Zimbra™ Collaboration Suite Multi-Server Installation Guide

Release 6.0

Open Source Edition

October 2009

Legal Notices

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@porcupiine.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 a Yahoo! Company
701 First Avenue
Sunnyvale, California 94089 USA
408.349.3000
www.zimbra.com

September 2009 ZCS 6.0

Rev 1(6.0.2) 10/2/2009

Table of Contents

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

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.

For More Information

Zimbra documentation, including a readme text file, the administration guide, and other Zimbra guides are copied to the servers during the installation. The major documentation types are listed below. You can access all the documents on the Zimbra website, www.zimbra.com and from the administration console, Help Desk page.

- **Administrator's Guide**. This guide describes product architecture, server functionality, administration tasks, configuration options, and backup and restore procedures.
- **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 Guides**. These guide describes how to migrate users that are on Microsoft Exchange or Lotus Domino systems to the Zimbra Collaboration Suite.

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 configuration 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. 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 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 Jetty, 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 and is installed on one mailbox server. The Zimbra Logger installs tools for syslog aggregation and reporting. If you do not install Logger, the server statistics the server statistics section of the administration console will not display.

  Note: *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.
- **Zimbra Apache**. This package is installed automatically when Zimbra Spell is 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.

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	• Zimbra LDAP and Zimbra message store on one server • Zimbra MTA on a separate server. • Possibly include additional Zimbra MTA servers	• Zimbra LDAP on one server • Multiple Zimbra mailbox servers • Multiple Zimbra MTA servers	• Zimbra Master LDAP server • Replicas LDAP servers • Multiple Zimbra mailbox servers • Multiple Zimbra MTA servers

Downloading the Zimbra Software

For the latest Zimbra software download, go to 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 Migration Wizard for Exchange** .exe file to migrate Microsoft® Exchange server email accounts to the Zimbra server.
- **Zimbra Collaboration Suite Migration Wizard for Domino** .exe file to migrate Lotus Domino 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.

Supporting documentation can be found on the administration console Help Desk page or at www.zimbra.com.

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.

Common configuration options

The packages installed in common configuration include libraries, utilities, monitoring tools, and basic configuration files under Zimbra Core. These options are configured on all servers.

The table below describes the Main menu common configuration options.

Main Menu Options

Server Configured	Main Menu	Description
Common Configuration		
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 Admin password	Password for the Zimbra admin user and is configured on every server

Main Menu Options

Server Configured	Main Menu	Description
All	TimeZone	Select the time zone to apply to the default COS. The time zone that should be entered is the time zone that the majority of users in the COS will be located. The default time zone is PST (Pacific Time)
All	Require secure interprocess communications	By default startTLS is **YES**. When startTLS is enabled there is a secure communication between amavis and postfix and the LDAP server If this is disabled, ZCS disables the use of startTLS with the LDAP server
All servers, if installed	zimbra-snmp Installing SNMP is optional, but if installed it must be on all servers.	You can modify the following options • **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.
	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.

Zimbra LDAP server configuration options

These options are configured on the Zimbra LDAP server.
The table below describes the Main menu LDAP server configuration options

Zimbra LDAP Server Menu Options

Zimbra LDAP Server	zimbra-ldap	Configuration includes the following: • **Status** - Enabled. For replica LDAP servers the status is changed to Disabled. • **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 here. • **LDAP Root password**. This password is automatically generated and is used for internal LDAP operations. • **LDAP Replication password**. This password is automatically generated and is the password used by the LDAP replication server and must be the same password on the LDAP master server and on the replica server.

Zimbra LDAP Server	zimbra-ldap	• **LDAP Postfix password**. This password is automatically generated and is the password used by the postfix user to identify itself to the LDAP server and must be the same password on the LDAP master server and on the MTA server. • **LDAP Amavis password**.This password is automatically generated and is the password used by the amavis user to identify itself to the LDAP server and must be the same password on the LDAP master server and on the MTA server. •

Zimbra Mailbox server configuration options

These options are configured on the Zimbra Mailbox server.

The table below describes the Zimbra Mailbox server menu options

Zimbra Mailbox Server Menu Options

Zimbra Mailbox Server	zimbra-store	Configuration includes the following. • **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]. You may want to change this to your domain address. • **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. • By default, the automated spam training filter is enabled and two mail accounts are created. ***1 -Spam Training User*** to receive mail notification about mail that was not marked as junk, but should be. ***2 -Non-spam (HAM) training*** *user* to receive mail notification about mail that was marked as junk, but should not have been. 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. The spam training filter is automatically added to the cron table and runs daily.

Zimbra Mailbox Server Menu Options

Zimbra Mailbox Server	zimbra-store (continued)	• **Global Document Account** — This account is automatically created when ZCS is installed. The account holds the templates and the default Documents Notebook. The Documents feature is enabled from the COS or in individual accounts. These default port configurations are shown. • **SMTP host** • **Web server HTTP port**:- 80 • **Web server HTTPS port**: - 443 • **Web server mode** - Can be HTTP, HTTPS, Mixed, Both or Redirect. **Mixed** mode uses HTTPS for logging in and HTTP for normal session traffic **Both** mode means that an HTTP session stays HTTP, including during the login phase, and an HTTPS session remains HTTPS throughout, including the login phase. **Redirect** mode redirects any users connecting via HTTP to a HTTPS connection. All modes use SSL encryption for back-end administrative traffic. • **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
		•

Zimbra Mailbox Server Menu Options

Zimbra mailbox server	zimbra-logger	The Logger package is installed on the one mail server. 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 reporting.
Zimbra mailbox server	Default Class of Service Configuration	This menu lists major new features for the ZCS release and whether feature are enabled or not. When you change the feature setting during ZCS installation, you change the default COS settings.
Zimbra mailbox server	zimbra-spell	If installed, it is automatically enabled. When composing messages in the Zimbra Web Client, spell check can be run.
Zimbra mailbox server	zimbra-apache	When you install zimbra-spell, zimbra-apache gets installed automatically.

Zimbra MTA Server configuration options

Zimbra MTA server configuration involves installation of the Zimbra-MTA package. This also includes anti-virus and anti-spam components.

The table below describes the MTA server menu options

Zimbra MTA Server Menu Options

Zimbra MTA Server	zimbra-mta	The following options can be modified. • **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.* • **Bind password for postfix LDAP user**. This password must be the same as the postfix password configured on the master LDAP server. • **Bind password for amavis LDAP user**. This password must be the same as the amavis password configured on the master LDAP server.

Note: *New installs of ZCS limit spam/ham training to the first MTA installed. If you uninstall or move this MTA, you will need to enable spam/ham training on*

another MTA, as one host should have this enabled to run zmtrainsa --cleanup. To do this set **zmlocalconfig -e zmtrainsa_cleanup_host=TRUE**.

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.

Chapter 3 Preparing Your Server Environment

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

- 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 6.0 at the end of this guide.

Important: *The operating system that you use should be at the current patch level before you install ZCS. See the latest release notes for a list of the operating systems patches that have been tested with ZCS.*

Modifying Operating System Configurations

Configuration modifications for two of the most frequently used operating systems, Red Hat Enterprise Linux and Fedora, are described in this guide. The SUSE configuration would be similar to those described for the Red Hat Enterprise Linux. The MAC OS X requires no additional modifications.

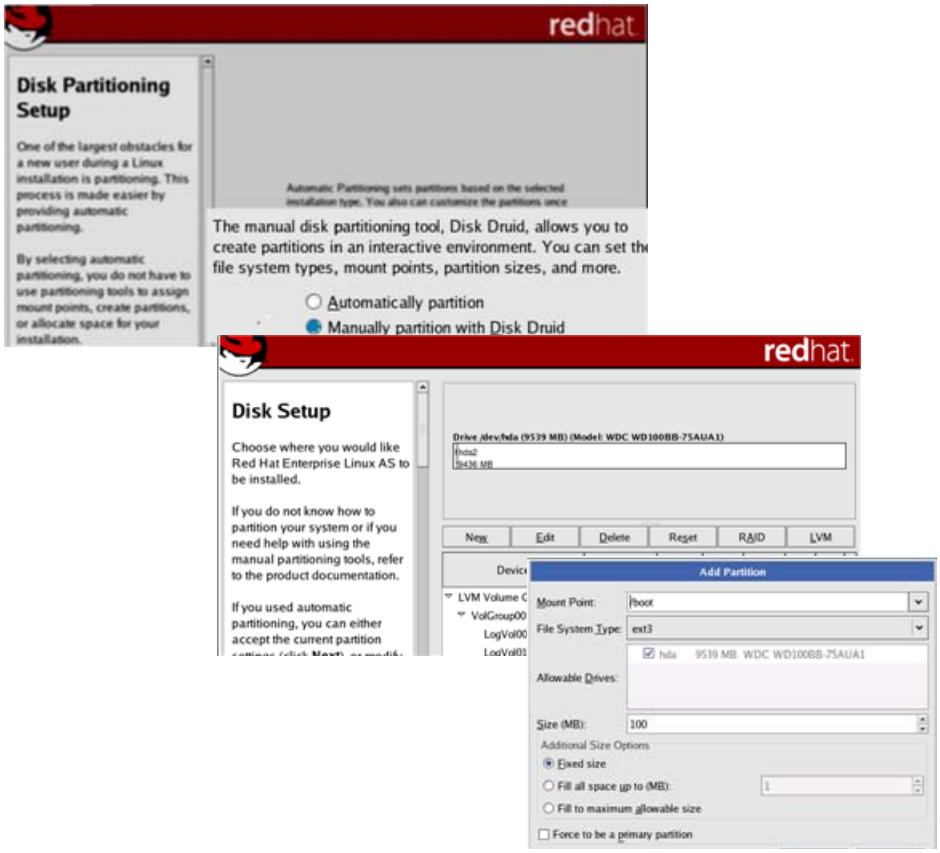
Other operating systems may require similar modifications, use this information as a reference to gauge whether your operating system may need to be modified. Also, search the Zimbra forums.

Installation Modifications for Red Hat Enterprise Linux

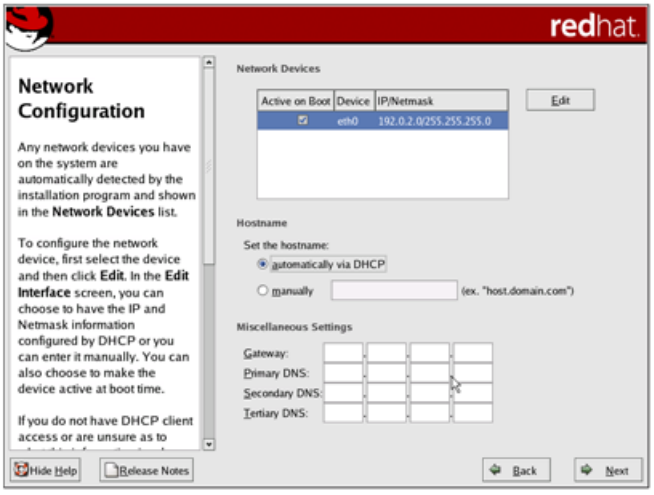
The Zimbra Collaboration Suite runs on the Red Hat Enterprise Linux,AS/AE 4 or 5 operating system. When you install the Red Hat software for the Zimbra Collaboration Suite, accept the default setup answers to install the minimum configuration, except for the following steps that must be modified.

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

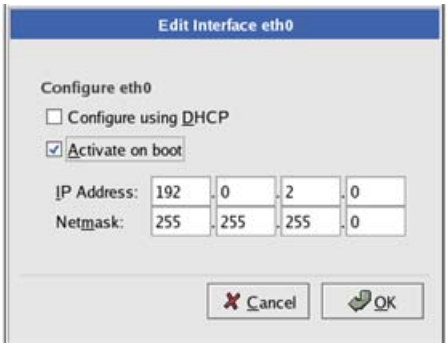
- **Disk Partitioning Setup**. Check **Manually partition with DiskDruid**. The disk partition should be set up as follows:
  - The **Mount Point/RAID Volume** size for the **/boot** partition should be 100 MB.
  - The **Swap** partition should be set to twice the size of the RAM on your machine.
  -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



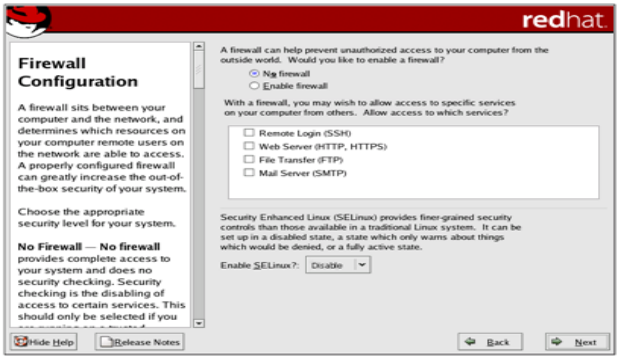
- **Network Configuration>Network Devices>Hostname** should be configured manually with the hostname [*mailhost.example.com]* of the Zimbra server.



- 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.*

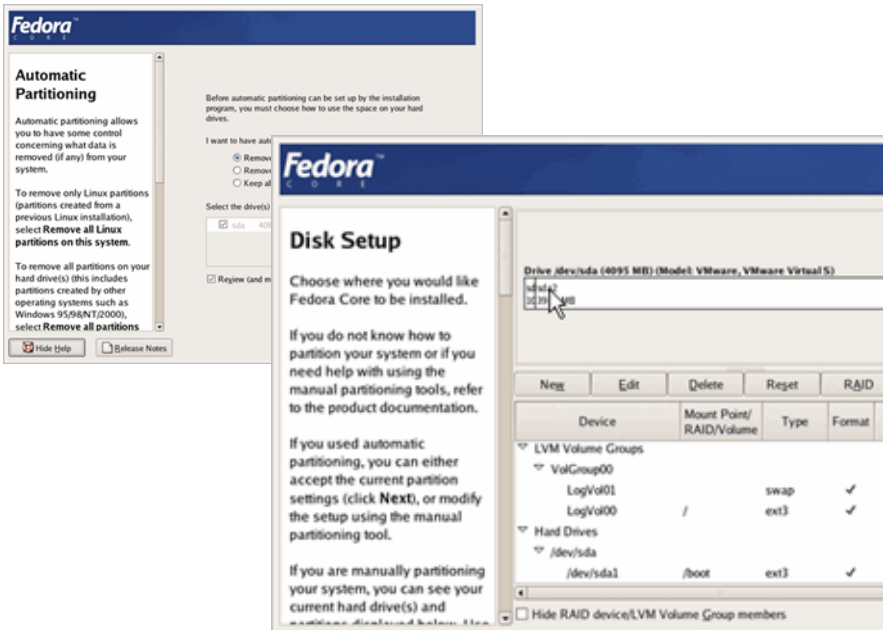
- You must disable Sendmail in order to run the Zimbra Collaboration Suite. Disable the Sendmail service with these commands, **chkconfig sendmail off, service sendmail stop.**
- A fully qualified domain name is required. Make sure that the FQDN entry in **/etc/hosts** appear before the hostnames. If 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 Modifications for Fedora

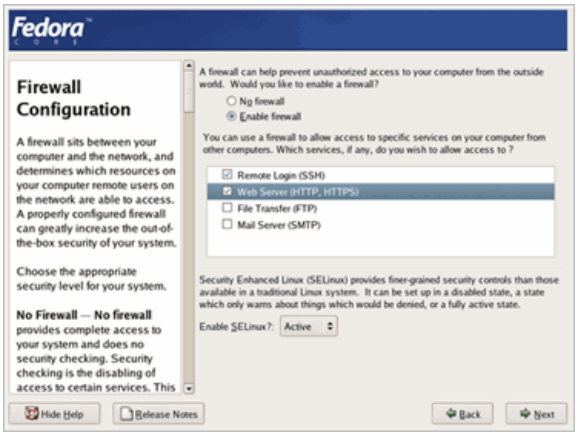
The Zimbra Collaboration Suite runs on the Fedora, Core 4 operating system. When you install the Fedora software for the Zimbra Collaboration Suite, accept the default setup answers, except for the following steps. Refer to the Fedora installation guide for detailed documentation about installing their 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 name [*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 application. The Sendmail command to stop the service is **/etc/init.d/sendmail stop**, to disable, is **chkconfig sendmail off**. The Postfix command to stop the service is **/etc/init.d/postfix stop**, to disable, is **chkconfig postfix stop**.
- Make sure that 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**

Linux File System Setup

The **ext3** file system is supported for Linux deployments. The file system should be mounted with the **noatime** option set.

The ext3 file system should have **dirsync** enabled. The zimbra mailbox server uses fsync(2) as necessary to ensure that data in the files are flushed from buffers to disk. That is, when an incoming message is received, fsync is called on the blob store message file before the MTA is given an acknowledgment that the message was received or delivered by the mailbox server.

However, when the Zimbra mailbox server or MTA creates new files, such as during message delivery, the update to the directory containing the file must be flushed to disk. Even if the data in the file is flushed with fsync, the file entry in the directory might be lost if the server crashed before the directory update is flushed to disk.

With the ext3 file system, to have directory updates be written to disk automatically and atomically, there are two options

- Add dirsync to the list of mount options, or
- Update directory attributes by running **chattr +D dir** on all the relevant directories.

If you are doing this for the first time, consider running **chattr -R +D** to recursively update a whole tree of directories; future sub-directories inherit the attribute from the parent directory. Zimbra recommends dirsync be enabled for all blob stores, Lucene search index directories, and MTA queues.

The following options are a guidelines for when creating an ext3 file system with the **mke2fs** command. Refer to ext3 documentation.

***Caution**: Running mke2fs will wipe **all** data from the partition. Make sure that you create the file system in the correct partition.*

-j	Create the file system with an ext3 journal.
-L SOME_LABEL	Create a new volume label. Refer to the labels in /etc/fstab.
-O dir_index	Use hashed b-trees to speed up lookups in large directories.
-m 2	Only 2% needs to be reserved for root on large file systems.
-i	For message store, option -i should be the expected average message size. Estimate this conservatively as the number of inodes can not be changed after creation.
-J size=400	Create a large journal.
-b 4096	Block size in bytes.
-R stride=16	Stride is used to tell the file system about the size of the RAID configuration. Stride * block size should be equal to RAID stripe size. Fopr example 4k blocks, 128k RAID stripes would set stride=32.

***Note:** For large ZCS deployments, see the Zimbra wiki, Performance Tuning Guidelines for Large Deployments article.*

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 4 Multiple-Server Installation

The multiple-server installation is straight-forward and easy to run. You run the same install script on each server, select the component(s) to install, and use the menu to configure the system.

After the installation is complete, two additional steps should be run as described in **“Final Set-Up” on page 42**:

- Fetch the ssh encryption keys
- Enable some logger functionality.

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.*

Important: *Before you start, verify that the system clocks are synced on all servers.*

Starting the Installation Process

For the latest Zimbra software download, go to www.zimbra.com. Save the Zimbra Collaboration Suite **tar** file to the computer from which you are installing the software.

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 29**.

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 filename]** to change to the correct directory. The file name includes the release and build date.
   - **./install.sh** to begin the installation.

   Note:

   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/packages/
zcs/packages/zimbra-spell-6.0.0_xx_1_5469.RHEL4-4116.i386.rpm
zcs/packages/zimbra-apache-6.0.0_xx_5469.RHEL4-4116.i386.rpm
zcs/packages/zimbra-core-6.0.0_xx_5469.RHEL4-4116.i386.rpm
zcs/packages/zimbra-logger-6.0.0_xx_5469.RHEL4-4116.i386.rpm
zcs/packages/zcs-cluster-6.0.0_GA_1469.RHEL4.tgz
zcs/packages/zimbra-cms-6.0.0_xx_5469.RHEL4-4116.i386.rpm
zcs/packages/zimbra-ldap-6.0.0_xx_5469.RHEL4-4116.i386.rpm
zcs/packages/zimbra-store-6.0.0_xx_5469.RHEL4-4116.i386.rpm
zcs/packages/zimbra-mta-6.0.0_xx_5469.RHEL4-4116.i386.rpm
zcs/packages/zimbra-snmp-6.0.0_xx_5469.RHEL4-4116.i386.rpm
zcs/README.txt
zcs/readme_binary.txt
zcs/docs/
.
.
.
[root@mailhost tmp]# cd zcs-NETWORK-6.0.0_XX_5469.RHEL4.4116
[root@mailhost zcs-NETWORK-6.0.0_xx_5469.RHEL4.4116]# ./install.sh

Operations logged to /tmp/install.log.27584
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 Zimbra software agreement is displayed and includes a link to the license terms for the Zimbra Collaboration Suite. Read the agreement and press **Enter** to continue.

```
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
```

4. 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 again.

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 you if would like to change the hostname. The domain name should have an 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 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. The welcome screen appears, click **Continue**.

3. The Zimbra Software License Agreement is displayed. Read the agreement and click **Continue**. A popup screen appears asking you to accept the terms of the license agreement to continue. Click **Agree**.

4. Select the destination volume to install the software. Click **Continue**.

5. The **Easy Install ...** dialog displays. Select the 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 7 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 in 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 under **“Starting the Installation Process” on page 27**.

Installing Zimbra LDAP Master Server

You must configure the Zimbra Master LDAP server before you can install other Zimbra servers. You can set up LDAP replication, configuring a master LDAP server and replica LDAP servers, either configuring all LDAP servers now or after you set up the initial ZCS servers. See Chapter 5, Configuring LDAP Replication.

1. Follow steps 1 through 4 in **“Starting the Installation Process” on page 27** to open an SSH session to the LDAP server, log on to the server as **root**, and unpack the Zimbra software.
2. Type **Y** and press **Enter** to install the **zimbra-ldap** package. The MTA, Store and Logger packages should be marked **N**. In the following screen shot example, the package to be installed is emphasized.

   Note: *If SNMP is being used, the SNMP package is installed on every Zimbra server. Mark* **Y***.*

```
Select the packages to install

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


Installing:
    zimbra-core
    zimbra-ldap

This system will be modified. Continue [N} Y
```

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

   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 (*).

   To navigate the Main menu, select the menu item to change. You can modify any of the values. See **Table , “Main Menu Options,” on page 9** for a description of the Main menu.

```
Main menu

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

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

4. Type **1** to display the **Common Configuration** submenus.

```
Common Configuration:
    1)Hostname:                          ldap-1.example.com
    2)Ldap master host:                  ldap-1.example.com
    3)Ldap port:                            389
    4)Ldap Admin password:                  set
    5)Require secure interprocess communications      Yes
    6)TimeZone:              (GMT-08.00) Pacific Time (US & Canada)
```

5. Type **4** to display the automatically generated LDAP admin password. You can change this password. Write down the LDAP password, the LDAP host name and the LDAP port. You must configure this information when you install the mailbox servers and MTA servers.

   LDAP Admin Password _____

   LDAP Host name _____

   LDAP Port _____

6. Type **6** to set the correct time zone, if your time zone is not Pacific Time.

7. Type **r** to return to the Main menu.

8. From the Main menu, type **2** -**zimbra-ldap** to view the **Ldap configuration** settings.

```
Ldap configuration

   1) Status:                                  Enabled
   2) Create Domain:                           yes
   3) Domain to create                         ldap-1.example.com
   4) Ldap Root password:                      set
   5) Ldap Replication password:               set
   6) Ldap Postfix password:                   set
   7) Ldap Amavis password:                    set
   8) Ldap Nginx password:                     set

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

Create Domain: [ldap-1.example.com] example.com
```

   - Type **3, Domain to create,** to change the default domain name to the domain name, (example.com).
   - The passwords listed in the LDAP configuration menu are automatically generated. You need these passwords when configuring the MTA and the LDAP replica servers. Write them down. If you want to change the passwords for LDAP root, LDAP replication, LDAP Postfix, LDAP Amavis, and LDAP Nginx, enter the corresponding number 4 through 8 and change the passwords.

     LDAP Replication password _____

     LDAP Postfix password _____

     LDAP Amavis password _____

     LDAP Nginx password _____

9. When changes to the LDAP configuration menu are complete, enter **r** to return to the main menu. Type **a** to apply the configuration changes.

10. When **Save Configuration data to file** appears, type **Yes** and press **Enter**.

11. The next request asks where to save the files. To accept the default, press **Enter**. To save the files to another directory, enter the directory and press **Enter**.

12. 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. This includes but is not limited to setting local config values, creating and installing SSL certificates, setting passwords, timezone preferences, and starting the servers, among other processes.

13. When **Configuration complete - press return to exit** displays, press **Enter**.

```
Select, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes]
Save config in file: [/opt/zimbra/config.5490]
Saving config in /opt/zimbra/config.5490...done

The system will be modified - continue? [No] y

Operations logged to /tmp/zmsetup.10282008-092627.log
Setting local config values...done
.
.
.
Operations logged to /tmp/zmsetup.log.2843

Configuration complete - press return to exit
```

The installation of the LDAP server is complete.

Installing Zimbra Mailbox Server

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

Note: *The zimbra-logger package is installed only on the first Zimbra mailbox server.*

Note:

1. Follow steps 1 through 4 in **"Starting the Installation Process" on page 27** to log on to the server as **root** and unpack the Zimbra software.

2. Type **Y** and press **Enter** to install the **zimbra-logger** (optional and only on one mailbox server), **zimbra-store**, and **zimbra-spell** (optional) packages. When zimbra-spell is installed, the **zimbra-apache** package also gets installed. In the following screen shot example, the packages to be installed are emphasized.

   Note: *If SNMP is being used, the SNMP package is installed on every Zimbra server. Mark* **Y***.*

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


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

The system will be modified. Continue [N] Y
```

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

   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 values. For information about the menu values, see "Planning for the Installation" chapter, Menu-Driven Configuration section.

```
Main menu

   1) Common Configuration:
        +Hostname:                              mailstore-1.example.com
******* +Ldap master host:                      UNSET
        +Ldap port:                             389
******* +Ldap Admin password:                   UNSET
        +Require secure interprocess communications: yes
        +TimeZone:                              (GMT-08.00) Pacific Time
(US & Canada)

   2) zimbra-store:                             Enabled
        +Create Admin User:                     yes
        +Admin user to create:             admin@mailstore-1.example.com
******* +Admin Password                         UNSET
        +Enable automated spam training:        yes
        +Spam training user:        spam.cc_v05j4@mailstore-1.example.com
        +Non-spam(Ham) training user:  ham.msoyzx@mailstore-1.example.com
        +Global Documents Account:              wiki@mailstore-
1.example.com
        +SMTP host                              mailstore-1.example.com
        +Web server HTTP port:                  80
        +Web server HTTPS port:                 443
        +Web server mode:                       http
        +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://mailstore-
1.example.com:7780/aspell.php
   3) zimbra-snmp:                              Enabled
   4) zimbra-logger:                            Enabled
   5) zimbra-spell:                             Enabled
   6) Default Class of Service Configuration:
        +Enable Instant Messaging Feature:      Disabled
        +Enable Briefcases Feature:             Disabled
        +Enable Tasks Feature:                  Disabled
        +Enable Notebook Feature:               Enabled
      c) Collapse menu
   r) Start servers after configuration         yes
   s) Save config to file
   q) Quit
```

4. Type **1** and press **Enter** to go to the **Common Configuration** menu.

```
Common Configuration:
    1)Hostname:                          mailstore-1.example.com
    2)Ldap master host:                  mailstore-1.example.com
    3)Ldap port:                            389
    4)Ldap Admin password:                  set
    5)Require secure interprocess communications      Yes
    6)TimeZone:              (GMT-08.00) Pacific Time (US & Canada)
```

   The mailbox server hostname is displayed. You must change the LDAP master host name and password to be the values configured on the LDAP server.

   - Type **2**, press **Enter**, and type the LDAP host name. (ldap-1.example.com in this example.)
   - Type **4**, press **Enter**, and type the LDAP password.

   After you set these values, the server immediately contacts the LDAP server. If it cannot contact the server, you cannot proceed.

   - Type **6** to set the correct time zone, if your time zone is not Pacific Time.

5. Type **r** to return to the Main menu.

6. From the Main menu, type **2** to go to the Store configuration menu.

```
Store configuration
1) Status:                              Enabled
   2) Create Admin User:                yes
   3) Admin user to create:             admin@mailstore-1.example.com
** 4) Admin Password                    UNSET
   5) Enable automated spam training:   yes
   6) Spam training user:               spam@mailstore-1.example.com
   7) Non-spam(Ham) training user:      ham@mailstore-1.example.com
   8) Global Documents Account:         wiki@mailstore-1.example.com
   9) SMTP host:                        mailstore-1.example.com
  10) Web server HTTP port:             80
  11) Web server HTTPS port:            443
  12) Web server mode:                  http
   14) IMAP server port:                 143
  15) IMAP server SSL port:             993
  16) POP server port:                  110
  17) POP server SSL port:              995
  18) Use spell check server:           yes
  19) Spell server URL:       http://mailstore-1.example.com:7780/
aspell.php


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

7. Configure the zimbra mailbox store server settings.

- Type **4** and set the password for the administrator account. The password is case sensitive and must be a minimum of six characters. During the install process, the admin account is provisioned on the mailbox store server. You log on to the administration console with this password.

Note: *By default, the email addresses for the admin account, spam, non-spam, wiki are set to be the zimbra mailstore server address. You may want to change these to be the ZCS primary domain address instead. (example.com in this example)*

- Type the corresponding number to set the SMTP host. This is the mta-server host name.
- Type the corresponding number if you want to change the default web server mode. The communication protocol options are HTTP, HTTPS, mixed, both or redirect.

  Mixed mode uses HTTPS for logging in and HTTP for normal session traffic

  Both mode means that an HTTP session stays HTTP, including during the login phase, and an HTTPS session remains HTTPS throughout, including the login phase.

  Redirect mode redirects any users connecting via HTTP to a HTTPS connection.

  All modes use SSL encryption for back-end administrative traffic.
- If you install the zimbra spell package, it is installed on every mailstore. The http address for each is the mailstore server it is installed on host name.
-

8. Type **r** to return to the Main menu.
9. Review the Default Class of Service Configuration settings. If you want to change the COS default configuration of these features, type the number (6) for the **Default Class of Service Configuration**. Then type the corresponding number for the feature to be enabled or disabled. The default COS settings are adjusted to match.
10. When the mailbox server is configured, return to the Main menu and type **a** to apply the configuration changes. Press **Enter** to save the configuration data.
11. When **Save Configuration data to a file** appears, press **Enter**.
12. The next request asks where to save the files. To accept the default, press **Enter**. To save the files to another directory, enter the directory and then press **Enter**.
13. When **The system will be modified - continue?** appears, type **y** and press **Enter**.

The server is modified. Installing all the components and configuring the mailbox server can take a few minutes. This includes installing SSL certificates, setting passwords, setting ports, installing skins and zimlets, setting time zone preferences, and starting the servers, among other processes.

14. When **Configuration 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.32288]
Saving config in /opt/zimbra/config.32288...Done

The system will be modified - continue? [No] y

Operations logged to /tmp/zmsetup.10282008-110412.log
Setting local config zimbra_server_hostname to [mailhost.example.com]
.
.
.
Operations logged to /tmp/zmsetup.log.32288

Configuration complete - press return to exit
```

Installing Zimbra MTA on a Server

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

1. Follow steps 1 through 4 in **"Starting the Installation Process" on page 27** to open a SSH session to the MTA server, log on to the server as **root**, and unpack the Zimbra software.
2. Type **Y** and press **Enter** to install the **zimbra-mta** package. The other packages should be marked **N.** In the following screen shot example, the package to be installed is emphasized.

   Note: *If SNMP is used, it is installed on every server.*

```
Select the packages to install

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

Installing:
    zimbra-mta

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

3. Type **Y**, and press **Enter** to install the selected package(s).

   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 values.

```
Main menu

   1) Common Configuration:
        +Hostname:                              mta-1.example.com
******* +Ldap master host:                      UNSET
        +Ldap port:                             389
******* +Ldap Admin password:                   UNSET
        +Require secure interprocess communications: yes
        +TimeZone:                              (GMT-08.00) Pacific
Time (US & Canada)

   2) zimbra-mta:                               Enabled
********+MTA Auth host:                        mta-1.example.com
        +Enable Spamassassin:                   yes
        +Enable Clam AV:                        yes
        +Notification address for AV alerts:  admin@mta-1.example.com
******* +Bind password for postfix ldap user:  UNSET
******* +Bind password for amavis ldap user:   UNSET

   3) zimbra-snmp:                              Enabled
   4) zimbra-spell:                             Enabled
   5) Enable default backup schedule:           yes
   r) Start servers after configuration        yes
   s) Save config to file
   x) Expand menu
   q) Quit
```

4. The Main menu displays. Type **1** and press **Enter** to go to the **Common Configuration** menu.

```
Common Configuration:
    1)Hostname:                          mta-1.example.com
    2)Ldap master host:                  mta-1.example.com
    3)Ldap port:                            389
    4)Ldap Admin password:                  set
    5)Require secure interprocess communications      Yes
    6)TimeZone:              (GMT-08.00) Pacific Time (US & Canada)
```

   The mailbox server hostname is displayed. You must change the LDAP master host name and password to be the values configured on the LDAP server.

   - Type **2**, press **Enter**, and type the LDAP host name. (ldap-1.example.com in this example.)
   - Type **4**, press **Enter**, and type the LDAP password.

   After you set these values, the server immediately contacts the LDAP server. If it cannot contact the server, you cannot proceed.

   - Type **6** to set the correct time zone, if your time zone is not Pacific Time.

5. Type **r** to return to the Main menu.

6. Type **2** to go to the Mta menu.

```
Select, or press 'a' to apply config (? - help) 2

Mta configuration

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

   - 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.
   - You can change **5**, AV alerts notification address. This should be an address on the domain, such as the admin address. (admin@example.com)

     Note: *If you enter an address other than the admin address, you must provision an account with that address after the installation is complete.*

You must set the same postfix ldap user password and the same amavis ldap user password that is configured on the LDAP master server.

- Type **6** and enter the postfix password.
- Type **7** and enter the amavis password.

7. Type **r** to return to the Main menu.
8. When the MTA server is configured, return to the Main menu and type **a** to apply the configuration changes. Press **Enter** to save the configuration data.
9. When **Save Configuration data to a file** appears, press **Enter**.
10. The next request asks where to save the files. To accept the default, press **Enter**. To save the files to another directory, enter the directory and then press **Enter**.
11. When **The system will be modified - continue?** appears, type **y** and press **Enter**.

    The server is modified. Installing all the components and configuring the MTA server can take a few minutes. This can include setting passwords, setting ports, setting time zone preferences, and starting the server, among other processes.
12. 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 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:                     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 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.
- ZCS ships a default zimbra user with a disabled password. ZCS requires access to this account via ssh public key authentication. On most operating systems this combination is okay, but if you have modified pam rules to disallow any ssh access to disabled accounts then you must define a password for the zimbra UNIX account. This will allow ssh key authentication for checking remote queues. See the Zimbra wiki article, Mail Queue Monitoring.

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. 1.In order for the server statistics to display on the administration console, the syslog configuration files must be modified. 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/syslog stop**.
   c. Start the syslog daemon. Type **/etc/init.d/syslog start**.

Note: *On DEBIAN AND UBUNTU, step 2 is a s follows*

   a. Edit the /etc/default/syslogd file, add **-r** to the SYSLOGD_OPTIONS setting, **SYSLOGD_options="-r -m 0"**
   b. Stop the syslog daemon. Type **/etc/init.d/sysklogd stop**.
   c. Start the syslog daemon. Type **/etc/init.d/sysklogd start**.

Note about MTA servers

New installs of ZCS limit spam/ham training to the first MTA installed. If you uninstall or move this MTA, you will need to enable spam/ham training on another MTA, as one host should have this enabled to run zmtrainsa --cleanup. To do this, set **zmlocalconfig -e zmtrainsa_cleanup_host=TRUE**.

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.*

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**

Post Installation Tasks

Once the Zimbra Collaboration Suite is installed, you can log on to the administration console and configure additional domains, create Classes of Service, and provision accounts. See the Zimbra Administrator's Guide.

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

You can configure one account at a time with the New Account Wizard or you can create many accounts at once using the Bulk Provisioning Wizard.

Configuring One Account

The administration console New Account Wizard steps you through the account information to be completed.

1. From the administration console Navigation pane, click **Accounts**.

   Note: *Four accounts are listed: admin account, two spam training accounts, and a global Documents account. These accounts do not need any additional configuration.*

2. Click **New**. The first page of the **New Account Wizard** opens.

3. Enter the account name to be used as the email address and the last name. This the only required information to create an account.

4. You can click **Finish** at this point, and the account is configured with the default COS and global features.

   To configure aliases, forwarding addresses, and specific features for this account, proceed through the dialog before you click **Finish**.

When the accounts are provisioned, these accounts can immediately start to send and receive emails.

Configuring Many Accounts at Once

You can provision up to 500 accounts on once using the Bulk Account Wizard from the administration console. The wizard takes you through the steps to upload a .csv file with the account information and then provisions the user accounts. These accounts are configured with a user name, display name and password (optional). The accounts are automatically assigned the domain default COS.

Refer to the administration guide to learn more about provisioning accounts.

Import the Content of Users' Mailboxes

Zimbra's migration and import tools can be used to move users' email messages, calendars, and contacts from their old email servers to their accounts on the Zimbra server. When the user's files are imported, the folder hierarchy is maintained. These tools can be accessed from the administration console Download page and instruction guides are available from the Administration Console Help Desk.

Uninstalling Zimbra Collaboration Suite

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

1. Change directories 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 [zcsfilename]**.
5. Delete the zcs.tgz file, type **rm -rf zcs.tgz**.
6. Additional files may need to be delete. See the Zimbra Wiki Installation section on http://wiki.zimbra.com/index.php?title=Main_Page.

Note: For Mac, type **cd /;/opt/zimbra/libexec/installer/install-mac.sh - u**.

Chapter 5 Configuring LDAP Replication

Setting up LDAP replication lets you distribute Zimbra server queries to specific replica LDAP servers. Only one master LDAP server can be set up. This server is authoritative for user information, server configuration, etc. Replica LDAP servers can be defined to improve performance and to reduce the load on the master server. All updates are made to the master server and these updates are copied to the replica servers.

The Zimbra install program is used to configure a master LDAP server and additional read-only replica LDAP servers. The master LDAP server is installed and configured first, following the normal ZCS installation options. The LDAP replica server installation is modified to point the replica server to the LDAP master host.

When the master LDAP server and the replica LDAP servers are correctly installed, the following is automatically configured:

- 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 replica LDAP server. Replica LDAP servers are read-only.
- Zimbra servers are configured to query the replica LDAP server instead of the master LDAP server.

Installing Zimbra Master LDAP Server

You must install the master LDAP server before you can install replica LDAP servers. Refer to “Installing Zimbra LDAP Master Server” on page 30 for master LDAP server installation instructions. After the installation of the master LDAP server has completed continue to the section titled 'Enabling Replication on the LDAP Master.

Enable Replication on the LDAP Master

On the master LDAP server, as a Zimbra user, type: **/opt/zimbra/libexec/zmldapenablereplica** and press **Enter.** This enables replication on the LDAP Master.

Installing a Replica LDAP Server

The master LDAP server must be running when you install the replica server. You run the ZCS install program on the replica server to install the LDAP package.

Follow steps 1 through 4 in “Starting the Installation Process” on page 27 to open a SSH session to the LDAP server, log on to the server as root, and unpack the Zimbra software.

1. Type **Y** and press **Enter** to install the **zimbra-ldap** package. In the screen shot below, the package to be installed is emphasized.

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

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

3. Type **1** to display the Common Configuration submenus. Type **2** to change the **Ldap Master host** name to the name of the Master LDAP host.

4. Type **3**, to change the port to the same port as configured for the Master LDAP server.

5. Type **4** and change the password to the Master LDAP Admin user password. Type **r** to return to the main menu.
6. Type **2** to display the LDAP configuration submenu.
   - Type **2** and change **Create Domain:** to **No**.
   - Type **4** for **LDAP replication password**, enter the same password to match the value on the Master LDAP Admin user password for this local config variable.

   Note: *All passwords must be set to match the master ldap admin user password.To determine this value on the master LDAP, run* **zmlocalconfig -s ldap_replication_password**

Important: *If you have installed Zimbra MTA on the LDAP server, configure the Amavis and the Postfix passwords. To find these values, run*
zmlocalconfig -s ldap_amavis_password
zmlocalconfig -s ldap_postfix_password

```
Ldap configuration

   1) Status:                                  Enabled
   2) Create Domain:                           no
   3) Ldap Root password:                      set
   4) Ldap Replication password:               set
   5) Ldap Postfix password:                   set
   6) Ldap Amavis password:                    set
   7) Ldap Nginx password:                     set
```

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 on the replica LDAP server is complete. The content of the master LDAP directory is copied to the replica LDAP server.

Test the replica

1. Create several user accounts, either from the admin console or on the master LDAP server. The CLI command to create these accounts is

   zmprov ca <name@domain.com> <password>

   If you do not have a mailbox server setup, you can create domains instead. Use this CLI command to create a domain

   zmprov cd <domain name>

2. To see if the accounts were correctly copied to the replica LDAP server, on the replica LDAP server, type **zmprov -l gaa**. Type **zmprov gad** to check all domains.

   The accounts/domains created on the master LDAP server should display on the replica LDAP server.

In cases where the mailbox server is not setup, you can also use the following command for account creation.

zmprov ca <name@domain> <password> zimbraMailTransport <where_to_deliver>

Configuring Zimbra Servers to use LDAP Replica

To use the replica LDAP server instead of the master LDAP server, you must update the ldap_url value on the Zimbra servers that will query the replica instead of the master. For each server that you want to change:

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

2. Update the ldap_url value. Enter the replica LDAP 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. The master URL must always be included and is listed last.

Additional Steps for MTA hosts. After updating the ldap_url, rerun **/opt/zimbra/libexe/zmmtainit**.

This rewrites the Postfix configuration with the updated ldap_url.

Uninstalling an LDAP replica server

If you do not want to use an LDAP replica server, follow these steps to disable it.

Note: *Uninstalling an LDAP server is the same as disabling it on the master LDAP server.*

Remove LDAP replica from all active servers

1. On each member server, including the replica, verify the **ldap_url** value. Type **zmlocalconfig [ldap_url]**
2. Remove the disabled LDAP replica server URL from zmlocalconfig. Do this by modifying the **ldap_url** to only include enabled ZCS LDAP servers. The master LDAP server should always be at the end of the **ldap_url** string value.

```
zmlocalconfig -e ldap_url="ldap://<replica-server-host> ldap://
<master-server-host>"
```

Disable LDAP on the Replica

To disable LDAP on the replica server,

1. Type **zmcontrol stop** to stop the Zimbra services on the server.
2. To disable LDAP service, type

```
zmprov -1 ms <zmhostname> -zimbraServiceEnabled ldap
```

3. Type **zmcontrol start** to start other current Zimbra services on the server.

Additional steps for MTA host. After updating the **ldap_url** with **zmlocalconfig**, rerun **/opt/zimbra/libexec/zmmtainit**. This rewrites the Postfix configuration with the updated **ldap_url**.

System Requirements for Zimbra Collaboration Suite 6.0

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

	Requirements
Servers	Evaluation and Testing • Intel/AMD 32-bit or 64-bit CPU 1.5 GHz • 1 GB RAM • 5 GB free disk space for software and logs • Temp file space for installs and upgrades* • Additional disk space for mail storage Production environments • Minimum - 32-bit OS with Intel/AMD 2.0 GHZ+ CPU Recommended - 64-bit OS • Minimum - 2 GB RAM Recommend minimum - 4 GB RAM • Temp file space for installs and upgrades* • 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 *Temp files space- The zimbra-store requires 5GB for /opt/zimbra, plus additional space for mail storage. The other nodes require 100MB. General Requirements • Firewall Configuration should be set to “No firewall”, and the Security Enhanced Linux (SELinux) should be disabled • RAID-5 is not recommended for installations with more than 100 accounts.

Mac Server	Evaluation and Testing • 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
Mac Server	Production environments • 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 *There are known issues using ZCS on Macs with the Intel Core Duo. See the Release Note.
Operating System Network Edition	• Red Hat® Enterprise Linux®, AS/ES 5 • Red Hat® Enterprise Linux®, AS/ES 4 (32-bit, 64-bit) Note: We expect that the 6.0.x series of ZCS will be the last release supported on RHEL4. Based on this expectation, we suggest that new RHEL systems use RHEL5. • Mac OS x 10.5 or later (Intel) • Mac OS® X 10.4.7 or later Cluster feature is not available on Mac OS X versions. Note: We expect that the 6.0.x series of ZCS will be the last release supported with Mac OS X 10.4.x. • SUSE Linux Enterprise Server 11 (64-bit only) • SUSE Linux Enterprise Server 10 (64-bit, 32-bit) Cluster feature is not available on SUSE Linux versions. Note: We expect that the 6.0.x series of ZCS will be the last release supported with SUSE ES 10. • Ubuntu 8.04 LTS Server Edition • Ubuntu 8.04 LTS Server Edition (64-bit, 32-bit) • Ubuntu 6.06.1 LTS Server Edition (64-bit, 32-bit) Cluster feature is not available on Ubuntu Linux versions. Note: We expect that the 6.0.x series of ZCS will be the last release supported with Ubuntu 6.0.6.1 LTS.

Operating System **Open Source Edition**	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.
File Systems	**ext3** file system for Linux deployments
Other Dependencies	For Red Hat Enterprise, Fedora Core and SuSE operating systems, the server must also have the following installed: • **NPTL**. Native POSIX Thread Library • **Sudo**. Superuser, required to delegate admins. • **libidn**. For internationalizing domain names in applications (IDNA) • **GMP**. GNU Multiple-Precision Library. • **compat-libstdc ++-33**. Compatibility Standard C++ libraries. For RHEL servers only For SLES 10 - compat-libstdc++-5.0.7 For SLES11 - libstdc++33 For Ubuntu 6.06 or 8.04 • Sudo • libidnll • libpcre3 • libexprt1 • libstd++6 • libstd++5 • libgmp3C2 Ubuntu 6 64-bit and Ubuntu 8 64-bit require libperl5.8.
	For Mac servers, Java 1.5 must be installed as the default Java.
Miscellaneous	• 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
Administrator Computers *These OS configurations have been tested and are known to work. Other configurations may work.	• Windows XP with either Internet Explorer 7.0 or Firefox 3.0 • Macintosh OS X 10.4 or later with Firefox 3.0 or later

End User Computers using Zimbra Web Client These OS configurations have been tested and are known to work. Other configurations may work.	Minimum • Intel/AMD/Power PC CPU 750MHz • 256MB RAM Recommended • Intel/AMD/Power PC CPU 1.5GHz • 512MB RAM Operating system/ browser combination advanced ZWC: • Windows XP SP 3, Vista SP 2, Windows 7 with one of these browsers: Internet Explorer 8, 7 and 6.0** SP 2 or Firefox 3.0 and 3.5 Fedora Core 4 with Firefox 2.0 and 3.0 • Mac OS X 10.4 or later with Firefox 3.0 or Safari 4 Other browsers: Chrome Browsers available for use with standard ZWC: Firefox 3.5, 3.0, 2.0 IE 8, 7, 6 SP2** Safari 4, 3, 2 Chrome
End User Computers Using Other Clients	Minimum • Intel/AMD/Power PC CPU 750MHz • 256MB RAM Recommended • Intel/AMD/Power PC CPU 1.5GHz • 512MB RAM Operating system POP/IMAP combinations • Windows XP SP 3, Vista SP 2, Windows 7 with Outlook Express 6, Outlook 2003, (MAPI), Thunderbird • Fedora Core 4 or later with Thunderbird • Mac OS X 10.4 or later with Apple Mail **Accessibility and Screen Readers** Zimbra recommends that customers requiring use of screen readers for accessibility leverage the use of the Standard Zimbra Web Client (HTML). Zimbra continues to invest in improving the accessibility of this interface. The latest updates can be found at http://bugzilla.zimbra.com/show_bug.cgi?id=28516

	**Recommendation - If users are presently using IE 6, Zimbra strongly recommends that they upgrade to the latest version of Internet Explorer for optimal performance with ZWC.
Monitor	Display minimum resolution 1024 x 768
Internet Connection Speed	128 kbps or higher

Migration Wizard Requirements

Migration Wizard for Exchange - Accounts from Microsoft Exchange 2000, 2003, 2007 and 5.5 can be migrated to Zimbra Collaboration Suite.

Migration Wizard for Lotus Dominos - Accounts from Lotus Domino 6.0 or later can be migrated to Zimbra Collaboration Suite.

Import Wizard Requirements

Contents of a .pst file from accounts using Microsoft® Outlook® 2003 and 2007 can be imported to accounts on the Zimbra server.

ZCS 6.0

Rev 1 September 2009

Index

T

U

V

Z