



Zimbra™ Collaboration Suite Multi-Server Installation Guide

Open Source Edition

|

November 2010 Beta

Legal Notices

Copyright ©2005-2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware and Zimbra are registered trademarks or trademarks of VMware, Inc. in the United states and/or other jurisdiction. All other marks and names mentioned herein may be trademarks of their respective companies.

Zimbra, a division of VMware, Inc.

3401 Hillview Avenue
Palo Alto , California 94304 USA
www.Zimbra.com

11/2010- ZCS 7.0 Beta

Table of Contents

Table of Contents	iii
Chapter 1 Introduction	5
Audience	5
For More Information	5
Support and Contact Information	6
Chapter 2 Planning for the Installation	7
Zimbra Packages	7
Configuration Examples	8
Downloading the Zimbra Software	9
Supporting documentation can be found on the administration console Help Desk page or at www.zimbra.com	9
Menu-Driven Configuration	9
Common Configuration Options	10
Zimbra LDAP server configuration options	12
Zimbra Mailbox Server Configuration Options	13
Zimbra MTA Server Configuration Options	16
Configuring for Virtual Hosting	17
Chapter 3 Preparing Your Server Environment	19
System Requirements	19
Modifying Operating System Configurations	19
DNS Configuration Requirement	20
Chapter 4 Multiple-Server Installation	21
Starting the Installation Process	22
Installing Zimbra LDAP Master Server	24
Installing Zimbra Mailbox Server	27
Installing Zimbra MTA on a Server	33
Installing the zimbra-SNMP Package	36
Final Set-Up	37
Note about MTA servers	37
Verifying Server Configuration	38
Logging on to the Administration Console	38
Post Installation Tasks	38
Defining Classes of Service	39
Provisioning Accounts	39
Uninstalling Zimbra Collaboration Suite	40
Chapter 5 Configuring LDAP Replication	41
Installing Zimbra Master LDAP Server	42

Enable Replication on the LDAP Master	42
Installing a Replica LDAP Server	42
Test the replica	44
Configuring Zimbra Servers to use LDAP Replica	45
Uninstalling an LDAP replica server	45
Remove LDAP replica from all active servers	45
Disable LDAP on the Replica	45
Monitoring LDAP Replication Status	46
Feature Requirement	46
Error Codes and Status Explanations	46
System Requirements for Zimbra Collaboration Suite 7.0	49
Index	57

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 7.0

Topics in this chapter include:

- ◆ [Audience on page 5](#)
- ◆ [Zimbra Collaboration Suite License on page 5](#)
- ◆ [For More Information on page 5](#)
- ◆ [Support and Contact Information on page 6](#)

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.
- 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.

Topics in this chapter include:

- ◆ [Zimbra Packages on page 7](#)
- ◆ [Configuration Examples on page 8](#)
- ◆ [Downloading the Zimbra Software on page 9](#)
- ◆ [Zimbra License on page 10](#)
- ◆ [Menu-Driven Configuration on page 9](#)
- ◆ [Configuring for Virtual Hosting on page 17](#)
- ◆ [Configuring ZCS HTTP Proxy on page 21](#)
- ◆ [Configuring for Virtual Hosting on page 17](#)

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 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 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 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 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
<p>All ZCS components installed on one server</p> <p>See the Zimbra Installation Quick Start for installation instructions</p>	<ul style="list-style-type: none"> • Zimbra LDAP and Zimbra message store on one server • Zimbra MTA on a separate server. • Possibly include additional Zimbra MTA servers 	<ul style="list-style-type: none"> • Zimbra LDAP on one server • Multiple Zimbra mailbox servers • Multiple Zimbra MTA servers • One or more Zimbra Proxy servers 	<ul style="list-style-type: none"> • Zimbra Master LDAP server • Replicas LDAP servers • Multiple Zimbra mailbox servers • Multiple Zimbra MTA servers • Multiple Zimbra Proxy 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 following table 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
All	Secure interprocess communications	The default is YES. Secure interprocess communications requires that connections between the mail store, and other processes that use Java, use secure communications. It also specifies whether secure communications should be used between the master LDAP server and the replica LDAP servers for replication.
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)

Main Menu Options

Server Configured	Main Menu	Description
All servers, if installed	zimbra-snmp Installing SNMP is optional, but if installed it must be on all servers.	<p>You can modify the following options</p> <ul style="list-style-type: none"> • Enable SNMP notifications. The default is No. If you enter yes, you must enter the SNMP Trap hostname. • SNMP Trap hostname • Enable SMTP notification — The default is No. • SMTP Source email address — If you enter yes for SMTP notification, you must enter the SMTP source email address and SMTP Destination email address — destination email address.
	c) Collapse menu	Allows you to expand or collapse the menu.
	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.
	x) Expand menu	Expand menus to see the underlying options
	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	<p>Configuration includes the following:</p> <ul style="list-style-type: none">• Status — Enabled. For replica LDAP servers, the status can be changed to Disabled if the database is manually loaded after installation completes.• Create Domain — Yes. You can create one domain during installation. 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	<ul style="list-style-type: none">• 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 following table describes the Zimbra Mailbox server menu options.

Zimbra Mailbox Server Menu Options

Zimbra Mailbox Server	zimbra-store	<p>Configuration includes the following.</p> <ul style="list-style-type: none"> • Create Admin User - The administrator account is created during installation. This account is the first account provisioned on the Zimbra server and allows you to log on to the administration console. • Admin user to create - The default is admin@[mailhost.example.com]. 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. • Anti-virus quarantine user - A virus quarantine account is automatically created during installation. When AmivisD identifies an email message with a virus, the email is automatically sent to this mailbox. The virus quarantine mailbox is configured to delete messages older than 7 days. • Enable automated spam training - By default, the automated spam training filter is enabled and two mail accounts are created. <ul style="list-style-type: none"> 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. <p>These addresses are automatically configured to work with the spam training filter. The accounts created have a randomly selected name. To recognize what the account is used for you may want to change this name.</p> <p>The spam training filter is automatically added to the cron table and runs daily.</p>
-----------------------	--------------	---

Zimbra Mailbox Server Menu Options

Zimbra Mailbox Server	zimbra-store (continued)	<ul style="list-style-type: none"> • 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

		<ul style="list-style-type: none"> • Enable version update checks. ZCS automatically checks to see if a new ZCS update is available. The default is TRUE. • Enable version update notifications. This enables automatic notification when updates are available when this is set to TRUE. • Version update notification email. This is the email address of the account to be notified when updates are available. The default is to send the notification to the admin's account. • Version update source email. This is the email address of the account that sends the email notification. The default is the admin's account. <p>Note: The software update information can be viewed from the Administration Console Tools Overview pane.</p> <ul style="list-style-type: none"> •
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	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 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 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 following table describes the MTA server menu options:

MTA Server Configuration Options

Zimbra MTA Server	zimbra-mta	<p>The following options can be modified.</p> <ul style="list-style-type: none"> • MTA Auth host. This is configured automatically if the MTA authentication server host is on the same server, but must be configured if the authentication server is not on the MTA. The MTA Auth host must be one of the mailbox servers. • Enable Spamassassin. Default is enabled. • Enable ClamAV. Default is enabled. • Notification address for AV alerts. Sets the notification address for AV alerts. You can either accept the default or create a new address. If you create a new address, remember to provision this address from the admin console. <hr/> <p><i>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.</i></p> <hr/> <ul style="list-style-type: none"> • 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.

Topics in this chapter include:

- ◆ [System Requirements on page 19](#)
- ◆ [Modifying Operating System Configurations on page 19](#)
- ◆ [DNS Configuration Requirement on page 20](#)

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 7.0 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

The Zimbra Collaboration Suite runs on one of several operating systems, including Ubuntu® LTS, Red Hat® Enterprise Linux, and SUSE® Linux Enterprise.

Configuration modifications for frequently used operating systems are described in individual configuration documents. Other operating systems, such as may require similar modifications, and you can use the information contained in the individual configuration documents as a reference to gauge whether your operating system may need to be modified. Also, search the Zimbra Forums and Zimbra Wiki.

Note: *Zimbra recommends that the operating systems you use are updated with the latest patches that have been tested with ZCS. See the latest release notes to see the operating systems patch list that has been tested with ZCS.*

DNS Configuration Requirement

When you create a domain 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.

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.

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.

Topics in this chapter include:

- ◆ [Starting the Installation Process on page 22](#)
- ◆ [Installing Zimbra LDAP Master Server on page 24](#)
- ◆ [Installing Zimbra LDAP Master Server on page 24](#)
- ◆ [Installing Zimbra Mailbox Server on page 27](#)
- ◆ [Installing Zimbra MTA on a Server on page 33](#)
- ◆ [Installing zimbra-proxy on page 42](#)
- ◆ [Installing the zimbra-SNMP Package on page 36](#)
- ◆ [Final Set-Up on page 37](#)
- ◆ [Verifying Server Configuration on page 38](#)
- ◆ [Logging on to the Administration Console on page 38](#)
- ◆ [Post Installation Tasks on page 38](#)
- ◆ [Uninstalling Zimbra Collaboration Suite on page 40](#)

After the installation is complete, two additional steps should be run as described in **Final Set-Up on page 37**:

- 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

Important: Before you begin, make sure to:

- Confirm you have the latest system requirements and prerequisites for installing ZCS, as described in [System Requirements for Zimbra Collaboration Suite 7.0](#) on page 49.

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.

Step 1 through step 4 are performed for each server to be installed.

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>**). 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: 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-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20100916012803/
zcs-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20100916012803/packages/
zcs-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20100916012803/packages/
zimbra-apache_7.0.0_GA_2834.UBUNTU10_64_amd64.deb
.
.
zcs-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20101015012627/install.sh
zcs-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20101015012627/README.txt
.
[root@mailhost tmp]# cd zcs-NETWORK-
7.0.0_GA_2834.UBUNTU10_64.20101015012627
[root@mailhost tmp/zcs-NETWORK-
7.0.0_GA_2834.UBUNTU10_64.20101015012627# ./install.sh
.
.
Operations logged to /tmp/install.log.3833
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
```

Screenshots in this guide are examples of the Zimbra installation script. The actual script may be different.

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. 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 installation process quits. You must fix the problem and start the installation again. See Other Dependencies in System Requirements for Zimbra Collaboration Suite 7.0.

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 you would like to change the hostname. The domain name should have an MX record configured in DNS.

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](#).

Important: If you are installing more than one LDAP server, see [Chapter 5, Configuring LDAP Replication](#).

1. Follow steps 1 through 4 in **Starting the Installation Process on page 22** 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

Checking required space for zimbra-core

Installing:
  zimbra-core
  zimbra-ldap

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**. 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 “**Main Menu Options,**” on page 10 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)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**.

```

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes] y
Save config in file: [/opt/zimbra/config.26148]
Saving config in /opt/zimbra/config.26148...done.

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

Operations logged to /tmp/zmsetup.10192010-151126.log
Setting local config values...done.
.
.
.
Starting servers...done.
Setting up zimbra crontab...done.

Moving /tmp/zmsetup.10192010-151126.log to /opt/zimbra/log

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.*

1. Follow steps 1 through 4 in **Starting the Installation Process on page 22** 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
      +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.mszyzx@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
      +Enable version update checks: TRUE
      +Enable version update notifications: TRUE
      +Version update notification email: admin@mailstore-
1.example.com
      +Version update source email: admin@mailstore-
1.example.com

  3) zimbra-logger: Enabled
      4) zimbra-spell: Enabled
      5) zimbra-convertd: Enabled
      6) Default Class of Service Configuration:
          r) Start servers after configuration yes
          s) Save config to file
          x) Expand menu

          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)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@mailhost.example.com
** 4) Admin Password UNSET
 5) Anti-virus quarantine user: virus-
quarantine.zodi72xmm6@mailhost.example.com
 6) Enable automated spam training: yes
 7) Spam training user: spam.vviwu_izoj@mailhost.example.com
 8) Non-spam(Ham) training user: ham.unsbogyzer@mailhost.example.com
 9) SMTP host: mailhost.example.com
10) Web server HTTP port: 80
11) Web server HTTPS port: 443
12) Web server mode: http
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

21) Enable version update checks: TRUE
22) Enable version update notifications: TRUE

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

Password for admin@mailhost.example.com (min 6 characters):
[2LPoBSob] zimbra

```

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. **Enable version update checks** and **Enable version update notifications** are set to TRUE. ZCS automatically checks for the latest ZCS software updates and notifies the account that is configured in **Version update notification email**. You can modify this later from the administration console. 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 22** 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
        +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) 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:                       ldap-1.example.com
  3)Ldap port:                              389
  4)Ldap Admin password:                    set
  5)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.

-
- 13.

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 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/libexec/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 as 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/syslogd stop`.
- c. Start the syslog daemon. Type `/etc/init.d/syslogd 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 multiple accounts at once using the Account Migration tool from the administration console. The wizard guides you through the steps to import accounts from an external directory server, either Active Directory or an LDAP server. The wizard downloads account information from your directory and creates the accounts in ZCS.

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.

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.

Topics in this chapter include:

- ◆ [Installing Zimbra Master LDAP Server on page 42](#)
- ◆ [Enable Replication on the LDAP Master on page 42](#)
- ◆ [Installing a Replica LDAP Server on page 42](#)
- ◆ [Configuring Zimbra Servers to use LDAP Replica on page 45](#)
- ◆ [Uninstalling an LDAP replica server on page 45](#)

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 24 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 22 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] 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

```

- 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
```

- When **Save Configuration data to a file** appears, press **Enter**.
- 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.

- 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

- 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>
- 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.
3. Update the `ldap_master_url` value. Enter the master LDAP server URL, if not already set.

`zmlocalconfig -e ldap_master_url=ldap://<masterhost>:port`

Additional Steps for MTA hosts. After updating the `ldap_url`, rerun `/opt/zimbra/libexec/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 -l ms <zhostname> -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**.

Monitoring LDAP Replication Status

The Monitoring LDAP Replication Status feature monitors the change sequence number (CSN) values between an LDAP master server and an LDAP replica server. The replica server is considered a shadow copy of the master server. If the servers become out of sync, the monitoring feature indicates the problem. The out of sync time period is typically five minutes, although this value is configurable.

Feature Requirement

Run the script **zmreplchk** located in **/opt/zimbra/libexec**.

Important: This script must be run on a ZCS server that has a **localconfig** value set for **ldap_url** that includes all of the replica servers and ends with the master server.

Error Codes and Status Explanations

The following monitoring error codes and status explanations are given with this feature:

Error Code	Status	Description
Code 0	In Sync	The servers are currently in sync.
Code 1	No contact	No connection to the master server and the system exits.
Code 2	Stand-alone	The master server has no replica servers and is considered a standalone master server.
Code 3	Could not execute StartTLS	The replica server requires StartTLS and fails.
Code 4	Server down	The replica server is currently down.

Code 5	Unable to search	Searching the replica server for the context CSN fails.
Code 6	Xw Xd Xh Xm Xs behind	The replica server becomes out of sync. Status indicates amount of time the replica server is behind the master server in w=weeks, d=days, h=hours, m=minutes, and s=seconds.

For example, **ldap002.example.com** is the master server, and **ldap003.example.com** and **ldap004.example.com** are replicas servers. The following screen-shot shows that replica server **ldap003** is in sync with the master server, as indicated by the **Code:0** and **Status: In Sync**, and replica server **ldap004** is currently down, as indicated by **Code: 4** and **Status: Server down**.

```
zimbra@ldap002.example.com
Replica: ldap://ldap003.example.com:389 Code: 0 Status: In Sync
Replica: ldap://ldap004.example.com:389 Code: 4 Status: Server down
```

If the replica server becomes out of sync with the master server, the status given indicates in a time format how far behind the master server it has become:

```
Replica: ldap://ldap003.example.com:389 Code: 0 Status: In Sync
Replica: ldap://ldap004.example.com:389 Code: 6 Status: 0w 0d 0h 14m 42s behind
```

System Requirements for Zimbra Collaboration Suite 7.0

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

	Requirements
Servers	<p>Evaluation and Testing</p> <ul style="list-style-type: none">• 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 <p>Production environments</p> <ul style="list-style-type: none">• 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 <p>*Temp files space- The zimbra-store requires 5GB for /opt/zimbra, plus additional space for mail storage. The other nodes require 100MB.</p> <p>General Requirements</p> <ul style="list-style-type: none">• 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.

Operating System Network Edition	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> • Red Hat® Enterprise Linux®, AS/ES 6 (64-bit, mid-version) • Red Hat® Enterprise Linux®, AS/ES 5 (32-bit or 64-bit) • Red Hat® Enterprise Linux®, AS/ES 4 (32-bit or 64-bit) <p>Note: The 7.0.x series of ZCS will be the last release supported with RHEL4 (32-bit) and RHEL5 (32-bit). Based on this expectation, we suggest that new RHEL systems use RHEL5 (64-bit) or RHEL6 (64-bit).</p> <ul style="list-style-type: none"> • SUSE Linux Enterprise Server 11, SP1 (64-bit) • SUSE Linux Enterprise Server 10 (32-bit or 64-bit) <p>Note: Cluster feature is not available on SUSE Linux versions.</p> <p>Note: The 7.0.x series of ZCS will be the last release supported with SLES10 (32-bit). Based on this expectation, we suggest that new SUSE systems use SLES10 (64-bit) or SLES11 SP1 (64-bit).</p> <ul style="list-style-type: none"> • Ubuntu 10.04 LTS Server Edition (64-bit) • Ubuntu 8.04 LTS Server Edition (32-bit or 64-bit) <p>Note: Cluster feature is not available on Ubuntu Linux versions.</p> <p>Note: The 7.0.x series of ZCS will be the last release supported with Ubuntu 8.04 (32-bit). Based on this expectation, we suggest that new Ubuntu systems use Ubuntu 8.04 (64-bit) or Ubuntu 10.04 (64-bit).</p>
Operating System Open Source Edition	<p>In addition to supporting the operating systems listed above for the Network Edition, other operating system versions are available for the Open Source Edition. Check the Zimbra Open Source Downloads page on www.zimbra.com.</p>
File Systems	ext3 file system for Linux deployments

Other Dependencies	<p>For Red Hat Enterprise, Fedora Core and SUSE operating systems, the server must also have the following installed:</p> <ul style="list-style-type: none"> • NPTL. Native POSIX Thread Library • Sudo. Superuser, required to delegate admins. • libidn. For internationalizing domain names in applications (IDNA) • GMP. GNU Multiple-Precision Library. • compat-libstdc ++-33. Compatibility Standard C++ libraries. For RHEL servers only <p>For SLES10 - compat-libstdc++-5.0.7 For SLES11 - libstdc++33</p> <p>For Ubuntu 8.04</p> <ul style="list-style-type: none"> • Sudo • libidn11 • libpcre3 • libexpat1 • libstdc++6 • libstdc++5 • libgmp3C2 <p>Note: Ubuntu 8 (64-bit) requires libperl 5.8.</p>
Miscellaneous	<ul style="list-style-type: none"> • SSH client software to transfer and install the Zimbra Collaboration Suite software. • Valid DNS configured with an A record and MX record • Servers should be configured to run Network Time Protocol (NTP) on a scheduled basis

Administrator Computers	<p>The following operating system/browser combinations are supported:</p> <p>Windows 2000, XP, Vista, and Windows 7 with one of the following:</p> <ul style="list-style-type: none">• Internet Explorer 7.0 or 8.0• Firefox 3.0, 3.5 or 3.6• Safari 4 or 5• Google Chrome 2.1, 2.2, or 2.3 <p>Mac OS X 10.4, 10.5 or 10.6 with one of the following:</p> <ul style="list-style-type: none">• Firefox 3.0, 3.5 or 3.6• Safari 4 or 5• Google Chrome 2.1, 2.2, or 2.3 <p>Linux (Red Hat, Ubuntu, Debian, Fedora, or SUSE) with one of the following:</p> <ul style="list-style-type: none">• Firefox 3.0, 3.5 or 3.6• Google Chrome 2.1, 2.2, or 2.3 <p>Note: We expect that the 7.0.x series of ZCS will be the last release to support Firefox 3.0. Based on this expectation, we suggest a 3.5 or newer version of Firefox be used.</p>
------------------------------------	---

**End User Computers
using
Zimbra Web Client**

Note: Other
configurations may work.

Minimum

- Intel/AMD/Power PC CPU 750MHz
- 256MB RAM

Recommended

- Intel/AMD/Power PC CPU 1.5GHz
- 512MB RAM

For Zimbra Web Client - Advanced version:

The following operating system/browser combinations
for the advanced Zimbra Web Client are supported:

Windows 2000, XP SP 3, Vista SP 2, or Windows 7
with one of the following:

- Internet Explorer 7 or 8
- Firefox 3.0, 3.5 or 3.6
- Safari 4 or 5
- Google Chrome 2.1, 2.2, or 2.3

Mac OS X 10.4, 10.5, or 10.6 with one of the following:

- Firefox 3.0, 3.5 or 3.6
- Safari 4 or 5
- Google Chrome 2.1, 2.2, or 2.3

Linux (Red Hat, Ubuntu, Debian, Fedora, or SUSE)
with one of the following:

- Firefox 3.0, 3.5 or 3.6
- Google Chrome 2.1, 2.2, or 2.3

Note: We expect that the 7.0.x series of ZCS will be
the last release to support Firefox 3.0. Based on this
expectation, we suggest a newer version of Firefox be
used as listed above.

**End User Computers
using
Zimbra Web Client**
(continued)**For Zimbra Web Client - Standard version**

The following operating system/browser combinations for the standard Zimbra Web Client are supported:

Windows 2000, XP SP 3, Vista SP 2, or Windows 7 with one of the following browsers:

- Internet Explorer 6.0 SP2, 7 or 8
- Firefox 3.0, 3.5 or 3.6
- Safari 3, 4, or 5
- Google Chrome 2.1, 2.2, or 2.3

Mac OS X 10.4, 10.5, or 10.6 with one of the following browsers:

- Firefox 3.0, 3.5 or 3.6
- Safari 4 or 5
- Google Chrome 2.1, 2.2, or 2.3

Linux (Red Hat, Ubuntu, Debian, Fedora, or SUSE) with one of the following browsers:

- Firefox 3.0, 3.5 or 3.6
- Google Chrome 2.1, 2.2, or 2.3

Note: We expect that the 7.0.x series of ZCS will be the last release to support Internet Explorer 6.0 SP2, Firefox 3.0, and Safari 3. Based on this expectation, we suggest a newer supported browser version be used.

End User Computers Using Other Clients	<p>Minimum</p> <ul style="list-style-type: none"> • Intel/AMD/Power PC CPU 750MHz • 256MB RAM <p>Recommended</p> <ul style="list-style-type: none"> • Intel/AMD/Power PC CPU 1.5GHz • 512MB RAM <p>Operating system POP/IMAP combinations</p> <ul style="list-style-type: none"> • 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 <p>Accessibility and Screen Readers</p> <p>Zimbra recommends that customers requiring use of screen readers for accessibility leverage the use of the Standard Zimbra Web Client (HTML).</p> <p>Zimbra continues to invest in improving the accessibility of this interface.</p>
	<p>**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.</p>
Monitor	<p>Display minimum resolution 1024 x 768</p>
Internet Connection Speed	<p>128 kbps or higher</p>

Copyright © 2010 Zimbra and VMware, Inc. All rights reserved.

ZCS 7.0 November 2010

Index

A

administration console, logging on 38
administration console, URL 38

C

certificate authority 38
class of service 39
configuration options 8

D

disable MySQL 23
DNS 20
download software 9

F

feedback 6
firewall, Red Hat 20
forums, join Zimbra 6

I

import user mailboxes 40
installation process 22
installation, prerequisite software 23

L

LDAP replica, test 44
LDAP replication, configuring 45
LDAP replication, disable 45
LDAP replication, enable 42
LDAP replication, install 42
LDAP replication, password 43
LDAP replication, uninstall 45
LDAP server configuration 12
LDAP server, install 24
LDAP server, LDAP replication install 42
logger package 15

M

mailbox server, configuration 13
mailbox server, install 27
main menu options 10
menu - main, description 9
migrate mailbox 40
MTA Auth host 35
MTA server, configuration 16
MTA server, install 33
multiple-server installation 21

MX record 20

O

overview of Zimbra packages 7

P

passwords, amavis and postfix 43
port configurations, default 14
post installation tasks 38

R

relay host 20

S

server configuration, verify 38
SNMP, install 36
software agreement 23
spam training filter 13
spell checker, install 15
support, contact Zimbra 6
system requirements 19

T

test LDAP replica 44

U

uninstall ZCS 40
uninstall ZCS for Mac server 40
URL, administration console 38

V

virtual hosting 17

Z

Zimbra Collaboration Suite, uninstall 40
Zimbra packages 7
zmcontrol status 38

