.com/log
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail2.example.com/redolog
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail2.example.com/db/data
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail2.example.com/store
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail2.example.com/index
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail2.example.com/backup
.... mkdir -p /opt/zimbra-cluster/mountpoints/mail2.example.com/logger/
db/data

Enter cluster service name ("done" to finish): done

Mount points were created for the following cluster services:

mail1.example.com
mail2.example.com
```

Installing the Zimbra Collaboration Suite Software

Important: Before proceeding, review Chapter 3, *Planning for the Installation* to learn about the Zimbra packages that are installed. If you install the Logger package, it must be installed on each mailbox node but only enabled on the first active node.

For each active node in the cluster, install the Zimbra Collaboration Suite as follows. For a smooth installation, note these configuration points.

- When the Zimbra software is installed, the installation detects the hostname configured for the server and automatically inserts this name as the default hostname for various values. The server hostname must be changed to the cluster service name configured in [Step 4](#) in *Installing the Zimbra Cluster Software* section.

- *The LDAP server name and LDAP password are required. To find the LDAP password, after the LDAP server is installed, on the LDAP server, type `su - zimbra`, then type `zmlocalconfig -s ldap_root_password`.*
1. Log in as **root** to the server and **cd** to the directory where the Zimbra zcs.tgz file is saved. Type the following commands.
 - **tar xzvf zcs.tgz** to unpack the file
 - **cd zcs** to change to the correct directory
 - **./install.sh** to begin the installation

The installation process checks to see if Sendmail, Postfix, and MySQL software are running. If any of these are, you are asked to disable them. The default is **Yes** to disable them. Disabling MySQL is optional, but highly recommended.

The install.sh script displays a reference to the Zimbra Public License with an address to view the license, and then reviews the installed software to verify that the prerequisite software is installed. If any is missing, the installation stops.

2. When asked to select the packages to install, type **N** for the Zimbra-LDAP, and Zimbra MTA packages. Zimbra Store, Zimbra SNMP, Zimbra Logger and Zimbra Spell should be marked **Y**. Press **Enter**. (Of these packages, only Zimbra Store is required.)

```
Installing:
  zimbra-core
  zimbra-logger
  zimbra-snmp
  zimbra-store
  zimbra-apache
  zimbra-spell
```

The selected packages are installed on the mailbox server.

At this point the **Main menu** displays the default entries for the mailbox server you are installing.

3. Change the **Hostname** to one of the cluster service names entered *in [Step 4 in Installing the Zimbra Cluster Software section](#)* (In our example, this is **mail1.example.com**). Type **1**, and then type the cluster service name, press **Enter**.
4. Set the LDAP host and password.
 - Type **2** and then type the LDAP host name.
 - Type **4** and then type the LDAP password.

As you enter each of these values the server tries to contact the LDAP server. You can proceed when the LDAP server is successfully contacted.

5. Modify Zimbra-store. Type **5** to configure the SMTP host and set the web server mode, if it is not http.

- Type **2** and then type the Zimbra MTA host name.
- Type **3**, if you are changing the default mode. The communication protocol options are HTTP, HTTPS, or mixed. Mixed mode uses HTTPS for logging in and HTTP for normal session traffic. All modes use SSL encryption for back-end administrative traffic.

Important: For clustering, the Web mode must be identical on all nodes.

```
Store configuration

1) Status:                               Enabled
2) SMTP host:                             smtp.example.com
3) Web server mode:                       https
4) IMAP server port:                      143
5) IMAP server SSL port:                  993
6) POP server port:                       110
7) POP server SSL port:                   995
8) Use spell check server:                yes
9) Spell server URL:                      http://
mail1.example.com:7780/aspell.php

Select, or 'r' for previous menu [r]
Checking ldap on ldap.example.com:389...Success
```

6. If you installed the SNMP package, you will need to modify the default notification addresses. Type **6** to modify the SNMP packages.

Configure whether to be notified by SNMP or SMTP. The default is **No**. If you enter yes, you must enter additional information.

- For SNMP, enter the SNMP Trap host name.
- For SMTP, enter the SMTP source email address and destination email address. Type the same host address as configured in the LDAP server.

```
Snmp configuration

1) Status:                               Enabled
2) Enable SNMP notifications:             yes
3) SNMP Trap hostname:                   snmp.example.com
4) Enable SMTP notifications:            yes
5) SMTP Source email address:             admin@example.com
6) SMTP Destination email address:        admin@example.com

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

7. When Logger is installed, it must be enabled on **the first** node. All other nodes must install but disable Logger. To disable logger, type the menu number for Logger and press **Enter**.
8. If you have no other changes, type **a** to apply the configuration changes. Press **Enter**, after **Save configuration data?** displays.

9. When **The system will be modified - continue?** appears, type **Y** and press **Enter**.
10. After the **Operations logged to /tmp/zmsetup.log.xxx**, press **Enter**. The server is modified. Installing all the components and configuring the server can take a few minutes.
11. When **Installation complete - press return to exit** displays, press **Enter**.

Mounting Volumes for Cluster Service

- Mount the eight-volume set for a cluster service entered in Step 4 of the Installing the Zimbra Cluster Software. The volumes must be mounted before proceeding.

***Important:** Verify that the mounted volumes are empty before proceeding.*

Running Zimbra Cluster Post Install Script

1. To start the Zimbra post install cluster configuration script, **cd** to the zcs-cluster directory created in the Installing the Zimbra Cluster Software section. Type **./postinstall.pl** to begin post install.

```
[root@node1 zcs-cluster]# ./postinstall.pl
Disabling boot-time auto start of Zimbra applications.
.... chkconfig --del zimbra

Enabling remote syslogging
.
.
Installing RPMS
.
Installing RHCS patches
.
.
.
Modifying /etc/sudoers...

Backing up existing cluster.conf
.... mv /etc/cluster/cluster.conf /etc/cluster/cluster.conf.bak

Checking node type (active vs. standby)...
Enabling cluster administration in Admin Console

Setting cluster root in localconfig
.... su - zimbra -c 'zmlocalconfig -e zimbra_cluster_root=/opt/
zimbra-cluster'

Detecting service name installed on this node...
service name = mail1.example.com

Service-specific data files must be moved to SAN volumes. All SAN
volumes
for mail1.example.com service must now be mounted using mount points
created in /opt/zimbra-cluster/mountpoints/mail1.example.com
directory.

Are the SAN volumes mounted for mail1.example.com service? (Y/N) y
```

2. Type **Y** to confirm that the SAN volumes are mounted for the selected service.

The Zimbra processes are stopped, various cluster-specific adjustments are made to the Zimbra Collaboration Suite installation, and the data files are moved to the service-specific volumes.

```
Stopping Zimbra processes...
.... su - zimbra -c 'zmcontrol stop'
Host maill.example.com
    Stopping antispam...Done
    Stopping antivirus...Done
    Stopping logger...Done
    Stopping mailbox...Done
    Stopping snmp...Done
    Stopping spell...Done

Moving data files to /opt/zimbra-cluster/mountpoints/maill.example.com
.... mv -f /opt/zimbra/conf/* /opt/zimbra-cluster/mountpoints/
maill.example.com/conf
.... rmdir /opt/zimbra/conf
.... chown zimbra:zimbra /opt/zimbra-cluster/mountpoints/
maill.example.com/conf
.... mv -f /opt/zimbra/log/* /opt/zimbra-cluster/mountpoints/
maill.example.com/log
.... rmdir /opt/zimbra/log
.... chown zimbra:zimbra /opt/zimbra-cluster/mountpoints/
maill.example.com/log
.... mv -f /opt/zimbra/redolog/* /opt/zimbra-cluster/mountpoints/
maill.example.com/redolog
.... rmdir /opt/zimbra/redolog
.... chown zimbra:zimbra /opt/zimbra-cluster/mountpoints/
maill.example.com/redolog
.... mv -f /opt/zimbra/db/data/* /opt/zimbra-cluster/mountpoints/
maill.example.com/db/data
.... rmdir /opt/zimbra/db/data
.... chown zimbra:zimbra /opt/zimbra-cluster/mountpoints/
maill.example.com/db/data
.... mv -f /opt/zimbra/store/* /opt/zimbra-cluster/mountpoints/
maill.example.com/store
mv: cannot stat `/opt/zimbra/store/*': No such file or directory
.... rmdir /opt/zimbra/store
.... chown zimbra:zimbra /opt/zimbra-cluster/mountpoints/
maill.example.com/store... mv -f /opt/zimbra/index/* /opt/zimbra-
cluster/mountpoints/maill.example.com/index
mv: cannot stat `/opt/zimbra/index/*': No such file or directory
.... rmdir /opt/zimbra/index
.... chown zimbra:zimbra /opt/zimbra-cluster/mountpoints/
maill.example.com/index... mv -f /opt/zimbra/backup/* /opt/zimbra-
cluster/mountpoints/maill.example.com/backup
mv: cannot stat `/opt/zimbra/backup/*': No such file or directory
.... rmdir /opt/zimbra/backup
.... chown zimbra:zimbra /opt/zimbra-cluster/mountpoints/
maill.example.com/backup
.... mv -f /opt/zimbra/logger/db/data/* /opt/zimbra-cluster/
mountpoints/maill.example.com/logger/db/data
.... rmdir /opt/zimbra/logger/db/data
.... chown zimbra:zimbra /opt/zimbra-cluster/mountpoints/
.
.
.
```

- When the data has been moved, the eight volumes are unmounted. Press **Enter**, when asked.

```

About to unmount volumes for mail1.example.com service
Volumes to be unmounted:
 /opt/zimbra-cluster/mountpoints/mail1.example.com/conf
 /opt/zimbra-cluster/mountpoints/mail1.example.com/log
 /opt/zimbra-cluster/mountpoints/mail1.example.com/redolog
 /opt/zimbra-cluster/mountpoints/mail1.example.com/db/data
 /opt/zimbra-cluster/mountpoints/mail1.example.com/store
 /opt/zimbra-cluster/mountpoints/mail1.example.com/index
 /opt/zimbra-cluster/mountpoints/mail1.example.com/backup
 /opt/zimbra-cluster/mountpoints/mail1.example.com/logger/db/data
Press Enter to unmount volumes.
... umount /opt/zimbra-cluster/mountpoints/mail1.example.com/conf
... umount /opt/zimbra-cluster/mountpoints/mail1.example.com/log
... umount /opt/zimbra-cluster/mountpoints/mail1.example.com/redolog
... umount /opt/zimbra-cluster/mountpoints/mail1.example.com/db/data
... umount /opt/zimbra-cluster/mountpoints/mail1.example.com/store
... umount /opt/zimbra-cluster/mountpoints/mail1.example.com/index
... umount /opt/zimbra-cluster/mountpoints/mail1.example.com/backup
... umount /opt/zimbra-cluster/mountpoints/mail1.example.com/logger/
db/data

Done.

```

Repeat these steps for every active node in the cluster.

Configuring the Standby Mailbox Server Node

For the standby mailbox server node, install and configure the following software:

- Red Hat Cluster Suite software
- Zimbra Cluster software
- Zimbra Collaboration Suite software

Installing the Red Hat Cluster Suite Software

install the required RPMs and the **rgmanager** RPM for *Red Hat Cluster Suite with DLM*. See the Red Hat Cluster Suite documentation, *Determining RPMs To Install Determining* section for descriptions and the installation instructions.

Installing the Zimbra Cluster Software

The Zimbra Cluster software is installed and run on each standby node. The software automates the cluster configuration process. The software is a standard compressed tar file. Save the file to the computer from which you will install the software.

The stand-by node is configured exactly the same as the active nodes. You define the same group ID and user ID and identify the cluster service names.

1. Log in as **root** to the Zimbra mailbox server and go to the directory where the Zimbra **zcs-cluster.tgz** file is saved. Untar and type **./install.pl** to begin.
2. Type the Zimbra group ID (GID) to be used. The same group ID number must be configured on every node. The default is 500. Change the default, if you changed it for the active nodes.
3. Type the Zimbra user ID (UID) to be used. The same user ID number must be configured on every node. The default is 500. Change the default, if you changed it for the active nodes.
4. Type the first cluster service name, press **Enter**. Type as **mail1.example.com**. Mount points are created.
5. Continue to add each standby cluster service. The same cluster service names must be entered as on the active nodes
6. Type **Done**, when finished.

Installing the Zimbra Collaboration Suite Software on the Standby Node

Install the Zimbra Collaboration Suite on the standby node. For detailed description of the installation process, review the Zimbra Collaboration Suite Multi-Server Installation Guide.

Important: For a smooth installation, note these configuration points.

- When the Zimbra software is installed, the installation detects the hostname configured for the server and automatically inserts this name as the default hostname for various values. **For the standby node, do not change from the default.**
 - The LDAP server name and LDAP password are required. To find the LDAP password, after the LDAP server is installed, on the LDAP server, type **su - zimbra**, then type **zmlocalconfig -s ldap_root_password**.
1. Log in as **root** to the Zimbra server and **cd** to the directory where the Zimbra **zcs.tgz** file is saved. Type the following commands.

- **tar xzvf zcs.tgz** to unpack the file
- **cd zcs** to change to the correct directory
- **./install.sh** to begin the installation

The installation process checks to see if Sendmail, Postfix, and MySQL software are running. If any of these are, you are asked to disable them. The default is **Yes** to disable them. Disabling MySQL is optional, but highly recommended.

The **install.sh** script displays a reference to the Zimbra Public License with an address to view the license, and then reviews the installed software to verify that the prerequisite software is installed. If any is missing, the installation stops.

2. When asked to select the packages to install, install the same packages you installed on the active nodes. In our example, type **N** for the Zimbra-LDAP, and Zimbra MTA packages. Zimbra store, Zimbra SNMP, Zimbra Logger and Zimbra Spell should be marked **Y**. Press **Enter**. (Logger, Spell, and SNMP packages are optional, but if installed on the active nodes, must be installed on the standby node.)

```
Installing:
zimbra-core
zimbra-logger
zimbra-snmpp
zimbra-store
zimbra-apache
zimbra-spell
```

3. The selected packages are installed on the mailbox server. At this point, the **Main menu** displays the default entries for the mailbox server you are installing.
4. Set the LDAP host and password.
 - Type **2**, and then type the LDAP host name.
 - Type **4**, and then type the LDAP password.

As you enter each of these values, the server tries to contact the LDAP server. You can proceed when the LDAP server is successfully contacted.

5. Modify zimbra-store. Type **5** to configure the SMTP host and set the web server mode, if it is not http.
 - Type **2**, for SMTP host, and then type the Zimbra MTA host name.
 - Type **3**, if you are changing the default mode. The communication protocol options are HTTP, HTTPS, or mixed. Mixed mode uses HTTPS for logging in and HTTP for normal session traffic. All modes use SSL encryption for back-end administrative traffic.

Important: For clustering, the Web mode must be identical on all nodes.

```
Store configuration

1) Status:                               Enabled
2) SMTP host:                             smtp.example.com
3) Web server mode:                       https
4) IMAP server port:                      143
5) IMAP server SSL port:                  993
6) POP server port:                       110
7) POP server SSL port:                   995
8) Use spell check server:                yes
9) Spell server URL:                      http://
mail1.example.com:7780/aspell.php

Select, or 'r' for previous menu [r]
Checking ldap on ldap.example.com:389...Success
```

- If you installed the SNMP package, you will need to modify the default notification addresses. Type **6** to modify the SNMP packages.

Configure whether to be notified by SNMP or SMTP. The default is **No**. If you enter yes, you must enter additional information.

- For SNMP, enter the SNMP Trap host name.
- For SMTP, enter the SMTP source email address and destination email address. Type the same address as configured in the LDAP server.

```

Snmp configuration

1) Status:                               Enabled
2) Enable SNMP notifications:            yes
3) SNMP Trap hostname:                   snmptrap.com
4) Enable SMTP notifications:            yes
5) SMTP Source email address:             admin@example.com
6) SMTP Destination email address:       admin@example.com

```

- If Logger is installed, it must be disabled on all standby nodes. To disable logger, type the menu number for logger and press **Enter**.
- When you have no other changes, type **a** to apply the configuration changes. Press **Enter** after **Save configuration data?** displays.
- When **The system will be modified - continue?** appears, type **Y** and press **Enter**.
- After the **Operations logged to /tmp/zmsetup.log.xxx**, press **Enter**. The server is modified. Installing all the components and configuring the server can take a few minutes.
- When **Installation complete - press return to exit** displays, press **Enter**.

Running the Cluster Post Install Script

Now you prepare this server to be the standby server in the cluster. Start the Zimbra cluster post install script.

Note: *Unlike installation of active nodes, no SAN volumes are mounted on standby nodes prior to running the post install script.*

- Log in as **root** to the Zimbra server and **cd** to the directory where the Zimbra **zcs-cluster.tgz** file is saved. Type the following commands:
 - cd zcs-cluster** to change to the correct directory
 - ./postinstall.pl** to begin the post install. The Zimbra processes are stopped, various cluster-specific adjustments are made to the Zimbra Collaboration Suite installation, and unnecessary data files are deleted.

```
[root@node3 zcs-cluster]# ./postinstall.pl
Disabling boot-time auto start of Zimbra applications.
.... chkconfig --del zimbra

Creating cluster configuration directory
.... mkdir -p /etc/cluster

Checking node type (active vs. standby)...
This is a standby node.

.... su - zimbra -c 'zmtlscctl https 2> /dev/null'

Deleting data files
.... rm -rf /opt/zimbra/tomcat/conf
.... ln -s /opt/zimbra/conf/tomcat /opt/zimbra/tomcat/conf
.... rm -rf /opt/zimbra/tomcat/logs
.... ln -s /opt/zimbra/log/tomcat /opt/zimbra/tomcat/logs

Done.
```

Modify Zimbra LDAP and Zimbra MTA Servers for Logger Service

You must modify the syslog setup on the Zimbra LDAP server and Zimbra MTA servers.

1. On the LDAP server, as root, run `/opt/zimbra/bin/zmsyslogsetup`.
2. On the MTA server, as root, run `/opt/zimbra/bin/zmsyslogsetup`.

Configuring Red Hat Cluster for Zimbra Collaboration Suite

When all the software is installed and the Zimbra installation on the servers configured, use the Zimbra cluster configurator script to prepare Red Hat Cluster Suite to run the Zimbra Collaboration Suite. **The cluster configurator script is run on only one of the active mailbox nodes.**

The cluster configurator asks a series of questions to gather information about the cluster and generate the cluster configuration file, `/etc/cluster/cluster.conf`. This is the main configuration file of Red Hat Cluster Suite.

The cluster configurator installs the generated configuration file on each cluster node as `/etc/cluster/cluster.conf`.

Note: *The Zimbra cluster configurator should generate correct configuration file for most installations, but some cases are more complicated. For instance if you are using multiple fence devices or highly customized SAN setup, the configurator script will not work. In those cases, use the configurator to generate an initial cluster.conf. Then run the graphical Red Hat Cluster Configuration Tool, to make the necessary changes. Using the Zimbra Cluster configurator script first is recommended, because the script automates the*

steps for the basic configuration. After using the Red Hat Cluster Configuration Tool, you must manually copy the final cluster.conf file to each cluster host.

The Zimbra configurator script guides you through creating the cluster configuration file. The following is configured:

- Fence Device - This is the network power switch. Each mailbox node in the cluster is plugged into the fence device. The cluster uses the fence device for I/O fencing during a failover.
- Cluster Nodes - This section is used to add members to the cluster and configure a fence device setting for each member.
- Managed Resources - The preferred node for each service and the list of volumes to be mounted from the SAN are configured

To use the configurator script

1. To start the Zimbra configuration script, **cd** to the zcs-cluster directory created in the Installing the Zimbra Cluster Software section. Type **./configure-cluster.pl**. The configurator checks to verify that the server installation is correct.
2. All servers in the cluster must be installed before you can proceed. When **Is installation finished on all cluster nodes?** displays, type **y** to continue.
3. Enter a name to identify this cluster. Press **Enter**. Each cluster on the same network must have a distinct name.

Important: *Make sure you enter a name that is not in use! Each Red Hat Cluster Suite cluster on the same network must have a distinct name to avoid interfering with another Red Hat Cluster Suite cluster.*

```
[root@node1 zcs-cluster]# ./configure-cluster.pl

Zimbra Collaboration Suite Cluster Configurator

This script will guide you through creating an initial configuration
file for Red Hat Cluster Suite.  A series of questions will be asked
to collect the necessary information.  At the end, the configuration
data will be saved to a file and the file will be copied to all
cluster nodes, as /etc/cluster/cluster.conf on each node.

Press Enter to continue.
-----

Checking for Zimbra home... Found.
Checking for Zimbra cluster root... Found.
Checking for cluster mount points root... Found.
Checking for Red Hat Cluster Suite RPMs...
ccs-1.0.2-0
cman-1.0.2-0
dlm-1.0.0-5
fence-1.32.6-0
rgmanager-1.9.39-0
system-config-cluster-1.0.16-1.0

Installation looks good on this node.

You must finish installation on all cluster nodes before configuring
the cluster.  Is installation finished on all cluster nodes? (Y/N) y
-----

Each Zimbra cluster on the network must have a unique name.
Enter the cluster name:zimbra-cluster
```

4. Select the network power switch type that is used as the fence device.
Configure the fence device host name/IP address, login, and password.

```
A fence device is needed by the cluster for I/O fencing during a
failover. The power cord of each cluster node must be plugged into an
APC or WTI network power switch device, and the cluster will control
the power switch to reboot the node being fenced. While Red Hat
Cluster Suite supports a variety of fence devices, for the purpose of
this configuration process assume you are using APC or WTI, and also
assume all nodes are plugged into a single device. If you are using
a different fence device or more than one device, you can correct the
generated configuration file later with the system-config-cluster GUI
tool.

Choose device vendor:
  1) APC
  2) WTI
Choose from above (1-2): 1
Enter fence device hostname/IP address: apc.example.com
Enter fence device login [apc]:
Enter fence device password: <password>
```

5. Enter the fully-qualified hostname for each of the nodes in the cluster and the plug number associated with the node's power cord. When all the nodes are identified, type **Done**.

```
For each cluster node you must provide its fully-qualified hostname
and the plug number on the fence device.
```

```
Enter node hostname ("done" if no more): node1.example.com
Enter fence device plug number for node1.example.com: 1
```

```
Enter node hostname ("done" if no more): node2.example.com
Enter fence device plug number for node2.example.com: 2
```

```
Enter node hostname ("done" if no more): node3.example.com
Enter fence device plug number for node3.example.com: 3
```

```
Enter node hostname ("done" if no more): done
```

6. Next, you select the cluster service, the preferred node for that service, and the volume set-up to be mounted from the SAN.

Note: You can place all service data on a single volume or chose to place the service data in eight volumes. Single volume is recommended for testing environments only. A more customized volume configuration is possible, but the configurator script only supports single- or eight-volume volume sets. This is a limitation of the configurator script, not of Zimbra Collaboration Suite or of Red Hat Cluster Suite.

```
For each service you need to choose a preferred node to run on, and
enter the list of volumes to be mounted from the SAN.
```

```
Choose a service:
  1) mail1.example.com
  2) mail2.example.com
  3) Done
Choose from above (1-3): 1
```

```
Choose preferred node on which to run service mail1.example.com:
  1) node1.example.com
  2) node2.example.com
  3) node3.example.com
Choose from above (1-3): 1
```

```
A Zimbra cluster service must mount service-specific data volumes.
Two choices are provided in this configuration process. All service
data can be placed on a single volume, or multiple volumes can be
used for different types of data files. In the multiple-volumes case
eight volumes are used per service.
```

```
Choose volume setup type:
  1) single volume
  2) multiple volumes
Choose from above (1-2): 2
```

7. A prompt is displayed for each volume in the service's volume set. Enter the SAN volume device name for the mount point in the prompt. (These names are the volumes defined when you created the 8 volumes on the SAN as described in [“Preparing the SAN” on page 42.](#))

```
1. Configuration directory:
Volume mail1.example.com-conf:
  mount point = /opt/zimbra-cluster/mountpoints/mail1.example.com/
  conf
  Enter device name: /dev/sdb5
2. Log directory:
Volume mail1.example.com-log:
  mount point = /opt/zimbra-cluster/mountpoints/mail1.example.com/log
  Enter device name: /dev/sdb6
3. Redolog directory:
Volume mail1.example.com-redolog:
  mount point = /opt/zimbra-cluster/mountpoints/mail1.example.com/
  redolog
  Enter device name: /dev/sdb7
4. MySQL data directory:
Volume mail1.example.com-db-data:
  mount point = /opt/zimbra-cluster/mountpoints/mail1.example.com/db/
  data
  Enter device name: /dev/sdb8
5. Message store directory:
Volume mail1.example.com-store:
  mount point = /opt/zimbra-cluster/mountpoints/mail1.example.com/
  store
  Enter device name: /dev/sdb9
6. Search index directory:
Volume mail1.example.com-index:
  mount point = /opt/zimbra-cluster/mountpoints/mail1.example.com/
  index
  Enter device name: /dev/sdb10
7. Backup directory:
Volume mail1.example.com-backup:
  mount point = /opt/zimbra-cluster/mountpoints/mail1.example.com/
  backup
  Enter device name: /dev/sdb11
8. Logger MySQL data directory:
Volume mail1.example.com-logger-db-data:
  mount point = /opt/zimbra-cluster/mountpoints/mail1.example.com/
  logger/db/data
  Enter device name: /dev/sdb12
```

8. Continue to configure the preferred nodes and the volume sets for the remaining cluster services.
9. When finished choosing the services, select **Done**. Press **Enter**, and then press **Enter** again to view a summary of the configuration.

```
Finished collecting information.
Press Enter to view summary of the configuration.

Configuration Summary
-----

Cluster Name: example-cluster

Fence Device:
  name:   fence-device
  agent:  fence_apc
  ipaddr: apc.example.com
  login:  apc
  passwd: <password>

Nodes:
  node1.example.com - fence port 1
  node2.example.com - fence port 2
  node3.example.com - fence port 3

Services:
.
.mail1.example.com
  ipaddr: 000.000.000.000
  preferred node: node1.example.com
  volumes:
    mail1.example.com-conf
    mountpoint: /opt/zimbra-cluster/mountpoints/
.
.
.
-----

About to save configuration file.
Enter filename [/tmp/cluster.conf.19003]:
-----
```

10. After viewing the summary, save the configuration to a file. You can either accept the default or rename the configuration file.

Note: If you made a mistake, press **Ctrl-C** to abort the configurator script and start over.

Copying the files to all cluster nodes

The configuration file must now be copied to all cluster nodes. The Zimbra configurator script can copy the files, or you can do it manually. This is a continuation of the configurator script.

11. The script offers to do the copy via scp. To automatically copy the **cluster.conf** file to all nodes, type **y**. Enter the root password of each node when asked.

```
Cluster configuration saved in /tmp/cluster.conf.17815
This file must be copied to all cluster nodes now. This script can
do it for you using scp, or you can do it manually.
Copy to all cluster nodes using scp? (Y/N) y

Copying /tmp/cluster.conf.17815 to node1.example.com:/etc/cluster/
cluster.conf ... scp /tmp/cluster.conf.17815
root@node1.example.com:/etc/cluster/cluster.conf
root@node1.example.com's password:
cluster.conf.17815                100% 5439      5.3KB/s
00:00

Copying /tmp/cluster.conf.17815 to node2.example.com:/etc/cluster/
cluster.conf... scp /tmp/cluster.conf.17815 root@node2.example.com:/
etc/cluster/cluster.conf
root@node2.example.com's password:
cluster.conf.17815                100% 5439      5.3KB/s
00:00

Copying /tmp/cluster.conf.17815 to node3.example.com:/etc/cluster/
cluster.conf... scp /tmp/cluster.conf.17815 root@node3.example.com:/
etc/cluster/cluster.conf
root@node3.example.com's password:
cluster.conf.17815                100% 5439      5.3KB/s
00:00

Configuration generated and pushed to all cluster nodes.

If necessary, use system-config-cluster GUI tool to further customize
the cluster configuration. You must manually copy the updated
cluster.conf to all nodes.

Press Enter to continue.
```

Important: Use the Red Hat Cluster Configuration Tool if you want to further customize the cluster configuration after the configuration file is generated and copied to all cluster nodes. If you customize the configuration file, you must then manually copy the updated cluster.conf to all nodes.

Start the Red Hat Cluster Suite Daemons

After the cluster configuration file is copied to every node, you can start the Red Hat Cluster Suite daemons.

Important: In order to start the cluster daemons correctly, you must be logged on to each node before proceeding, and to see any errors, you should have two sessions open for each node. In our example, you would have six screens opened. You enter a command for one node, then enter the same command for the second, and so forth. You must enter each command on all nodes, before proceeding to the next command.

- Log on to each node as root.
- Run **tail -f /var/log/messages**, on each node to watch for any errors.

- Open another session for each node.

To start the Red Hat Cluster Service on a member, type the following commands in this order. Remember to enter the command on all nodes before proceeding to the next command.

1. **service ccsd start**. This is the cluster configuration system daemon that synchronizes configuration between cluster nodes.
2. **service cman start**. This is the cluster heartbeat daemon. The command may not complete on all nodes immediately. It returns when all nodes have established heartbeat with one another.
3. **service fenced start**. This is the cluster I/O fencing system that allows cluster nodes to reboot a failed node during failover.
4. **service rgmanager start**. This manages cluster services and resources.

The **service rgmanager start** command returns immediately, but initializing the cluster and bringing up the Zimbra Collaboration Suite application for the defined cluster services may take some time.

After all commands have been issued on all nodes, run **clustat** command on one node, to verify all cluster services have been started.

Continue to enter the **clustat** command, until it reports all nodes have joined the cluster, and all services have been started.

Because nodes may not join the cluster in sequence, some of the services may start on nodes that are different from the configured preferred nodes. This is expected and eventually will be restarted on the configured preferred node.

When clustat shows all services are running on the preferred nodes, the cluster configuration is complete.

What to do if cluster services does not relocate to preferred node

If the services does not relocate to the preferred nodes after several minutes, you can issue Red Hat Cluster Suite utility commands to manually correct the situation.

Note: *Not starting correctly on the preferred nodes usually is an issue that happens only the first time the cluster is started.*

For each cluster service that is not running on the correct preferred node, run **clusvcadm -d <cluster service name>**, as root on one of the cluster nodes.

```
[root@node1.example.com]#clusvcadm -d mail1.example.com
```

This disables the service by stopping all associated Zimbra processes, releasing the service IP address, and unmounting the service's SAN volumes.

To enable a disabled service, run **clusvcadm -e <service name> -m <node name>**. This command can be run on any cluster node. It instructs the specified node to mount the SAN volumes of the service, bring up the service IP address, and start the Zimbra processes.

```
[root@node1.example.com]#clusvcadm -e mail1.example.com -m
node1.example.com
```

Testing the Cluster Set up

To perform a quick test to see if failover works:

1. Log in to the remote power switch and turn off an active mailbox node.
2. To watch the standby node take over the failed service, run **clustat**, on one of the other nodes.
3. Run **tail -f /var/log/messages**. You will observe the cluster becomes aware of the failed node, I/O fence it, and bring up the failed service on a standby node.

View Zimbra Cluster Status

Go the Zimbra administration console to check the status of the Zimbra cluster. The **Server Status** page shows the cluster server, the node, the services running on the cluster server, and the time the cluster was last checked. The standby nodes are displayed as standby. If a service is not running, it is shown as disabled. Managing and maintaining the Zimbra Cluster is through the Red Hat Cluster Manager.

System Requirements for Zimbra Collaboration Suite 4.0

Zimbra Collaboration Suite system requirements for both the Network Edition and the Open Source Edition.

Requirements	
Servers	<i>Evaluation and Testing</i> <ul style="list-style-type: none">• Intel/AMD 32-bit CPU 1.5 GHz• 1 GB RAM• 5 GB free disk space for software and logs• Additional disk space for mail storage <i>Production environments</i> <ul style="list-style-type: none">• Intel/AMD CPU 32-bit 2.0 GHZ+• Minimum - 2 GB RAM Recommend - 4 GB• 10 GB free disk space for software and logs (SATA or SCSI for performance, and RAID/Mirroring for redundancy)• Additional disk space for mail storage <p>Note: RAID-5 is not recommended for installations with more than 100 accounts.</p>
Mac Server	<i>Evaluation and Testing</i> <ul style="list-style-type: none">• PPC Mac (G4 or better), Intel Core Solo, or Intel Core Duo*• 1 GB RAM• 5 GB free disk space for software and logs• Additional disk space for mail storage

<p>Mac Server (continued)</p>	<p><i>Production environments</i></p> <ul style="list-style-type: none"> • PPC Mac (G5 or better), Intel Core Solo, or Intel Core Duo* • Minimum - 2 GB RAM Recommend - 4 GB • 10 GB free disk space for software and logs • Additional disk space for mail storage <p>*There are known issues using ZCS on Macs with the Intel Core Duo. See the Release Note.</p>
<p>Operating System Network Edition</p>	<ul style="list-style-type: none"> • Red Hat® Enterprise Linux®, AS/ES version 4. (32-bit, 64-bit) For clustering, version 4, update 3 is required. The operating system must be configured as described in this guide. • Mac OS® X 10.4.7 <p>Note: Max OS X server installs, the following features are not included: attachment indexing/search, view attachments as HTML, clustering.</p> <ul style="list-style-type: none"> • SUSE ES 9 (32-bit) <p>Note: SUSE server installs, the following features are not included: clustering</p>
<p>Operating System Open Source Edition</p>	<p>In addition to supporting the operating systems listed above for the Network Edition, other OS versions are available for the Open Source Edition. Check the Zimbra Open Source Downloads page on www.zimbra.com.</p>

<p>Other Dependencies</p>	<p>For Red Hat Enterprise, Fedora Core and SuSE operating systems, the server must also have the following installed:</p> <ul style="list-style-type: none"> • NPTL. Native POSIX Thread Library • Sudo. Superuser, required to delegate admins. • libidn. For internationalizing domain names in applications (IDNA) • cURL. A command line tool for transferring files with URL syntax • fetchmail. A remote-mail retrieval and forwarding utility used for on-demand TCIP/IP links. • GMP. GNU Multiple-Precision Library. • compat-libstdc++-33. Compatibility Standard C++ libraries. NOTE: The 32-bit version of the compat-libstdc rpm package is required for both 32-bit or 64-bit servers. • For Red Hat Enterprise only: compat-libstdc++-296
	<p>For Mac servers, Java 1.5 must be installed as the default Java.</p>
<p>Miscellaneous</p>	<ul style="list-style-type: none"> • SSH client software to transfer and install the Zimbra Collaboration Suite software. • Valid DNS configured with an A record and MX record • Servers should be configured to run Network Time Protocol (NTP) on a scheduled basis
<p>Administrator Computers *These OS configurations have been tested and are known to work. Other configurations may work.</p>	<ul style="list-style-type: none"> • Windows XP with either Internet Explorer 6.0 SP 2 or Firefox 1.5 • Macintosh OS X 10.4 with Firefox 1.5

End User Computers using Zimbra Web Client *These OS configurations have been tested and are known to work. Other configurations may work.	Minimum <ul style="list-style-type: none">• Intel/AMD/Power PC CPU 750MHz• 256MB RAM Recommended <ul style="list-style-type: none">• Intel/AMD/Power PC CPU 1.5GHz• 512MB RAM Operating system/ browser combinations <ul style="list-style-type: none">• Windows XP with either Internet Explorer 6.0 SP 2 or Firefox 1.5• Fedora Core 4 with Firefox 1.5• Mac OS X 10.4 with Firefox 1.5 or Safari 2.0.4 (Beta)
End User Computers Using Other Clients *These OS configurations have been tested and are known to work. Other configurations may work.	Minimum <ul style="list-style-type: none">• Intel/AMD/Power PC CPU 750MHz• 256MB RAM Recommended <ul style="list-style-type: none">• Intel/AMD/Power PC CPU 1.5GHz• 512MB RAM Operating system POP/IMAP combinations <ul style="list-style-type: none">• Windows XP with either Outlook Express 6 , Outlook 2003 (MAPI), or Thunderbird 1.0.7• Fedora Core 4 with Thunderbird 1.0.7• Mac OS X 10.4 with Apple Mail
Monitor	Display minimum resolution 1024 x 768
Internet Connection Speed	128 kbps or higher

Migration Wizard Requirements

Accounts from Microsoft Exchange 2000, 2003 and 5.5 can be migrated to Zimbra Collaboration Suite

Import Wizard Requirements

Contents of a .pst file from accounts using Microsoft® Outlook® 2003 can be imported to accounts on the Zimbra server.

Zimbra Mobile for Network Edition only

Zimbra Mobile provides mobile data access to email, calendar, and contacts for users of selected mobile phones.

Zimbra Mobile supports native synchronization with the following devices at a Beta quality level.

- Treo™ 650 , Treo 700p
- Windows Mobile 5 devices

Zimbra Mobile supports synchronization with the following devices via “Mail for Exchange”.

- Symbian S60/S80 smart devices such as Nokia E Series

Zimbra Mobile supports synchronization with BlackBerry devices via certified third-party partner solutions.

Rev 9/20/06

Index

A

administration console, logging on 33
administration console, URL 33

C

certificate authority 33
class of service 33
configuration options 12
configure proxy server 17
contact Zimbra 6

D

DNS 10
download software 12

F

feedback 6
firewall, Red Hat 9
forums, join Zimbra 6
FQDN 10

I

IMAP proxy server 17
installation on Mac servers 23
installation process 21

J

Java 1.5, setting default on Mac server 10

L

LDAP replication 35
LDAP replication, configuring 40
LDAP replication, install 37
LDAP replication, setting up 39
LDAP server configuration 14
LDAP server, install 24
LDAP server, LDAP replication install 35
license 5
license, extended trial 5
load balancing on ZCS 18
logger package 17

M

mailbox server configuration 15
mailbox server, install 26
menu - main, description 13
modify Red Hat Enterprise OS 8
MTA Auth host 30
MTA server configuration 16
MTA server, install 29
MX record 10

O

overview of Zimbra packages 11

P

perdition 17
POP proxy server 17
port configurations, default 15
port mapping for IMAP/POP proxy server 18
post installation tasks 32

R

relay host 10

S

Sendmail, disable 10
server configuration, verify 32
SNMP, install 31
software agreement 22
spam training filter 15
spell checker, install 17
support, contact Zimbra 6
system requirements 7

T

trial license 5

U

URL, administration console 33

V

virtual hosting 18

Z

Zimbra packages 11
zmcontrol status 32