# Zimbra™ Collaboration Suite
# Multi-Server Installation Guide

**ZCS 4.0**
**Open Source Edition**
**August 2006**

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

August 2006t

# Table of Content


**Chapter 1 Introduction . . . . . 3**

Audience . . . . . 3
For More Information . . . . . 3
Support and Contact Information . . . . . 4

**Chapter 2 Preparing Your Server Environment . . . . . 5**

System Requirements . . . . . 5
Modifying Operating System Configurations . . . . . 8
Installation Modifications for Red Hat Enterprise Linux . . . . . 9
Installation Modifications for Fedora . . . . . 11
Installation Modification for Mac Servers . . . . . 13
DNS Configuration Requirement . . . . . 13

**Chapter 3 Planning for the Installation . . . . . 15**

Configuration Examples . . . . . 16
Downloading the Zimbra Software . . . . . 16
Menu-Driven Configuration . . . . . 17
Configuring IMAP and POP Proxy Server . . . . . 21
Configuring for Virtual Hosting . . . . . 22
Load Balancing on ZCS . . . . . 22

**Chapter 4 Multiple-Server Installation . . . . . 25**

Starting the Installation Process . . . . . 25
Starting the Installation Process on the Mac Server . . . . . 27
Installing Zimbra LDAP Master Server . . . . . 28
Installing Zimbra Mailbox Server . . . . . 30
Installing Zimbra MTA on a Server . . . . . 33
Installing the Zimbra-SNMP package . . . . . 35
Final Set-Up . . . . . 35
Verifying Server Configuration . . . . . 36
Post Installation Tasks . . . . . 36
Logging on to the Administration Console . . . . . 36
Defining Classes of Service . . . . . 37
Provisioning Accounts . . . . . 37
Uninstalling Zimbra Collaboration Suite . . . . . 37

**Chapter 5 LDAP Replication Installation . . . . . 39**

Installing Zimbra LDAP Master Server . . . . . 39
Installing a LDAP Replica Server . . . . . 41
Setting Up Zimbra LDAP Servers for Replication . . . . . 43
Configuring Zimbra Servers to use LDAP Replica . . . . . 44

# 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 Open Source Edition 4.0.

## 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, 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.

## 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

| | Requirements |
|---|---|
| **Servers** | *Minimum*<br>• Intel/AMD 32-bit CPU 1.5 GHz<br>• 1 GB RAM<br>• 5 GB free disk space for software and logs<br>• Additional disk space for mail storage<br><br>*Recommended*<br>• Intel/AMD 32-bit CPU 2.0GHZ+<br>• 2 GB RAM<br>• 10 GB free disk space for software and logs (SATA or SCSI for performance, and RAID/Mirroring for redundancy)<br>• Additional disk space for mail storage |

| | |
|---|---|
| **Mac® Server** | *Minimum*<br>• PPC Mac (G4 or better) or Intel Core Duo*<br>• 1 GB RAM<br>• 5 GB free disk space for software and logs<br>• Additional disk space for mail storage<br><br>*Recommended*<br>• PPC Mac (G5 or better) or Intel Core Duo*<br>• 2 GB RAM<br>• 10 GB free disk space for software and logs<br>• Additional disk space for mail storage<br><br>*There are known issues using ZCS on Macs with the Intel Core Duo. See the 3.1 Release Notes. |
| **Operating System**<br>Open Source Edition | • Red Hat® Enterprise Linux®, AS/ES Version 4, (32-bit, 64-bit)<br>• Fedora Core 4 or 5 (32-bit)<br>• Mac OS® X 10.4.5 or .6<br>• SUSE ES 9 or SUSE 10<br><br>Red Hat Enterprise Linux and Fedora Core OS configuration requirements are described in this guide. |

| | |
|---|---|
| **Other Applications** | For Red Hat Enterprise, Fedora Core and SuSE operating systems, the server must also have the following installed:<br>• **NPTL**. Native POSIX Thread Library<br>• **Sudo**. Superuser, required to delegate admins.<br>• **libidn**. For internationalizing domain names in applications (IDNA)<br>• **cURL**. A command line tool for transferring files with URL syntax<br>• **fetchmail.** A remote-mail retrieval and forwarding utility used for on-demand TCIP/IP links.<br>• **GMP**. GNU Multiple-Precision Library.<br>• **compat-libstdcc++-33**. Compatibility Standard C++ libraries.<br>• For Red Hat Enterprise only - **compat-libstdcc++-296** |
| | 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.<br>• Valid DNS configured with an A record and MX record |
| **Administrator Computers**<br>*These OS configurations have been tested and are known to work. Other configurations may work. | • Windows XP with either Internet Explorer 6.0 or Firefox 1.5<br>• Macintosh OS X 10.4 with Firefox 1.5 |

| | |
|---|---|
| **End User Computers using Zimbra Web Client**<br>*These operating system configurations have been tested and are known to work. Other configurations may work. | *Minimum*<br>• Intel/AMD/Power PC CPU 750MHz<br>• 256MB RAM<br><br>*Recommended*<br>• Intel/AMD/Power PC CPU 1.5GHz<br>• 512MB RAM<br><br>Operating system/ browser combinations<br>• Windows XP with either Internet Explorer 6.0 or Firefox 1.5<br>• Fedora Core 4 with Firefox 1.5<br>• Mac OS X 10.4 with Firefox 1.5 or Safari 2.0.3 |
| **End User Computers Using Other Clients**<br>*These OS configurations have been tested and are known to work. Other configurations may work. | *Minimum*<br>• Intel/AMD/Power PC CPU 750MHz<br>• 256MB RAM<br><br>*Recommended*<br>• Intel/AMD/Power PC CPU 1.5GHz<br>• 512MB RAM<br>•<br>Operating system IMAP combinations<br>• Windows XP with either Outlook Express 6, Outlook 2003 for MAPI or IMAP, or Thunderbird 1.0.7<br>• Fedora Core 4 with Thunderbird 1.0.7<br>• Mac OS X 10.4 with Apple Mail |
| Monitor | Display minimum resolution<br>1024 x 768 |
| Internet Connection Speed | 128 kbps or higher |

## 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.

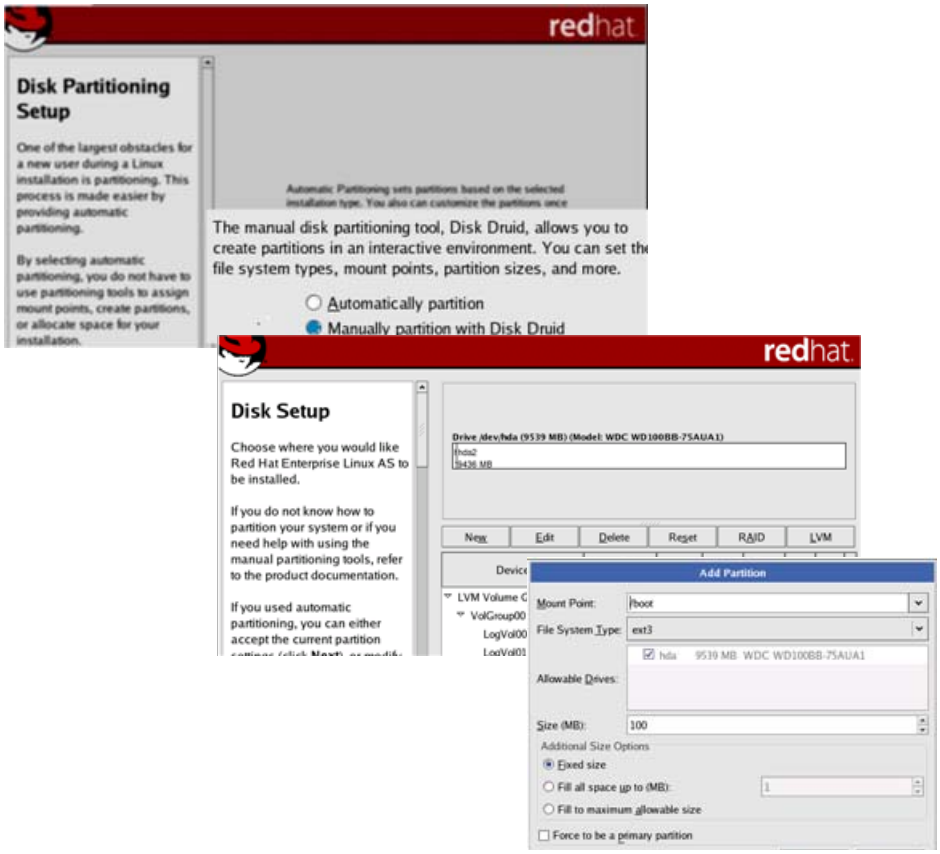
Other operating systems may require similar modifications, use this information as a reference to gauge whether your operating system may need to be modified. Also, search the Zimbra forums.

## Installation Modifications for Red Hat Enterprise Linux

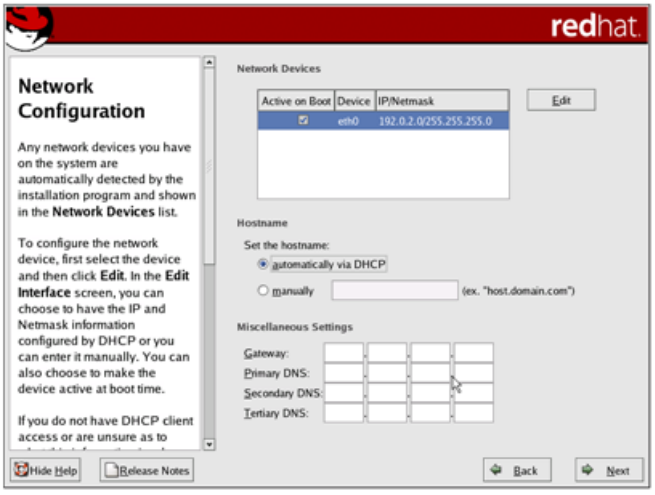
The Zimbra Collaboration Suite runs on the Red Hat Enterprise Linux, 4 operating system. When you install the Red Hat software for the Zimbra Collaboration Suite, you should accept the default setup answers to install the minimum configuration, except the following steps must be modified.

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

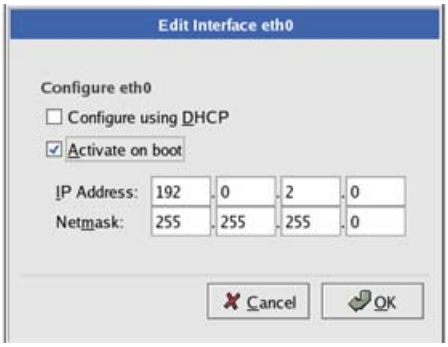
- **Disk Partitioning Setup**. Check **Manually partition with DiskDruid**. The disk partition should be set up as follows:
  - The **Mount Point/RAID Volume** size for the /**boot** partition should be 100 MB.
  - The **Swap** partition should be set to twice the size of the RAM on your machine.
  -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



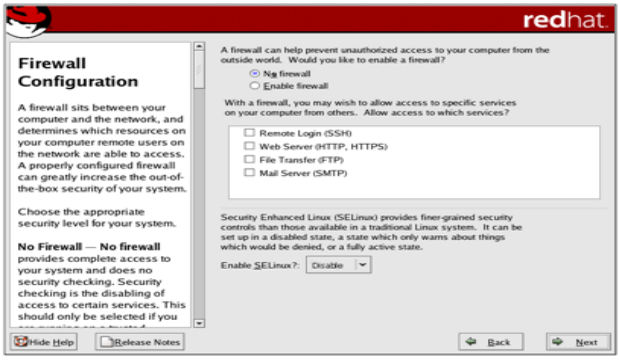

- **Network Configuration>Network Devices>Hostname** should be configured manually with the hostname [*mailhost.example.com]* of the Zimbra server.




- 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.*

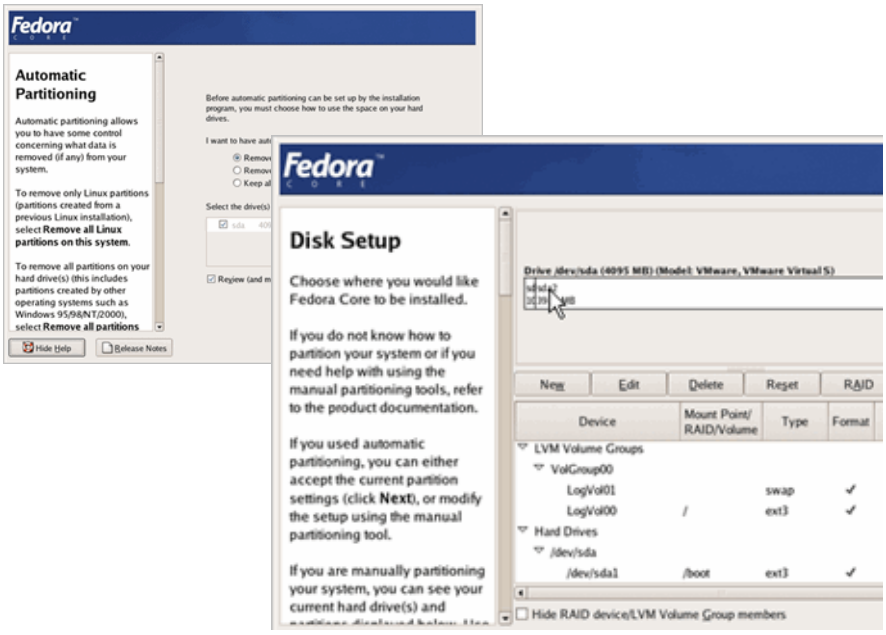
- You must disable Sendmail in order to run the Zimbra Collaboration Suite. Disable the Sendmail service with these commands, **chkconfig sendmail off, service sendmail stop.**
- A fully qualified domain name is required. Make sure that the FQDN entry in **/etc/hosts** appear before the hostnames. If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

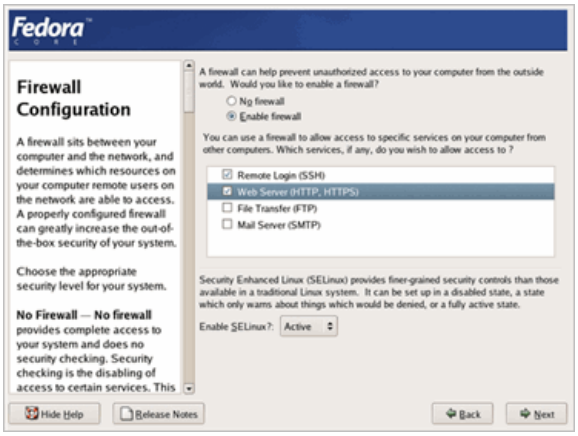
The Zimbra Collaboration Suite runs on the Fedora, Core 3 operating system. When you install the Fedora software for the Zimbra Collaboration Suite, accept the default setup answers, except for the following steps. Refer to the Fedora installation guide for detailed documentation about installing their 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**

## 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 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.<br>See the Zimbra Installation Quick Start for installation instructions. | • Zimbra LDAP and Zimbra message store on one server<br>• Zimbra MTA on a separate server.<br>• Possibly include additional Zimbra MTA servers configured | • Zimbra LDAP on one server<br>• Multiple Zimbra mailbox servers<br>• Multiple Zimbra MTA servers | • Zimbra LDAP server as master<br>• LDAP replicas<br>• Multiple Zimbra mailbox servers<br>• 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 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 Import Wizard. See the Migration Wizard Guide for information about the Migration Wizard file.

## 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. |

**Table 2 Main Menu Options**

| Server Configured | Main Menu | Description |
|---|---|---|
| Zimbra LDAP Server | zimbra-ldap | Configuration includes the following:<br>• **Create Domain** - Yes. You can create one domain during installation and additional domains can be created from the administration console.<br>• **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.<br>• **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.<br>• **Admin user to create** - The default is admin@[mailhost.example.com].<br>• **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 | • By default, the automated spam training filter is enabled and two mail accounts are created.<br><br>*Spam Training User* to receive mail notification about mail that was not marked as junk, but should be.<br>*Non-spam (HAM) training user* to receive mail notification about mail that was marked as junk, but should not have been.<br>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.<br>The spam training filter is automatically added to the cron table and runs daily.<br><br>These default port configurations are shown.<br>• **SMTP host**<br>• **Web server HTTP port**:- 80<br>• **Web server HTTPS port**: - 443<br>• **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.<br>• **Enable POP/IMAP proxy**, default No. See “Configuring IMAP and POP Proxy Server” on page 21.<br>• **IMAP server port**: 143<br>• **IMAP server SSL port**: 993<br>• **POP server port**: 110<br>• **POP server SSL port**: 995<br>• **Use spell checker server**: yes (if installed)<br>• **Spell server URL**: http://<example.com>:7780/aspell.php |

**Table 2 Main Menu Options**

| Server Configured | Main Menu | Description |
|---|---|---|
| Zimbra MTA Server | zimbra-mta | The following options can be modified.<br>• **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.<br>• **Enable Spamassassin**. Default is enabled.<br>• **Enable ClamAV**. Default is enabled.<br>• **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.<br>• |
| All servers, if installed | zimbra-snmp<br>Installing SNMP is optional, but if installed it must be on all servers. | You can modify the following options<br>• **Enable SNMP notifications**. The default is **No**. If you enter yes, you must enter the SNMP Trap hostname.<br>• SNMP Trap hostname<br>• **Enable SMTP notification** - The default is **No**.<br>• **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. |
| | 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 zmibra_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 27.

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 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
```

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 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 of 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 15 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 17 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 t**o 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:        loqpu@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
```

4. 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.

5. 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.

   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.

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

### 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.**