Zimbra Collaboration
Multi-Server Installation Guide

Zimbra Collaboration 8.6

Open Source Edition

December 2014

Legal Notices

Zimbra, Inc.
3000 Internet Blvd., Suite 200
Frisco, Texas 75034

www.zimbra.com

Zimbra Collaboration 8.6.0, GA - December 2014

Table of Contents

1 Introduction

Information in this guide is intended for persons responsible for installing the Zimbra Collaboration. 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 Open Source Edition 8.6

Topics in this chapter include:

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 administrator 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 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 guides describe how to migrate users that are on Microsoft Exchange or Lotus Domino systems to the Zimbra Collaboration.

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 Zimbra Sales to purchase Zimbra Collaboration.
- 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.
- 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 **www.zimbra.com** and submit a bug report. Make sure you provide enough detail so that the bug can be easily duplicated.

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 (ZCS).

Topics in this chapter include:

Zimbra Application 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 application 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 ZCS. 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 MariaDB© 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.
- **Web application services**. The Jetty web application server runs web applications (webapps) on any store server. It provides one or more web application services.

- **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 Proxy**. Zimbra Proxy is a high-performance reverse proxy service for passing IMAP[S]/POP[S]/HTTP[S] client requests to other internal ZCS services.This package is normally installed on the MTA server(s) or on its own independent server(s). When the zimbra-proxy package is installed, the proxy feature is enabled by default. Installing the Zimbra Proxy is highly recommended, and required if using a separate web application server.
- **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.
-

Configuration Examples

ZCS 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. Contact Zimbra Sales for more information about setting up your environment.

Downloading the Zimbra Software

For the latest Zimbra software download, go to http://www.zimbra.com/downloads/. Save the Zimbra Collaboration download file to the computer from which you will install the software.

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

You can access these download files from your administration console>Tools and Migration>Download page, and instruction guides are available from the Help Center page or from http://www.zimbra.com/support/.

- EWS is a separately licensed add-on feature.

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	LDAP Base DN	The base DN describes where to load users and groups. In LDAP form, it is cn=Users. Default is cn=zimbra.
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)
All	IP Mode	IPv4 or IPv6. IPv4 is the default.
All	Default SSL digest	Sets the default message digest to use when generating certificate. Defaults is sha256.

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.	You can modify the following options • **Enable SNMP notifications**. The default is **No**. If you enter yes, you must enter the SNMP Trap hostname. • SNMP Trap hostname • **Enable SMTP notification** — The default is **No**. • **SMTP Source email address** — If you enter yes for SMTP notification, you must enter the SMTP source email address and **SMTP Destination email address** — destination email address.
	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	Configuration includes the following: • **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. • **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. • **LDAP Bes Searcher password**.

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	Configuration includes the following. • **Create Admin User** - The administrator account is created during installation. This account is the first account provisioned on the Zimbra server and allows you to log on to the administration console. • **Admin user to create** - The user name assigned to the administrator account. Once the administrator account has been created, it is suggested that you do not rename the account as automatic ZCS notifications might not be received. • **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. **1 -Spam training user** to receive mail notification about mail that was not marked as junk, but should be. **2 -Non-spam (HAM) training user** to receive mail notification about mail that was marked as junk, but should not have been. These addresses are automatically configured to work with the spam training filter. The accounts created have a randomly selected name. To recognize what the account is used for you may want to change this name. The spam training filter is automatically added to the cron table and runs daily.

Zimbra Mailbox Server Menu Options

Zimbra Mailbox Server	zimbra-store (continued)	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 check server**: yes (if installed) • **Spell server URL**: http://<example.com>:7780/aspell.php
		• **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. **Note**: The software update information can be viewed from the Administration Console Tools Overview pane. • • •

Zimbra Mailbox Server Menu Options

Zimbra mailbox server	zimbra-logger	The Logger package is installed on the one mail server. If installed, it is automatically enabled. Logs from all the hosts are sent to the mailbox server where the logger package is installed. This data is used to generate the statistics graphs and reporting.
Zimbra mailbox server	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 mailbox server	zimbra-dnscache	Intended primarily on MTAs for optimized DNS and RBL lookups. Can also be installed on mailstores and proxy servers.
Zimbra mailbox server	zimbra-snmp	Installing the Zimbra-SNMP package is optional. If you choose to install Zimbra-SNMP for monitoring, the package should be run on every server (Zimbra server, Zimbra LDAP, Zimbra MTA) that is part of the Zimbra configuration. Zimbra uses swatch to watch the syslog output to generate SNMP traps.
Zimbra mailbox server	zimbra-apache	When you install zimbra-spell, zimbra-apache gets installed automatically.
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-memcached	Zimbra Memcached is a separate package from zimbraproxy and is automatically selected when the zimbra-proxy package is installed. One server must run zimbramemcached when the proxy is in use. All installed zimbraproxies can use a single memcached server.
Zimbra mailbox server	Enable VMware HA	VMware HA Clustering Heartbeat is only available when running within a virtual machine running vmware-tools.
Zimbra mailbox server	Default Class of Service Configuration	This menu lists major new features for the ZCS release and whether feature are enabled or not. When you change the feature setting during ZCS installation, you change the default COS settings.
Zimbra mailbox server	Start servers after configuration	Start servers after configuration.
Zimbra mailbox server	Save config to file	Save the configuration to file.

Zimbra Mailbox Server Menu Options

Zimbra mailbox server	Expand menu	Expand the menu.

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	The following options can be modified. • **MTA Auth host.** This is configured automatically if the MTA authentication server host is on the same server, but must be configured if the authentication server is not on the MTA. The MTA Auth host must be one of the mailbox servers. • **Enable Spamassassin**. Default is enabled. • **Enable ClamAV**. Default is enabled. To configure attachment scanning, see Scanning Attachments in Outgoing Mail. • **Notification address for AV alerts**. Sets the notification address for AV alerts. You can either accept the default or create a new address. If you create a new address, remember to provision this address from the admin console. ***Note:*** *If the virus notification address does not exist and your host name is the same as the domain name on the Zimbra server, the virus notifications queue in the Zimbra MTA server and cannot be delivered.* • **Bind password for postfix LDAP user**. This password must be the same as the postfix password configured on the master LDAP server. • **Bind password for amavis LDAP user**. This password must be the same as the amavis password configured on the master LDAP server.

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

Scanning Attachments in Outgoing Mail

You can enable real-time scanning of attachments in outgoing emails sent using the Zimbra Web Client. If enabled, when an attachment is added to an email, it is scanned using ClamAV prior to sending the message. If ClamAV detects a virus, it will block attaching the file to the message. By default, scanning is configured for a single node installation.

To enable in a multi-node environment, one of the MTA nodes needs to be picked for handling ClamAV scanning. Then enable the following:

```
zmprov ms <mta server> zimbraClamAVBindAddress <mta server>
zmprov mcf zimbraAttachmentsScanURL clam://<mta server>:3310/
zmprov mcf zimbraAttachmentsScanEnabled TRUE
```

Overview of the Zimbra Proxy Server

Zimbra Proxy (Nginx-Zimbra) is a high-performance reverse proxy server that passes IMAP[S]/POP[S]/HTTP[S] client requests to other internal ZCS services. A reverse proxy server is an Internet-facing server that protects and manages client connections to your internal services. It can also provide functions like: GSSAPI authentication, throttle control, SSL connection with different certificates for different virtual host names, and other features.

In a typical use case, Zimbra Proxy extracts user login information (such as account id or user name) and then fetches the route to the upstream mail server or web servers' address from "Nginx Lookup Extension", and finally proxy the interactions between clients and upstream ZCS servers. To accelerate the speed of route lookup, memcached is introduced, which caches the lookup result. The subsequent login with the same username is directly proxied without looking up in Nginx Lookup Extension.

You can install the Zimbra Proxy package on a mailbox server, MTA server, or on its own independent server. When the Zimbra Proxy package is installed, the proxy feature is enabled. In most cases, no modification is necessary.

Benefits for using the Zimbra Proxy include:

- Centralizes access to Mailbox servers
- Load Balancing
- Security
- Authentication
- SSL Termination
- Caching
- Centralized Logging and Auditing
- URL Rewriting

For more information, see the wiki page http://wiki.zimbra.com/wiki/Zimbra_Proxy_Guide.

Zimbra Proxy Components and Memcached

Zimbra Proxy is designed to provide a HTTP[S]/POP[S]/IMAP[S] reverse proxy that is quick, reliable, and scalable. Zimbra Proxy includes the following:

- **Nginx**. A high performance HTTP[S]/POP[S]/IMAP[S] proxy server which handles all incoming HTTP[S]/POP[S]/IMAP[S] requests.
- **Zimbra Proxy Route Lookup Handler.** This is a servlet (also named as Nginx Lookup Extension or NLE) located on the ZCS mailbox server. This servlet handles queries for the user account route information (the server and port number where the user account resides).

Memcached is a high performance, distributed memory object caching system. Route information is cached for further use in order to increase performance. **zimbra-memcached** is a separate package that is recommended to be installed along with **zimbra-proxy**.

Zimbra Proxy Architecture and Flow

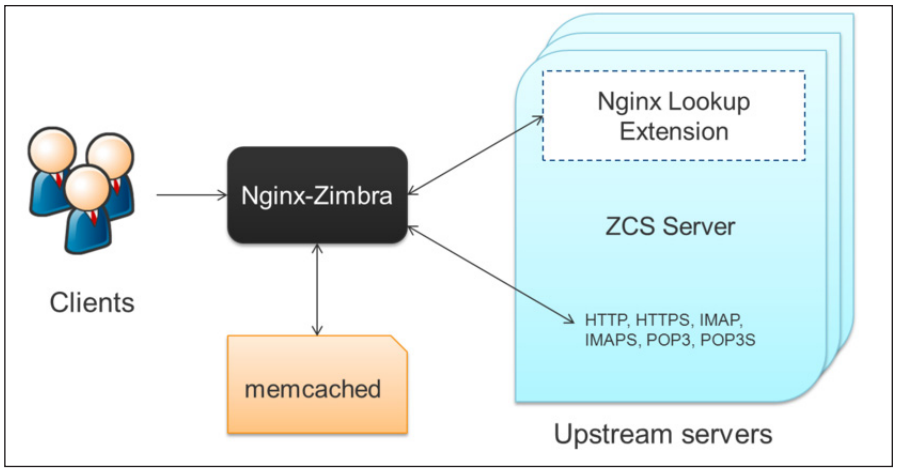
The following sequence explains the architecture and the login flow when an end client connects to Zimbra Proxy.

1. End clients connect to Zimbra Proxy using HTTP[S]/POP[S]/IMAP[S] ports.
2. Proxy attempts to contact a memcached server (elected from the available memcached servers, using a round-robin algorithm) if available and with caching enabled to query the upstream route information for this particular client.
3. If the route information is present in memcached, then this will be a cache-hit case and the proxy connects to the corresponding Zimbra Mailbox server right away and initiates a web/mail proxy session for this client. The memcached component stores the route information for the configured period of time (configurable and one hour by default). Zimbra proxy uses this route information instead of querying the Zimbra Proxy Route Lookup Handler/NLE until the default period of time has expired.
4. If the route information is not present in memcached, then this will be a cache-miss case, so Zimbra Proxy will proceed sending an HTTP request to an available Zimbra Proxy Route Lookup Handler/NLE (elected by round-robin), to look up the upstream mailbox server where this user account resides.
5. Zimbra Proxy Route Lookup Handler/NLE locates the route information from LDAP for the account being accessed and returns this back to Zimbra Proxy.

6. Zimbra Proxy uses this route information to connect to the corresponding Zimbra Mailbox server and initiates a web/mail proxy session. It also caches this route information into a memcached server so that the next time this user logs in, the memcached server has the upstream information available in its cache, and Zimbra Proxy will not need to contact NLE.The end client is transparent to this and behaves as if it is connecting directly to the Zimbra Mailbox server.

Zimbra Proxy Position in ZCS Runtime

The following figure displays the positions of Zimbra Proxy and its relationships to other components of ZCS.



Deployment Strategy

The deployment strategy and position with respect to non-proxy hosts, Zimbra actively suggests using the Proxy server on the edge (either on an independent server or on the same server running LDAP/MTA) with mailbox servers behind it. In the case of multiple proxies, an external load balancer can be placed in front to distribute the load evenly among the proxy servers. Note the Zimbra Proxy package does not act as a firewall and needs to be behind the firewall in customer deployments.

Configuration during installation

zimbra-proxy package needs to be selected during the installation process (it is installed by default). It is highly recommended to install memcached as well along with proxy for better performance.

```
Install zimbra-proxy [Y]
Install zimbra-memcached [Y]
```

This would install and enable all IMAP[S]/POP[S]/HTTP[S] proxy components with the following default configuration.

Proxy configuration

```
1) Status:                              Enabled
2) Enable POP/IMAP Proxy:               TRUE
3) IMAP proxy port:                     143
4) IMAP SSL proxy port:                 993
5) POP proxy port:                      110
6) POP SSL proxy port:                  995
7) Bind password for nginx ldap user:   set
8) Enable HTTP[S] Proxy:                TRUE
9) HTTP proxy port:                     80
10) HTTPS proxy port:                   443
11) Proxy server mode:                  https
```

Zimbra Proxy Ports

The following ports are used either by Zimbra Proxy or by Zimbra Mailbox (if Proxy is not configured). If you have any other services running on these ports, turn them off.

End clients connect directly to Zimbra Proxy, using the Zimbra Proxy Ports. Zimbra Proxy connects to the Route Lookup Handler/NLE (which resides on Zimbra Mailbox server) using the Zimbra Mailbox Ports.

Zimbra Proxy Port Mapping

Zimbra Proxy Ports (External to ZCS)	
HTTP	80
HTTPS	443
POP3	110
POP3S (Secure POP3)	995
IMAP	143
IMAPS (Secure IMAP)	993
Zimbra Mailbox Ports (Internal to ZCS)	
Route Lookup Handler	7072
HTTP Backend (if Proxy configured)	8080
HTTPS Backend (if Proxy configured)	8443
POP3 Backend (if Proxy configured)	7110
POP3S Backend (if Proxy configured)	7995
IMAP Backend (if Proxy configured)	7143
IMAPS Backend (if Proxy configured)	7993

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 **Configure>Domains>Virtual Hosts** page. 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.

3 Preparing Your Server Environment

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

Topics in this chapter include:

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 at the end of this guide.

Modifying Operating System Configurations

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.*

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

Installation modifications for frequently used operating systems are described in individual configuration documents found on the ZCS documentation website, such as *Installation Modifications for ZCS with Ubuntu LTS*, or *Installation Modifications for ZCS with Red Hat*. Other operating systems may require similar modifications, and you can use the information contained in these documents as a reference to gauge whether your operating system might need to be modified.

A full default installation of the Linux distribution that you select is required.

For more information, refer to the System Requirements for Zimbra Collaboration document for information on hardware and software configurations supported by Zimbra Collaboration.

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 **Configure>Global Settings>MTA** page 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.*

4 Multiple-Server Installation

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

When the server installation is complete after final set-up and server configuration steps are run, the servers are started and the status is displayed.

Topics in this chapter include:

Order of Installation

1. Zimbra LDAP server(s)
2. Zimbra MTA server(s)
3. Zimbra Proxy server(s)
4. Zimbra Mailbox server(s) options:
   - Zimbra Mailbox Server, which includes the mailstore services and webapp services (mailstore server + UI server)

   or

   - Zimbra Web Application Server Split mode, which includes:
     - a Zimbra mailstore server (mailstore server)
     - a Zimbra webapp server (UI server)

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 on page 69.

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

Note: *The screen shots are examples of the Zimbra installation script. The actual script may be different.*

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 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.*

```
[root@mailhost tmp]# tar xzvf zcs.tgz
zcs-NETWORK-8.6.0_GA_3033.UBUNTU10_64.20100916012803/
zcs-NETWORK-8.6.0_GA_3033.UBUNTU10_64.20100916012803/packages/
zcs-NETWORK-8.6.0_GA_3033.UBUNTU10_64.20100916012803/packages/
zimbra-apache_8.6.0_GA_3033.UBUNTU10_64_amd64.deb
.
.
zcs-NETWORK-8.6.0_GA_3033.UBUNTU10_64.20101015012627/install.sh
zcs-NETWORK-8.6.0_GA_3033.UBUNTU10_64.20101015012627/README.txt
.
[root@mailhost tmp]# cd zcs-NETWORK-
8.6.0_GA_3033.UBUNTU10_64.20101015012627
[root@mailhost tmp/zcs-NETWORK-
8.6.0_GA_3033.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-dnscache...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 MariaDB software are running. If any application is running, you are asked to disable it. The default is **Yes** to disable the applications. Disabling MariaDB is optional, but highly recommended. Sendmail and Postfix must be disabled for the Zimbra Collaboration to start correctly.

3. Next, the installer checks to see that the prerequisite packages are installed as listed in the Other Dependencies section of the System Requirements for Zimbra Collaboration.

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

Installing Zimbra LDAP Master Server

You must configure the Zimbra LDAP Master 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 7, Configuring LDAP Replication.

1. Follow steps 1 through 4 in Starting the Installation Process on page 26 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-dnscache [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
3) Enable default backup schedule: 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)
    7)IP Mode:                              ipv4
    8) Default SSL digest:                      sha256
```

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.

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
   9) Ldap Bes Searcher 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/zmsetup081320xx-162256.log
Setting local config values...done.
.
.
.
Starting servers...done.
Setting up zimbra crontab...done.

Moving /tmp/zmsetup081320xx-162256.log to /opt/zimbra/log


Configuration complete - press return to exit
```

The installation of the LDAP server is complete.

Installing the 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 the following configuration options:

- The **Zimbra Mailbox Server** containing mailstore services and webapp services (mailstore server + UI server)

or

- The **Zimbra Web Application Server Split**, which includes:
  - Mailstore server providing the backend SOAP/REST functionality
  - UI server providing the web UI functionality (static html/js/css content)

You can have more than one of the above configurations. In a web application server split environment, you must have at least one mailstore server and one UI server in your configuration.

Important: *A web application server split environment must have proxy and memcached installed.*

Install Zimbra Mailbox Services

1. Follow steps 1 through 4 in Starting the Installation Process on page 26 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 mail server) and **zimbra-store**. 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-dnscache [Y] N
Install zimbra-snmp [Y] Y
Install zimbra-store [Y] Y
Install zimbra-apache [Y] Y
Install zimbra-spell [Y] Y



Installing:
    zimbra-core
    zimbra-logger
    zimbra-snmp
    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)
        +IP Mode:                             ipv4
   2) zimbra-ldap:                            Enabled
   3) zimbra-store:                           Enabled
        +Create Admin User:                   yes
        +Admin user to create: admin@mailstore-1.example.com
******* +Admin Password                       UNSET
        +Anti-virus quarantine user:: virus-
quarantine.gw98bctr0@mailstore-1.example.com
        +Enable automated spam training:      yes
        +Spam training user: spam.cc_v05j4@mailstore-1.example.com
        +Non-spam(Ham) training user:  ham.msoyzx@mailstore-
1.example.com
        +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
        +Install mailstore (service webapp):   yes
        +Install UI (zimbra,zimbraAdmin webapps): yes
        +Version update notification email: admin@mailstore-
1.example.com
        +Version update source email: admin@mailstore-1.example.com
 4) zimbra-mta:                               Enabled
 5) zimbra-snmp:                              Enabled
 6) zimbra-logger:                            Enabled
   7) zimbra-spell:                             Enabled
   8) zimbra-convertd:                          Enabled
   9) Enable VMware HA:                         Enabled
  10) 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: UNSET
3) Ldap port: 389
** 4) Ldap Admin password: UNSET
5) LDAP Base DN: cn=zimbra
6) Secure interprocess communications: yes
7) TimeZone: America/Chihuahua
8) IP Mode: ipv4
9) Default SSL digest: sha256
```

   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.

   To obtain the LDAP password, you will need to log on to the LDAP server as the zimbra user, and run the following command:

   zmlocalconfig -s zimbra_ldap_password

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

   - Type **7** to set the correct time zone.

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

  25) Install mailstore (service webapp):      yes
  26) Install UI (zimbra,zimbraAdmin webapps): yes
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.
- **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.
- If the zimbra-proxy package is not installed on the mailbox server, two menu options are displayed so you can preconfigure the mailbox server for use with the zimbra proxy server:
  - **Configure for use with mail proxy**
  - **Configure for use with web proxy**

  Set either or both of these to TRUE if you are going to set up zimbra-proxy. The zimbra-proxy ports display in the menu when these are set to TRUE.
-

- Configure the mailstore and webapp services either on a single server or in a split server configuration.
  - To install mailstore server only, set **Install UI (zimbra,zimbraAdmin webapps)** value to **no**, which will exclude the web services.
  - To install UI server only, set the **Install mailstore (service webapp)** to **no**, which will exclude mailstore services.
  - To install both the mailstore and UI services on the same server, confirm the **Install mailstore (service webapp)** and **Install UI (zimbra,zimbraAdmin webapps)** are set to **yes**. The default is **yes**.

Note: *See the release notes for additional configuration information for installing a split node environment.*

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

    The server is modified. Installing all the components and configuring the mailbox server can take a few minutes. This includes installing SSL certificates, setting passwords, setting ports, installing skins and zimlets, setting time zone preferences, and starting the servers, among other processes.
14. When **Configuration complete - press return to exit** displays, press **Enter**.

The installation of the mailbox server is complete.

```
Select, or press 'a' to apply config (? - help) a
Save configuration data? [Yes]
Save config in file: [/opt/zimbra/config.32288]
Saving config in /opt/zimbra/config.32288...Done

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

Operations logged to /tmp/zmsetup.070320xx-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 26 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** and **zimbra-dnscache** packages. 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-dnscache [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
    zimbra-dnscache

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
        +LDAP Base DN:                          cn=zimbra
        +Secure interprocess communications:    yes
        +TimeZone:                              (GMT-08.00) Pacific
Time (US & Canada)
        +IP Mode:                               ipv4
        +Default SSL digest:                    sha256


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

3) zimbra-dnscache:                           Enabled
   4) Enable default backup schedule:            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)LDAP Base DN:                         cn=zimbra
    6)Secure interprocess communications    yes
    7)TimeZone:                            (GMT-08.00) Pacific Time
(US & Canada)
    8)IP Mode:                              ipv4
    9) Default SSL digest:                  sha256
```

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 **7** to set the correct time zone.

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) Enable OpenDKIM:                         yes
  6) Notification address for AV alerts: admin@mta-1.example.com
**7) Bind password for postfix ldap user:     UNSET
**8) 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 **6**, 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 **7** and enter the postfix password.
- Type **8** 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.

route information (upstream mailbox server for each endclient)

-

Installing Zimbra Proxy on a separate server

The LDAP host name and the Zimbra LDAP password must be known to the proxy server. If not, the proxy server cannot contact the LDAP server and the installation fails.

1. Follow steps 1 through 4 in Starting the Installation Process on page 26 to open a SSH session to the server, log on to the server as **root**, and unpack the Zimbra software.

2. Select to install the zimbra-proxy package and the zimbra-memcached package. The other packages should be marked **N**. If you have not installed zimbra-proxy on another server, you must have at least one instance of zimbra-memcached installed to cache the data for NGINX, as shown in the following screen shot example.

Note: *If SNMP is used, the zimbra-snmp package must also be installed.*

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

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

   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 **7** to set the correct time zone.

5. Type **r** to return to the Main menu.
6. Type **2** to select zimbra-proxy.

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. See Set Up the SSH Keys.
- 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. See Enabling Server Statistics Display.
- Zimbra Collaboration 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, http://wiki.zimbra.com/wiki/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

In order for the server statistics to display on the administration console, the syslog configuration files must be modified.

Important: *Zimbra Collaboration supports the default syslog of a supported operating system. Depending on your operating system, the steps contained in this section might not be correct. See your operating system documentation for specific information about how to enable syslog.*

1. 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 either **syslog** or **rsyslog** to log statistics from remote machines:

For syslog:

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**

For syslog on Debian or Ubuntu:

a. Edit the /etc/default/syslogd file, add -r to the SYSLOGD_OPTIONS setting, **SYSLOGD_options="-r -m 0"**

b. Stop the syslog daemon. Type **/etc/init.d/sysklogd stop**

c. Start the syslog daemon. Type **/etc/init.d/sysklogd start**

For rsyslog:

a. Uncomment the following lines in **/etc/rsyslog.conf**

```
$modload imudp
$UDPServerRun 514
```

b. Restart rsyslog

For rsyslog on RHEL or CentOS:

a. Uncomment the following lines in **/etc/rsyslog.conf**

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

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

For syslog-ng on SuSE:

a. Uncomment the following from **/etc/syslog-ng/syslog-ng.conf**:

```
#
# uncomment to process log messages from network:
#
#udp(ip("0.0.0.0") port(514));
```

Spam/Ham Training on 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 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

1. 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:

- In case of Mailbox servers containing backend mailstore and UI services together (mailstore server + UI server), you can access the admin console directly using **https://<mailstore hostname>:<zimbraAdminPort>** (default value of zimbraAdminPort is 7071).
- In case of a deployment having even a single mailbox server running in Web Application server split mode, the admin console needs to be accessed strictly through the proxy using **https://<proxy hostname>:<zimbraAdminProxyPort>** after switching zimbraReverseProxyAdminEnabled to TRUE and restarting the proxy (default value of zimbraAdminProxyPort is 9071).

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

Note: *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****.*

2. 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 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 page 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 Account Migration 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

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/wiki/UnInstall_Zimbra.

5 Adding a Mailbox Server to a Single Server Configuration

In the Zimbra Collaboration (ZCS) single server environment, the LDAP, MTA, and mailbox services are on one machine. This chapter explains how to add a new machine that is configured as a mailbox server to a single server configuration and how to remove the mailbox server from the single server node.

Setup Requirements For Adding a Mailbox Server

- The new machine you are adding must have the same operating system, including the latest version and patch levels, as installed on the single server.
- The system clock must be configured with the same time on both machines.
- You must install the same version of the ZCS software that is installed on the single server node.
- A copy of the ZCS license needs to be added to a directory on the new machine.
- If you are adding Zimbra Proxy to ZCS, this should be installed on the existing single-server before you set up the new mailbox server. See the Multi-server Installation chapter, Installing zimbra-proxy section.

Overview of Process

- Zimbra Mailbox Server is installed on the prepared machine.
- Customized configuration for the single-server, such as custom themes and Zimlets are added to the new mailbox server.
- Commercial SSL certificates are added to the new mailbox server.
- User accounts are moved from the single server to the new mailbox server.
- If you are moving all accounts from the single server, the mailbox server is stopped on the single server machine.

Configuring the Mailbox Server

The host name and zmhostname configured on the mailbox server is the same as on the name on the single server.

Make sure you know the LDAP master password as you configure it on the sever that is being added. To find the master LDAP password on the single server node, type

```
zmlocalconfig -s zimbra_ldap_password
```

Important: *Before you begin make sure you have an up-to-date backup!*

1. Follow steps 1 through 4 in Starting the Installation Process on page 26 to log on to the server as **root** and unpack the Zimbra software.
2. Type Y for each package you are installing.
   - Install **zimbra-store**, and **zimbra-spell** (optional) packages. When zimbra-spell is installed, the **zimbra-apache** package also is installed.
   - If zimbra proxy is configured, install **memcached**.
   - The **zimbra-logger** package is installed only on one mailbox server. If you are moving all mailboxes to this server from the original single server, install the **zimbra logger** package.
   - If Archive and Discovery is installed on the single-server node, install **zimbra-archiving** on the new mailbox server.

Note: *If SNMP is being used, type* **Y** *for the* **zimbra-SNMP***. If SNMP is used, it is installed on every Zimbra server.*

---

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

   The mailbox server hostname is displayed. You must change the LDAP master host name and password to be the values configured on the single-server node.
   - Type **2**, press **Enter**, and type the LDAP host name.
   - 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.
5. Type **r** to return to the Main menu.
6. From the Main menu, type **2** to go to the Store configuration menu.
   - Type **4** and set the password for the administrator account. This should be the same password as configured on the original single-server node.

- 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.
- If you are setting up IMAP/POP proxy servers, type the corresponding number to enable the servers.
- If the zimbra-proxy is used and is installed on another server, configure the following menu options
  - Configure for use with mail proxy
  - Configure to use with web proxy

  Set either or both of these to TRUE if you are going to set up zimbra - proxy.
- Type the corresponding menu number to install the Zimbra license file. Enter the location of the license file. For example, if you saved the license file to the tmp directory, you would type /tmp/ZCSLicense.xml. You cannot proceed without a license file.
-

7. 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.
8. When **Save Configuration data to a file** appears, press **Enter**.
9. 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**.
10. 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.
11. When **Configuration complete - press return to exit** displays, press **Enter**.

The installation of the mailbox server is complete.

Adding Customized Features

Any customizing of themes, or Zimlets, and any signed certificates stored on the single-server must be added to the new mailbox server. See the Zimbra Collaboration Administrator Guide for information about adding the customized features.

Testing the Configuration

To make sure that the new mail store server is correctly configured, create a new user on the new mailbox server and log into the account to verify that your configuration is correct. See Provisioning Accounts in the Multiple-Server Installation chapter.

Move Mailboxes

The command, **zmmboxmove**, is run to move user accounts from the mailbox server on the single-sever node to the new mailbox server.

You can set global options to exclude items from the mailbox move. See the Zimbra Collaboration Administrator Guide, Managing User Accounts chapter for more information about the mailbox move feature.

Move the following types of mailboxes

- User accounts.
- Admin mailboxes. If you do not move the admin mailbox, you cannot log into the Zimbra Web Client.
- Spam and ham mailboxes.

Note: *If you were using Archive and Discovery on the single server mailbox, move the archival mailboxes as well.*

Move Mailboxes Using CLI zmmboxmove

1. To move a mailbox to a new server

   zmmboxmove -a <email@address> --from <servername> --to <servername>

2. To verify that the content of the mailbox was moved successfully, go to the administration console, select the account that was moved. Click **View Mail** on the toolbar. When the account opens, verify that the account's content is displayed and can be opened.

3. Purge the mailbox from the old server

   zmpurgeoldmbox -a <email@address> -s <oldservername>

Turn Off Mailbox Server on Single-Server Node

When all mailboxes have moved from the single-server node to the new mailbox server node, disable the Mailbox services on the original single-server machine.

1. On the original single-server node, disable the following mailbox server components:

   - mailbox. zmprov -l ms <singleserver.com> **-- -zimbraServiceEnabled mailbox**

- logger. zmprov -l ms <singleserver.com> **-- -zimbraServiceEnabled logger**
- stats. zmprov -l ms <singleserver.com> **-- -zimbraServiceEnabled stats**
- spell. zmprov -l ms <singleserver.com> **-- -zimbraServiceEnabled spell**
- convertd. zmprov -l ms <singleserver.com> **-- -zimbraServiceEnabled convertd**

If archiving was installed, disable it as well,

zmprov -l ms <singleserver.com> **-- -zimbraServiceEnabled archiving**

2. After the mailbox services are disabled, verify that antispam, antivirus, ldap, mta, snmp, proxy, and memcached are the only services on the original single-server node.

   zmprov -l gs <singleserver.com> | grep -i serviceenabled

6 Configuring Multi-Master Replication

Set up multi-master LDAP replication to have a copy of the LDAP database saved on each server in a group of LDAP servers identified for multi-master replication (MMR). The database can be updated by any member of the group. If one master fails, the other masters continue to update the database.

The Zimbra install program is used to configure the multi-master LDAP servers. Each master LDAP server is given an unique identifier when they are configured and zmlocalconfig is used to add the ldap server to the multi-master group.

You can also promote an existing replica to be part of the multi-master group.

Topics in this chapter include:

Managing Multiple Master LDAP Servers

When you enable multi-master replication, you assign a server ID to each master server to identify them in the group. This is used to distinguish the servers in the group and to help resolve conflicts that might occur.

In addition, each server is configured to assign internal replication ID's that are unique to that specific server. Other LDAP master server can use the same replication ID, but within the server, these replication IDs must be unique.

You can run the ZCS multiple master CLI, **zmldapquery-mmr** from a specific master to see the server ID for that master and all multi-master servers that are in the group and to see the replication ID values for those masters.

On the server, enter the command as

/opt/zimbra/libexec/zmldapquery-mmr

Enabling Multi-Master Replication on Initial Stand-Alone LDAP Master

Before you can enable the multi-master replication feature, you must know the hostname of the first secondary master that is being added to the group. The hostname is entered when you enable the feature. Once you enable the multi-master replication feature, you do not need to run the command again.

When zmlocalconfig is run the first time, the master LDAP servers are configured as follows:

- The first master LDAP server ID is set to 1.
- The master LDAP server is put in a group with a secondary master that is listening to LDAP on port 389.
- The replication ID is set to 100 by default on the secondary master.
- Writes initiated from the server go to the ldap master1 by default. If ldap master1 is down, writes move to ldap master2

1. To enable the feature run:

   ./libexec/zmldapenable-mmr -s 1 -m ldap://<<master2.example.com>>:389/

2. Once the feature is enabled use the zmlocalconfig command to add the LDAP servers to a group.

   zmlocalconfig -e ldap_master_url="ldap://<<master1.example.com>>:389 ldap://<<master2.example.com>>:389"

Installing a Secondary Master LDAP Server

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

Passwords Required to Install the Secondary Master

Before you install a secondary master, you must know the following passwords:

- Zimbra admin LAP password
- LDAP replication password
- NGINX LDAP password
- Amavis LDAP password
- Postfix LDAP password

To find these passwords, on the ZCS server run

zmlocalconfig -s | grep passw | grep ldap

Setting Up a Secondary Master LDAP Server

1. Follow steps 1 through 4 in Starting the Installation Process on page 26 to open a 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.
3. Type **Y**, and press **Enter** to modify the system. The selected packages are installed.

   The Main menu shows the default entries for the LDAP server.
4. Type **1** to display the Common Configuration submenus.
   a. Type **2** to change the **Ldap Master host** name to the name of the primary master name host (example, master1.example.com).
   b. Type **4** to change the **LDAP admin password** to the Zimbra admin password of the primary master.

   Type **r** to return to the main menu.
5. Type **2** to display the LDAP configuration submenu.
   a. Type **4** to change the type to **mmr**.
   b. Note that **5**, LDAP Server ID, is set to **2**. If this is the second master, leave it unchanged. If it the third or later master, select 5 and update the server ID.

   The next four steps are to change the default passwords on this server to match the passwords on the master1 LDAP server.
   c. Type **7** to change the LDAP replication password.
   d. Type **8** to change the LDAP postfix password.
   e. Type **9** to change the LDAP amavis password.
   f. Type **10** to change the LDAP NGINX password.

   Type **r** to return to the main menu.
6. 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 is complete.
10. Update the **ldap_master_url** attribute to contain both masters, enter this new master as the first master in the list.

zmlocalconfig -e ldap_master_url="ldap://<<master2.example.com>>:389 ldap://<<master1.example.com>>:389"

Promote Existing Replicas to Multi-Master LDAP Servers

In an existing ZCS setup where there is already a single master and multiple replicas, you can promote an existing replica to become a secondary master.

1. On the master LDAP server find the LDAP replication, Postfix, Amavis, and NGINX passwords

   zmlocalconfig -s | grep passw | grep ldap

2. Change the LDAP passwords on the server you are promoting to be the same as the first master LDAP server.

   - LDAP replication password = zmldappasswd -l <password>
   - LDAP postfix password = zmldappasswd -p <password>
   - LDAP amavis password = zmldappasswd -a <password>
   - LDAP NGINX password = zmldappasswd -n <password>

3. Assign the next Server ID to this master. This example is 3

   /opt/zimbra/libexec/zmldappromote-replica-mmr -s 3

4. Update the **ldap_master_url** attribute to add the master to the list.

   zmlocalconfig -e ldap_master_url="ldap://<<master1.example.com>>:389 ldap://<<master2.example.com>>:389 ldap://<<master3.example.com>>:389"

This updates the replica to be a multi-master replica, enabled with a server ID. It is automatically configured to be a paired master with the master it was previously replicating from.

Deleting a Multi-Master Replication Node

To delete a multi-master replication (MMR) node, use the following steps.

Note: *Deleting an MMR node can only be performed in ZCS 8.0.7 and later.*

1. Update the **ldap_master_url** and **ldap_url** on every node, removing the LDAP MMR node that will be shut down.
2. Wait 5-10 minutes to ensure the modification is in place.
3. Monitor **/var/log/zimbra.log** on the MMR node that will be shut down and confirm it is no longer receiving modification traffic.
4. Run **ldap stop** on the MMR node that is being shut down.

5. Log into the remaining MMR nodes and perform the following:
   a. **/opt/zimbra/libexec/zmldapmmrtool -q**
   b. Find the matching RID for the MMR node you shut down
   c. **/opt/zimbra/libexec/zmldapmmrtool -d -o RID**

Example of Deleting an MMR Node

The following is an example of using **zmldapmmrtool**:

1. There are three MMR servers, ldap1.example.com, ldap2.example.com, ldap3.example.com, with ldap3.example.com being shut down.

   ```
   zimbra@ldap1:/tmp/mmr$ ./zmldapmmrtool -q
   Master replication information
   Master replica 1
   rid: 100 URI: ldap://ldap2.example.com:389/ TLS: critical
   Master replica 2
   rid: 101 URI: ldap://ldap3.example.com:389/ TLS: critical
   ```

2. The RID being used by ldap3.example.com is 101. This agreement can be deleted with:

   ```
   zimbra@ldap1:/tmp/mmr$ ./zmldapmmrtool -d -o 101
   ```

3. Confirm the deletion.

   ```
   zimbra@ldap1:/tmp/mmr$ ./zmldapmmrtool -q
   Master replication information
   Master replica 1
   rid: 100 URI: ldap://ldap2.example.com:389/ TLS: critical
   zimbra@ldap1:/tmp/mmr$
   ```

4. Repeat on the remaining node(s).

Monitoring Multiple LDAP Master 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 master servers.*

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 additional servers. The following screen-shot shows the additional master servers are in sync with the master server, as indicated by the **Code:0** and **Status: In Sync**, and master server **ldap005** is currently down, as indicated by **Code: 4** and **Status: Server down**.

```
zimbra@ldap002.example.com
Master: ldap://ldap003.example.com:389 Code: 0 Status: In Sync CSN:
20120528123456.123456Z#000000#001#000000
Master: ldap://ldap004.example.com:389 Code: 0 Status: In Sync CSN:
20120528123456.123456Z#000000#001#000000
Master: ldap://ldap005.example.com:389 Code: 4 Status: Server down
```

7 Configuring LDAP Replication

Topics in this chapter include:

Configuring LDAP Replication Overview

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

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

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

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

Installing Zimbra Master LDAP Server

You must install the master LDAP server before you can install replica LDAP servers. Refer to Installing Zimbra LDAP Master Server on page 28 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 26 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-logger [Y] n
Install zimbra-mta [Y] n
Install zimbra-dnscache [N] n
Install zimbra-snmp [Y] n
Install zimbra-store [Y] n
Install zimbra-apache [Y] n
Install zimbra-spell [Y] n
Install zimbra-convertd [N] n
Install zimbra-memcached [Y] n
Install zimbra-proxy [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
.
.
.
.
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.

```
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)
```

4. Type **2** to change the **Ldap Master host** name to the name of the Master LDAP host.
5. Type **3**, to 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 Admin user password. Type **r** to return to the main menu.
7. Type **2** to display the LDAP configuration submenu.

```
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
```

- 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

8. 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
```

9. When **Save Configuration data to a file** appears, press **Enter**.
10. 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.
11. When **Installation complete - press return to exit** displays, press **Enter**.

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

Test the Replica

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

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

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

   zmprov cd <domain name>

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

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

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

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

Configuring Zimbra Servers to Use LDAP Replica

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

1. Stop the Zimbra services on the server. Type zmcontrol stop.
2. Update the ldap_url value. Enter the replica LDAP server URL

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

   Enter more than one replica hostnames in the list typed as "ldap://<replicahost1> ldap://<replicahost2> ldap://<masterhost>". The hosts are tried in the order listed. The master URL must always be included and is listed last.
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 <zmhostname> -zimbraServiceEnabled ldap
```

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

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

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* ***l*****dap_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

This document contains Zimbra Collaboration system requirements and language information for both the Network Edition and Open Source Edition.

	Requirements

Servers	**Evaluation and Testing**
	• Intel/AMD 64-bit CPU 1.5 GHz
	• RAM requirements:
	  • For single server installations, a minimum of 8GB of RAM is required.
	  • For multi-server installations, contact Zimbra sales for recommendations.
	• 5 GB free disk space for software and logs
	• Temp file space for installs and upgrades*
	• Additional disk space for mail storage
	Production environments
	• Intel/AMD 2.0 GHZ+ 64-bit CPU
	• RAM requirements:
	  • For single server installations, a minimum of 8GB of RAM is required.
	  • For multi-server installations, contact Zimbra sales for recommendations.
	• Temp file space for installs and upgrades*
	• 10 GB free disk space for software and logs (SATA or SCSI for performance, and RAID/Mirroring for redundancy)
	• Additional disk space for mail storage
	*Temp files space: The zimbra-store requires 5GB for /opt/zimbra, plus additional space for mail storage. The other nodes require 100MB.
	General Requirements
	• Firewall Configuration should be set to “No firewall”.
	• RAID-5 is not recommended for installations with more than 100 accounts.

Operating System Network Edition	The following operating systems are supported: • Red Hat® Enterprise Linux® 7 (64-bit) • CentOS Linux® 7 (64-bit) • Red Hat Enterprise Linux 6 (64-bit), patch level 4 or later is required • CentOS Linux 6 (64-bit), patch level 4 or later is required • Ubuntu 14.04 LTS Server Edition (64-bit) • Ubuntu 12.04.4 LTS Server Edition (64-bit) running the saucy (3.11) or later kernel is required. Note: If the original install was done with Ubuntu 12.04.2 or earlier, manual intervention is required to switch to the saucy (3.11) or later kernel series. See https://wiki.ubuntu.com/Kernel/LTSEnablementStack for further information. • SUSE Linux Enterprise Server (SLES) 11, SP3 (64-bit) is required. ***Important! Zimbra Collaboration 8.6 is the last supported release of SLES 11.***
Virtualization Network Edition	The following hypervisors are supported: • VMware vSphere 4.x • VMware vSphere 5.x
Operating System Open Source Edition	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.
File Systems	The following file systems are supported: • **ext3** or **ext4** file system for Linux deployments • **NFS** for backup only

Other Dependencies	Netcat (nc) is required on all operating systems using Zimbra Collaboration. The nc utility must be installed prior to installation or upgrading. For SUSE and Ubuntu systems, disable AppArmor and verify that services are not running before installing Zimbra Collaboration. For Red Hat Enterprise, Fedora Core and SUSE operating systems, the server must also have the following installed: • **NPTL**. Native POSIX Thread Library • **Sudo**. Superuser, required to delegate admins. • **libidn**. For internationalizing domain names in applications (IDNA) • **GMP**. GNU Multiple-Precision Library. For Ubuntu 14 and Ubuntu 12: • Sudo • libidn11 • libpcre3 • libexpat1 • libgmp3c2
Miscellaneous	• SSH client software to transfer and install the Zimbra Collaboration 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
 	
Note: Other configurations may work.
	The following operating system/browser combinations are supported:
	
	Windows XP with required updates, Vista, Windows 7, or Windows 8 with one of the following:
	• Internet Explorer 8.0 and higher
	  • IE8.x for XP
	  • IE9.x and higher for Vista/Windows 7
	  • IE10 and higher for Windows 8
	• The latest stable release of:
	  • Firefox
	  • Safari
	  • Google Chrome
	
	Mac OS X 10.5, 10.6, 10.7, or 10.8 with one of the following:
	• The latest stable release of:
	  • Firefox
	  • Safari
	  • Google Chrome
	
	Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following:
	• The latest stable release of:
	  • Firefox
	  • Google Chrome

Administrator Console Monitor	Display minimum resolution 1024 x 768

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 XP with required updates, Vista, Windows 7, or Windows 8 with one of the following:
	• Internet Explorer 8.0 and higher
	  • IE8.x for XP
	  • IE9.x and higher for Vista/Windows 7
	  • IE10 and higher for Windows 8
	• The latest stable release of:
	  • Firefox
	  • Safari
	  • Google Chrome
	
	Mac OS X 10.5, 10.6, 10.7, or 10.8 with one of the following:
	• The latest stable release of:
	  • Firefox
	  • Safari
	  • Google Chrome
	
	Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following:
	• The latest stable release of:
	  • Firefox
	  • Google Chrome

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 XP with required updates, Vista, Windows 7, or Windows 8 with one of the following:
	• Internet Explorer 8.0 and higher
	  • IE8.x for XP
	  • IE9.x and higher for Vista/Windows 7
	  • IE10 and higher for Windows 8
	• The latest stable release of:
	  • Firefox
	  • Safari
	  • Google Chrome
	
	Mac OS X 10.5, 10.6, 10.7, or 10.8 with one of the following:
	• The latest stable release of:
	  • Firefox
	  • Safari
	  • Google Chrome
	
	Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following browsers:
	• The latest stable release of:
	  • Firefox
	  • Google Chrome

End User Computers Using Other Clients	Minimum • Intel/AMD/Power PC CPU 750MHz • 256MB RAM Recommended • Intel/AMD/Power PC CPU 1.5GHz • 512MB RAM Operating system POP/IMAP combinations • Windows XP SP 3, Vista SP 2, Windows 7 with Outlook Express 6, Outlook 2003, (MAPI), Thunderbird • Fedora Core 4 or later with Thunderbird • Mac OS X 10.4 or later with Apple Mail **Accessibility and Screen Readers** Zimbra recommends that customers requiring use of screen readers for accessibility leverage the use of the Standard Zimbra Web Client (HTML). Zimbra continues to invest in improving the accessibility of this interface. **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.
Exchange Web Services	EWS Clients • Outlook 2011 (MAC only), Apple Desktop Clients (OS X, 10.8+) EWS Interoperability • Exchange 2007+
Monitor	Display minimum resolution 1024 x 768
Internet Connection Speed	128 kbps or higher

Zimbra Connector for Outlook Network Edition only	
Operating System	• Windows 8 • Windows 7 • Vista • Windows XP with required updates ***Important****! Windows XP is deprecated. The 8.x series of Zimbra Collaboration is the last release to support Microsoft Outlook 2003 and Microsoft Windows XP*
Microsoft Outlook	• Outlook 2013: 32-bit and 64-bit editions of Microsoft Outlook are supported. • Outlook 2010: 32-bit and 64-bit editions of Microsoft Outlook are supported. • Outlook 2007: Client computers must have Microsoft Office Outlook 2007 SP3 or later installed. • Outlook 2003: Client computers must have Microsoft Office Outlook 2003 SP3 or later installed. ***Important!*** *Outlook 2003 is deprecated. The 8.x series of Zimbra Collaboration is the last release to support Microsoft Outlook 2003 and Microsoft Windows XP.*

Zimbra Mobile Network Edition only

Zimbra Mobile (MobileSync) provides mobile data access to email, calendar, and contacts for users of selected mobile operating systems, including:

Smartphone Operating Systems:

- iOS6, iOS7, iOS8
- Android 2.3 and above
- Windows Mobile 6.0 and above
- Microsoft Outlook using the Exchange ActiveSync (EAS)

Non-Smartphone Operating Systems:

- Various device/operating system combinations with mobile WAP browser.

See the Zimbra web site http://www.zimbra.com/products/zimbra_mobile.html for more information.

Zimbra Touch Client - Network Edition only

Supported devices for the Zimbra Touch Client include:

- iOS6+: iPad®, iPad mini®, iPhone®, iPod touch®
- Android 4.0+: Nexus 7, Nexus 10, Samsung Galaxy Tab™, Samsung Galaxy S® III, Samsung Galaxy S® 4, Galaxy Nexus™

Zimbra Connector for BlackBerry Enterprise Server

Network Edition only

Zimbra Connector for BlackBerry Enterprise Server (ZCB) provides seamless, real-time synchronization of Zimbra user mailbox data to BlackBerry devices. See the Zimbra web site http://www.zimbra.com/products/blackberry-enterprise-server.html for more information.

Available Languages

This section includes information about available languages, including End User Translations and Administrator Translations.

End User Translations

Component	Category	Languages
Zimbra Web Client	Application/UI	Arabic, Basque (EU), Chinese (Simplified PRC and Traditional HK), Danish, Dutch, English (AU, UK, US), French, French Canadian, German, Hindi, Hungarian, Italian, Japanese, Korean, Malay, Polish, Portuguese (Brazil), Portuguese (Portugal), Romanian, Russian, Spanish, Swedish, Thai, Turkish, Ukrainian
Zimbra Web Client - Online Help (HTML)	Feature Documentation	Dutch, English, Spanish, French, Italian, Japanese, German, Portuguese (Brazil), Chinese (Simplified PRC and Traditional HK), Russian
Zimbra Web Client - End User Guide (PDF)	Feature Documentation	English
Zimbra Connector for Microsoft Outlook	Installer + Application/UI	Arabic, Basque (EU), Chinese (Simplified PRC and Traditional HK), Danish, Dutch, English (AU, UK, US), French, French Canadian, German, Hindi, Hungarian, Italian, Japanese, Korean, Malay, Polish, Portuguese (Brazil), Portuguese (Portugal), Romanian, Russian, Spanish, Swedish, Thai, Turkish, Ukrainian
Zimbra Connector for Microsoft Outlook - End User Guide (PDF)	Feature Documentation	English

Administrator Translations

Component	Category	Languages
Zimbra Admin Console	Application	Arabic, Basque (EU), Chinese (Simplified PRC and Traditional HK), Danish, Dutch, English (AU, UK, US), French, French Canadian, German, Hindi, Hungarian, Italian, Japanese, Korean, Malay, Polish, Portuguese (Brazil), Portuguese (Portugal), Romanian, Russian, Spanish, Swedish, Turkish, Ukrainian
Zimbra Admin Console Online Help (HTML)	Feature Documentation	English
"Documentation" *Install + Upgrade / Admin Manual / Migration / Import / Release Notes / System Requirements*	Guides	English
Zimbra Connector for Microsoft Outlook - Admin Guide (PDF)	Install + Configuration Guide	English

Revision History

Zimbra Collaboration 8.6.0, GA
Released December, 2014

Zimbra, Inc.
3000 Internet Blvd., Suite 200
Frisco, Texas 75034

www.zimbra.com

Zimbra Collaboration 8.6.0

December 2014

Index

Symbols