



Zimbra Collaboration Multi-Server Installation Guide

v8.8.9, July, 2018

Table of Contents

License	1
Introduction	2
Audience	2
Zimbra Collaboration License	2
For More Information	2
Support and Contact Information	2
Zimbra Port Mapping	3
External access	3
Internal access	3
System Access and Intra-Node Communication	6
Planning for the Installation	8
Zimbra Application Packages	8
Configuration Examples	10
Downloading the Zimbra Software	10
Zimbra Licensing (Network Edition Only)	11
Zimbra License Requirements	11
License Usage by Zimbra Collaboration Account Type	12
License Activation	12
Automatic License Activation	12
Manual License Activation	12
License Not Installed or Activated	13
Obtaining a License	13
Menu-Driven Configuration	13
Main Menu options	14
Common Configuration Options	16
Ldap configuration	17
Zimbra Logger	18
MTA Server Configuration Options	19
DNS Cache	20
Snmp configuration	21
Store configuration	22
Proxy configuration	24
IMAPD configuration	25
Scanning Attachments in Outgoing Mail	26
Overview of the Zimbra Proxy Server	26
Zimbra Proxy Components and Memcached	27
Zimbra Proxy Architecture and Flow	27
Zimbra Proxy Position in Zimbra Collaboration Runtime	28

Deployment Strategy	28
Configuration during installation	29
Zimbra Proxy Ports	29
Configuring for Virtual Hosting	30
Preparing Your Server Environment	31
System Requirements	31
Modifying Operating System Configurations	31
Configuring High-Fidelity Document Preview (Network Edition Only)	31
Install Language and Font Packages	32
DNS Configuration Requirement	32
Multiple-Server Installation	33
Starting the Installation Process	33
Installing Zimbra LDAP Master Server	36
Installing the Zimbra Mailbox Server	41
Install Zimbra Mailbox Services	42
Installing Zimbra MTA on a Server	49
Installing Zimbra Proxy	53
Installing on the MTA Server	53
Installing on a separate server	54
Installing Zimbra IMAPD	57
Installing on the Mailbox Server	57
Installing on a separate server	58
Installing zimbra-archiving Package	61
Installing the zimbra-SNMP Package	62
Final Set-Up	63
Set Up the SSH Keys	63
Enabling Server Statistics Display	63
Spam/Ham Training on MTA servers	64
Verifying Server Configuration	64
Logging on to the Administration Console	65
Post Installation Tasks	65
Defining Classes of Service	65
Provisioning Accounts	66
Configuring One Account	66
Configuring Many Accounts at Once	66
Import the Content of Users' Mailboxes	66
Ephemeral Data Migration	67
Installing Zimbra X Webclient	67
Uninstalling Zimbra Collaboration	70
Adding a Mailbox Server to a Single Server Configuration	71
Setup Requirements For Adding a Mailbox Server	71

Overview of Process	71
Configuring the Mailbox Server	71
Adding Customized Features	73
Testing the Configuration	74
Move Mailboxes	74
Move Mailboxes Using CLI zmmboxmove	74
Turn Off Mailbox Server on Single-Server Node	74
Configuring Multi-Master Replication	76
Managing Multiple Master LDAP Servers	76
Installing a Secondary Master LDAP Server	77
Passwords Required to Install the Secondary Master	77
Setting Up a Secondary Master LDAP Server	77
Promote Existing Replicas to Multi-Master LDAP Servers	78
Deleting a Multi-Master Replication Node	79
Example of Deleting an MMR Node	79
Monitoring Multiple LDAP Master Status	80
Feature Requirement	80
Error Codes and Status Explanations	80
Configuring LDAP Replication	82
Configuring LDAP Replication Overview	82
Installing Zimbra Master LDAP Server	82
Enable Replication on the LDAP Master	82
Installing a Replica LDAP Server	82
Test the Replica	85
Configuring Zimbra Servers to Use LDAP Replica	86
Uninstalling an LDAP Replica Server	86
Remove LDAP Replica from All Active Servers	86
Disable LDAP on the Replica	87
Monitoring LDAP Replication Status	87
Feature Requirement	87
Error Codes and Status Explanations	87
System Requirements for Zimbra Collaboration	89
Zimbra Connector for Outlook (Network Edition Only)	94
Zimbra Mobile (Network Edition Only)	95
Zimbra Touch Client (Network Edition Only)	95
Available Languages	96
End User Translations	96
Administrator Translations	96
Zimbra Network NG Modules: First Steps	98
Switching to Backup NG	98
Backup Path Limitations	98

Backup NG Initialization	98
Switching to Mobile NG	98
What Happens after the Switch	99
Mobile NG Initialization	99
Switching to HSM NG	99
Switching to Admin NG	100
Admin NG Initialization	100

License



Synacor, Inc., 2016-2018

© 2016-2018 by Synacor, Inc. Zimbra Collaboration Multi-Server Installation Guide

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License unless another license agreement between you and Synacor, Inc. provides otherwise. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/4.0> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Synacor, Inc., 2016
40 La Riviere Drive, Suite 300
Buffalo, New York 14202

<http://www.synacor.com>

Introduction

Information in this guide is intended for persons responsible for installing 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 Network Edition 8.8.9.

Audience

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

Zimbra Collaboration License

A Zimbra license is required in order to create accounts in Zimbra Collaboration Network Edition. You cannot install Zimbra Collaboration Network Edition without a license. For more information about licenses, see [Zimbra License Requirements](#)

If you do not have a license, go to Zimbra's website <https://www.zimbra.com> to obtain a license from the Network Downloads area.

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, <https://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 <https://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.

- Network Edition customers can contact support at support@zimbra.com.
- Explore the [Zimbra Forums](#) for answers to installation or configuration problems.
- Join the Zimbra Community Forum, to participate and learn more about 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.

Zimbra Port Mapping

External access

These are ports typically available to mail clients.

Port	Protocol	Zimbra Service	Description
25	smtp	mta	incoming mail to postfix
80	http	mailbox / proxy	web mail client (disabled by default in 8.0)
110	pop3	mailbox / proxy	POP3
143	imap	mailbox / proxy	IMAP
443	https	mailbox / proxy - web mail client	HTTP over TLS
465	smtps	mta	Incoming mail to postfix over TLS (Legacy Outlook only? If possible, use 587 instead)
587	smtp	mta	Mail submission over TLS
993	imaps	mailbox / proxy	IMAP over TLS
995	pop3s	mailbox / proxy	POP3 over TLS
3443	https	proxy	User Certificate Connection Port (optional)
5222	xmpp	mailbox	Default server port
5223	xmpp	mailbox	Default legacy SSL port
9071	https	proxy admin console	HTTP over TLS (optional)

Internal access

These are ports typically only used by the Zimbra system itself.

Port	Protocol	Zimbra Service	Description
389	ldap	ldap	LC(ldap_bind_url)
636	ldaps	ldaps	if enabled via LC(ldap_bind_url)
3310	-	mta/clamd	zimbraClamAVBindAddress
5269	xmpp	mailbox	Server-to-Server communications between servers on the same cluster.
7025	lmtp	mailbox	local mail delivery; zimbraLmtpBindAddress
7026	milter	mailbox	zimbra-milter; zimbraMilterBindAddress
7047	http	conversion server	Accessed by localhost by default; binds to '*'
7071	https	mailbox	admin console HTTP over TLS; zimbraAdminBindAddress
7072	http	mailbox	ZCS nginx lookup - backend http service for nginx lookup/authentication
7073	http	mailbox	ZCS saslauthd lookup - backend http service for SASL lookup/authentication (added in ZCS 8.7)
7110	pop3	mailbox	Backend POP3 (if proxy configured); zimbraPop3BindAddress
7143	imap	mailbox	Backend IMAP (if proxy configured); zimbraImapBindAddress
7171	-	zmconfigd	configuration daemon; localhost
7306	mysql	mailbox	LC(mysql_bind_address); localhost
7307	mysql	logger	logger (removed in ZCS 7)

7780	http	mailbox	spell check
7993	imaps	mailbox	Backend IMAP over TLS (if proxy configured); zimbraImapSSLBindAddress
7995	pop3s	mailbox	Backend POP3 over TLS (if proxy configured); zimbraPop3SSLBindAddress
8080	http	mailbox	Backend HTTP (if proxy configured on same host); zimbraMailBindAddresses
8143	imap	imapd	IMAP server running independent of the mailboxd process
8443	https	mailbox	Backend HTTPS (if proxy configured on same host); zimbraMailSSLBindAddress
8465	milter	mta/opensslkim	OpenDKIM milter service; localhost
8735	zextras	mailbox	internal mailbox to mailbox communication.
8736	zextras	mailbox	distributed configuration
8993	imap	imapd	IMAP over TLS via IMAPD server running independent of the mailboxd process
10024	smtp	mta/amavisd	to amavis from postfix; localhost
10025	smtp	mta/master	opensslkim; localhost
10026	smtp	mta/amavisd	"ORIGINATING" policy; localhost
10027	smtp	mta/master	postjournal
10028	smtp	mta/master	content_filter=scan via opensslkim; localhost
10029	smtp	mta/master	"postfix/archive"; localhost
10030	smtp	mta/master	10032; localhost
10031	milter	mta/cbpolicyd	cluebringer policyd

10032	smtp	mta/amavisd	(antispam) "ORIGINATING_POST" policy
10663	-	logger	LC(logger_zmrrdfetch_port); localhost
23232	-	mta/amavisd	amavis-services / msg-forwarder (zeromq); localhost
23233	-	mta/amavisd	snmp-responder; localhost
11211	memcached	memcached	nginx route lookups, mbox cache (calendar, folders, sync, tags); zimbraMemcachedBind Address

System Access and Intra-Node Communication

In a multi-node environment the typical communication between nodes required includes:

Destination	Source(s)	Description
ALL		
22	ALL	SSH (system & zmrzd): host management
udp/53	ALL	DNS (system dnscache): name resolution
Logger		
udp/514	ALL	syslog: system and application logging
LDAP		
389	ALL	all nodes talk to LDAP server(s)
MTA		
25	ldap	sent email (cron jobs)
25	mbox	sent email (web client, cron, etc.)
antivirus		
3310	mbox	zimbraAttachmentsScanURL (not set by default)
memcached		
11211	mbox	mbox metadata data cache
11211	proxy	backend mailbox route cache
Mailbox (mbox)		
80	proxy	backend proxy http

110	proxy	backend proxy pop3
143	proxy	backend proxy imap
443	proxy	backend proxy https
993	proxy	backend proxy imaps
995	proxy	backend proxy pop3s
7025	mta	all mta talk to any mbox (LMTP)
7047	mbox	localhost by default; zimbraConvertURL
7071	mbox	all mbox talk to any mbox (Admin)
7072	proxy	zmlookup; zimbraReverseProxyLookupTarget
7073	mta	sasl auth; zimbraMtaAuthTarget (since ZCS 8.7)

Important: You cannot have any other web server, database, *LDAP*, or *MTA* server running, when you install Zimbra Collaboration. If you have installed any of those applications before you install Zimbra software, disable them. During Zimbra Collaboration installation, Zimbra makes global system changes that may break applications that are on your server.

Planning for the Installation

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

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 Collaboration 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 Zimbra Collaboration.



The Zimbra LDAP server must be configured before any other servers.

You can set up LDAP replication, configuring a master LDAP server and replica LDAP servers.

- **Zimbra Store:** This package 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 **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 Zimbra Collaboration services using **nginx**. 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 required as of ZCS 8.7.



By default Zimbra Proxy is configured to perform strict server name enforcement of the HTTP 'Host' header sent by clients for new installs. Strict server name enforcement may be disabled during the post-install configuration process in the Zimbra Proxy configuration section or using the `zimbraReverseProxyStrictServerNameEnabled` configuration option. Please see the Zimbra Proxy section of the administration guide for more details.

- **Zimbra Memcached:** This package is automatically selected when the **Zimbra-Proxy** package is installed and provides access to **Memcached**.



At least one server must run **zimbra-memcached** when the Zimbra Proxy service is in use.

You can use a single memcached server with one or more Zimbra proxies.

- **Zimbra SNMP:** Installing this package is optional.



If you choose to install **Zimbra-SNMP** for monitoring, this package should be installed on every Zimbra server.

- **Zimbra Logger:** Installing this package is optional. It is installed on one mailbox server. It provides tools for **syslog** aggregation and reporting.



- If you do not install **Zimbra Logger**, the server statistics section of the administration console will not display.
- The **Zimbra Logger** package must be installed at the same time as the **Zimbra Store** package.

- **Zimbra Spell:** This package is optional. It provides the open source spell checker **Aspell** used by the Zimbra Web Client.
- **Zimbra Apache:** This package is installed automatically when **Zimbra Spell** or **Zimbra Converttd** is installed.
- **Zimbra Converttd:** This package should be installed on at least one **Zimbra-Store** server. Only one **Zimbra-Converttd** package needs to be present in the Zimbra Collaboration environment. The default is to install one **Zimbra-Converttd** on each **Zimbra-Store** server.
- **Zimbra Archiving:** The Zimbra Archiving and Discovery feature is an optional feature for Zimbra Collaboration **Network Edition**.
Archiving and Discovery offers the ability to store and search all messages that were delivered to or sent by Zimbra Collaboration.
This package includes the **cross mailbox search** function which can be used for both live and archive mailbox searches.



Using Archiving and Discovery can trigger additional mailbox license usage. To find out more about Zimbra Archiving and Discovery, contact Zimbra sales.

- **Zimbra Chat:** Installing this package is optional. This package should be installed on at least

one **Zimbra-Store** server. Zimbra Chat includes a server extension with all the necessary modules to run an embedded XMPP Server, and an End-User Zimlet which connects to the server extension and offer to the users a rich point-to-point text-chat conversations. Zimbra Chat is marked as GA and supported starting Zimbra Collaboration 8.8.



The Zimbra Chat package must be selected and installed on every **Zimbra-Store**.

- **Zimbra Drive:** Installing this package is optional. This package should be installed on at least one **Zimbra-Store** server. *Zimbra Drive includes a server extension with all the necessary modules to connect and authenticate *Zimbra Users against a ownCloud or NextCloud Server, and an End-User Zimlet which allow users to perform actions to the their documents stored on ownCloud or Nextcloud. Zimbra Drive is marked as GA and supported starting Zimbra Collaboration 8.8.



The Zimbra Drive package must be selected and installed on every **Zimbra-Store**.



Zimbra Drive provides only a connectivity to a ownCloud or NextCloud Server. And is the Customer responsibility to maintain, backup, and protect the data stored on this ownCloud or NextCloud Servers.

The Zimbra server configuration is menu driven. The installation menu shows you the default configuration values. The menu displays the logical host name and email domain name [mailhost.example.com] as configured on the computer. You can change any of the values. For single server installs, you must define the administrator's password, which you use to log on to the administration console, and you specify the location of the Zimbra license xml file.

Configuration Examples

Zimbra Collaboration 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 Collaboration software download, go to <https://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.

Instruction guides are available from the Help Center page or from <https://www.zimbra.com/>

Zimbra Licensing (Network Edition Only)

Zimbra Collaboration licensing gives administrators better visibility and control into the licensed features they plan to deploy. The following is a summary of the feature attributes of a Zimbra Collaboration Network Edition license.

- **Accounts limit.** The maximum number of accounts you can create and the number of accounts created are shown.
- **Mobile accounts limit.** The maximum number of accounts that can have the native mail mobile feature enabled.
- **Touch Client accounts limit.** The maximum number of accounts that can have the touch client mobile feature enabled.
- **MAPI accounts limit.** The maximum number of accounts that can use Zimbra Connector for Microsoft Outlook (ZCO).
- **Exchange Web Services (EWS) accounts limit.** The maximum number of accounts that can use EWS for connecting to an Exchange server. EWS is a separately licensed add-on feature.
- **High-Fidelity Document Preview:** The maximum number of accounts that can use the High-Fidelity document preview facility. LibreOffice must be installed.
- **Archiving Accounts limit.** The maximum number of archive accounts that can be created. The archive feature must be installed.

Zimbra License Requirements

A Zimbra license is required in order to create accounts in the Network Edition of Zimbra Collaboration.

Several types of licenses are available:

- **Trial.** You can obtain a free Trial license from the Zimbra website, at <https://www.zimbra.com>. The trial license allows you to create up to 50 users. It expires in 60 days.
- **Trial Extended.** You can obtain a Trial Extended license from Zimbra Sales by contacting sales@zimbra.com or calling 1-972-407-0688. This license allows you to create up to 50 users and is valid for an extended period of time.
- **Subscription.** You must purchase the Zimbra Subscription license. This license is valid for a specific Zimbra Collaboration system and is encrypted with the number of Zimbra accounts (seats) you have purchased, the effective date, and expiration date of the subscription license.
- **Perpetual.** You must purchase the Zimbra Perpetual license. This license is similar to a subscription license and is valid for a specific Zimbra Collaboration system, is encrypted with the number of Zimbra accounts (seats) you have purchased, the effective date, and an expiration date of 2099-12-31. When you renew your support agreement, no new perpetual license is sent to you, but your Account records in the systems is updated with your new support end date.

License Usage by Zimbra Collaboration Account Type

A mailbox license is required for an account assigned to a person, including accounts created for archiving. Distribution lists, aliases, locations and resources do not count against the license.

Below is a description of types of Zimbra Collaboration accounts and if they impact your license limit.

- **System accounts.** System accounts are specific accounts used by Zimbra Collaboration. They include the spam filter accounts for junk mail (spam and ham), virus quarantine account for email messages with viruses, and GALsync account if you configure GAL for your domain. **Do not delete these accounts!** These accounts do not count against your license.
- **Administrator account.** Administrator accounts count against your license.
- **User accounts.** User accounts count against your license account limit. When you delete an account, the license account limit reflects the change.
- **Alias account.** Aliases do not count against your license.
- **Distribution list.** Distribution lists do not count against your license.
- **Resource account.** Resource accounts (location and resources) do not count against your Zimbra Collaboration license.

License Activation

All Network Edition installations require license activation. New installations have a 10 day grace period from the license issue date before requiring activation. Your license can be activated from the administration console by selecting

Configure>Global Settings>License

then clicking **Activate License** in the toolbar. You can also activate your license from the command line interface.



Upgraded Zimbra Collaboration versions require an immediate activation of a valid license to maintain network feature functionality.

Automatic License Activation

Licenses are automatically activated if the Zimbra Collaboration server has a connection to the Internet and can communicate with the Zimbra License server. If you are unable to automatically activate your license, see the next section on [Manual License Activation](#)

Manual License Activation

For systems that do not have external access to the Zimbra License server, you can use the Zimbra Support Portal to manually activate your license. Go to the Zimbra website at <https://www.zimbra.com> and click on the **Support** page to display the Zimbra Technical Support page. Click on the **Support Portal Login** button to display the Zimbra Support Portal page. Enter your email and password to log in.

If you have problems accessing the Support Portal, contact Zimbra Sales at sales@zimbra.com or by

calling 1-972-407-0688.

License Not Installed or Activated

If you fail to install or activate your Zimbra Collaboration server license, the following scenarios describe how your Zimbra Collaboration server will be impacted.

- **License is not installed.** If a license is not installed, the Zimbra Collaboration server defaults to single user mode where all features limited by license are limited to one user.
- **License is not valid.** If the license file is forged or could not be validated for other reasons, the Zimbra Collaboration server defaults to single user mode.
- **License is not activated.** A license activation grace period is 10 days. If for some reason the license is never activated, the Zimbra Collaboration server defaults to single user mode.
- **License is in future.** If the license starting date is still in the future, the Zimbra Collaboration server defaults to single user mode.
- **License is in grace period.** If the license ending date has passed and is within the 30 day grace period, all features limited by license are still enabled, but administrators may see license renewal prompts.
- **License expired.** If the license ending date has passed and the 30 day grace period expired, the Zimbra Collaboration server defaults to the feature set of the Open Source Edition.

Obtaining a License

Go to Zimbra's Website <https://www.zimbra.com> to obtain a trial license from the Network Downloads area. Contact Zimbra sales regarding a trial extended license, or to purchase a subscription license or perpetual license, by emailing sales@zimbra.com or calling 1-972-407-0688.

The subscription and perpetual license can only be installed on the Zimbra Collaboration system for which it is purchased. Only one Zimbra license is required for your Zimbra Collaboration environment. This license sets the number of accounts that can be created.

Current license information, including the number of accounts purchased, the number of accounts used, and the expiration date, can be viewed from the administration console's **Configure>Global Settings>License** page.

Menu-Driven Configuration

The default configuration installs Zimbra-LDAP, Zimbra-MTA with anti-virus and anti-spam protection, the Zimbra mailbox server, SNMP monitoring tools (optional), Zimbra-spell (optional), the logger tool (optional), and the Zimbra proxy on one server.

The menu driven installation displays the components and their existing default values. You can modify the information during the installation process. The table below describes the menu options.

Main Menu options

Server Configured	Menu Item	Description
Main Menu		

Server Configured	Menu Item	Description

All

	zimbra-drive	Installing the Zimbra-Drive package is optional. If you choose to install Zimbra-Drive for file sync-and-share, it should be installed on every Zimbra Store Server that is part of the Zimbra configuration. Please bear in mind you will need a third party server running ownCloud or Nextcloud.
Server Configuration	Menu Item	Description
	Enable VMware HA	Toggle whether VMware HA is enabled or not - defaults to no VMware HA Clustering Heartbeat is only available when running within a virtual machine running vmware-tools. (Network Edition only)
	Default Class of Service Configuration	This menu section lists major new features for the Zimbra Collaboration release and whether the feature is enabled or not. When you change the feature setting during Zimbra Collaboration installation, you change the default COS settings Having this control, lets you decide when to introduce new features to your users.
	Enable default backup schedule	Toggle whether VMware HA is enabled or not - defaults to yes The Zimbra Archiving and Discovery package is an optional feature for Zimbra Network Edition. Archiving and Discovery offers the ability to store and search all messages that were delivered to or sent by Zimbra. This package includes the cross mailbox search function which can be used for both live and archive mailbox searches. (Network Edition only)
s) Save configuration to file	At any time during the installation, you can save the configuration to file.	c) Collapse menu
Allows you to collapse the menu.	x) Expand menu	Expand menus to see the underlying options


Common Configuration Options

The packages installed in common configuration include libraries, utilities, monitoring tools, and basic configuration files under Zimbra Core.

Server Configured	Menu Item	Description
Common Configuration - These are common settings for all servers		
All	Hostname	The host name configured in the operating system installation
	LDAP master host	The LDAP host name. On a single server installation, this name is the same as the hostname. On a multi server installation, this LDAP host name is configured on every server
	LDAP port	The default port is 389
	LDAP Admin password	This is the master LDAP password. This is the password for the Zimbra admin user and is configured on every server
All except Zimbra LDAP Server	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.
	Time Zone	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 in. The default time zone is PST (Pacific Time).
	IP Mode	IPv4 or IPv6 .
	Default SSL digest	Sets the default message digest to use when generating certificate. Defaults is sha256 .

Ldap configuration

Server Configured	Menu Item	Description
zimbra-ldap - These options are configured on the Zimbra LDAP server.		

Server Configured	Menu Item	Description
Zimbra LDAP Server	Status	The default is Enabled . For replica LDAP servers, the status can be changed to Disabled if the database is manually loaded after installation completes.
	Create Domain	The default is 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	By default, this password is automatically generated and is used for internal LDAP operations.
	LDAP Replication password	This is the password used by the LDAP replication user to identify itself to the LDAP master and must be the same as the password on the LDAP master server.
	LDAP Postfix password	This is the password used by the postfix user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the password on the LDAP master 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 Nginx password	<p>This password is automatically generated and is used by the nginx user to identify itself to the LDAP server and must be the same password on the LDAP master server and on the MTA server.</p> <div>  <p>This option is displayed only if the zimbra-proxy package is installed.</p> </div>
	LDAP Bes Searcher password	This password is automatically generated and is used by the ldap BES user.


Zimbra Logger

Ser ver Co nfi gur ed	Menu Item	Description
Zim bra mai lbo x ser ver	zimbra-logger	The Logger package is installed on 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 for generating statistics graphs and reporting and for message tracing.

MTA Server Configuration Options

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

Ser ver Co nfi gur ed	Menu Item	Description
zimbra-mta		

Server Configured	Menu Item	Description
Zimbra MTA Server	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	<p>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.</p> <div>  <p>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 remain queued in the Zimbra MTA server cannot be delivered.</p> </div>
	Bind password for Postfix LDAP user	Automatically set. This is the password used by the postfix user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the password on the LDAP master server.
	Bind password for Amavis LDAP user	Automatically set. This is the password used by the amavis user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the amavis password on the master LDAP server.



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 on that host, do:

```
zmlocalconfig -e zmtrainsa_cleanup_host=TRUE
```

DNS Cache

Server Configured	Menu Item	Description
zimbra-dnscache (optional)		
Zimbra mailbox server	Master DNS IP address(es)	IP addresses of DNS servers
	Enable DNS lookups over TCP	yes or no
	Enable DNS lookups over UDP	yes or no
	Only allow TCP to communicate with Master DNS	yes or no


Snmp configuration

Server Configured	Menu Item	Description
zimbra-snmp (optional)		
All	Enable SNMP notifications	The default is yes .
	SNMP Trap hostname	The hostname of the SNMP Trap destination
	Enable SMTP notification	The default is yes .
	SMTP Source email address	From address to use in email notifications
	SMTP Destination email address	To address to use in email notifications

Store configuration

zimbra-store		
Zim bra Mai lbo x Ser ver	Create Admin User	Yes or No . 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 Zimbra Collaboration 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 AmavisD 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	Yes or No . By default, the automated spam training filter is enabled and two mail accounts are created - one for the Spam Training User and one for the Non-spam (HAM) Training User . See the next 2 menu items which will be shown if spam training is enabled. These addresses are automatically configured to work with the spam training filter. The accounts created have randomly selected names. To recognize what the accounts are used for, you may want to change their names. The spam training filter is automatically added to the cron table and runs daily.
	Spam Training User	to receive mail notification about mail that was not marked as junk, but should have been.
	Non-spam (HAM) Training User	to receive mail notification about mail that was marked as junk, but should not have been.
The default port configurations are shown		

zimbra-store		
Zim bra Mai lbo x Ser ver	SMTP host	Defaults to current server name
	Web server HTTP port:	default 80
	Web server HTTPS port:	default 443
	Web server mode	<p>Can be HTTP, HTTPS, Mixed, Both or Redirect.</p> <ul style="list-style-type: none"> • 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 an HTTPS connection. • All modes use SSL encryption for back-end administrative traffic.
	IMAP server port	default 143
	IMAP server SSL port	default 993
	POP server port	default 110
	POP server SSL port	default 995
	Use spell checker server	default Yes (if installed)
	Spell server URL	<a href="http://<example.com>:7780/aspell.php">http://<example.com>:7780/aspell.php
<p>If either or both of these next 2 options are changed to TRUE, the proxy setting on the mailbox store are enabled in preparation for setting up zimbra-proxy.</p>		

zimbra-store		
Zim bra Mai lbo x Ser ver	*Configure for use with mail proxy.	default FALSE
	*Configure for use with web proxy.	default FALSE
	Enable version update checks.	Zimbra Collaboration automatically checks to see if a new Zimbra Collaboration update is available. The default is TRUE .
	Enable version update notifications .	<div> This enables automatic notification when updates are available when this is set to TRUE. <div>  The software update information can be viewed from the Administration Console Tools Overview pane. </div> </div>
	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.

Proxy configuration

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.

It requires the separate package **Zimbra Memcached** which is automatically selected when the **zimbra-proxy** package is installed. One server must run **zimbramemcached** when the proxy is in use. All installed zimbra proxies can use a single memcached server.

Ser ver Co nfi gur ed	Menu Item	Description
zimbra-proxy		

Server Configured	Menu Item	Description
Mailbox server, MTAServer or own independent server	Enable POP/IMAP Proxy	default TRUE
	IMAP proxy port	default 143
	IMAP SSL proxy port	default 993
	POP proxy port	default 110
	POP SSL proxy port	default 995
	Bind password for nginx ldap user	default set
	Enable HTTP[S] Proxy	default TRUE
	HTTP proxy port	default 80
	HTTPS proxy port	default 443
	Proxy server mode	default https

IMAPD configuration

IMAPD is an external IMAP[S] service that may be used as a replacement for the embedded IMAP[S] service that runs inside of **mailboxd**. It is recommended for use when the IMAP(S) traffic for a given installation is overloading the mailbox servers and is not recommended with a single-server installation.

Server Configured	Menu Item	Description
zimbra-imapd		

Server Configured	Menu Item	Description
mailbox server or independent server	Add to upstream IMAP Servers?	<p>default no. If yes, the following global config settings will be applied:</p> <ul style="list-style-type: none"> This server will be added to the list of <code>zimbraReverseProxyUpstreamImapServers</code> Embedded IMAP[S] servers will be disabled.

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, the necessary configuration can be done using the following commands:

```
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 Zimbra Collaboration 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 server's address from the **Nginx Lookup Extension**, and finally proxies the interactions between clients and upstream Zimbra Collaboration 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
- URLRewriting

For more information, see the wiki page https://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 Zimbra Collaboration 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.

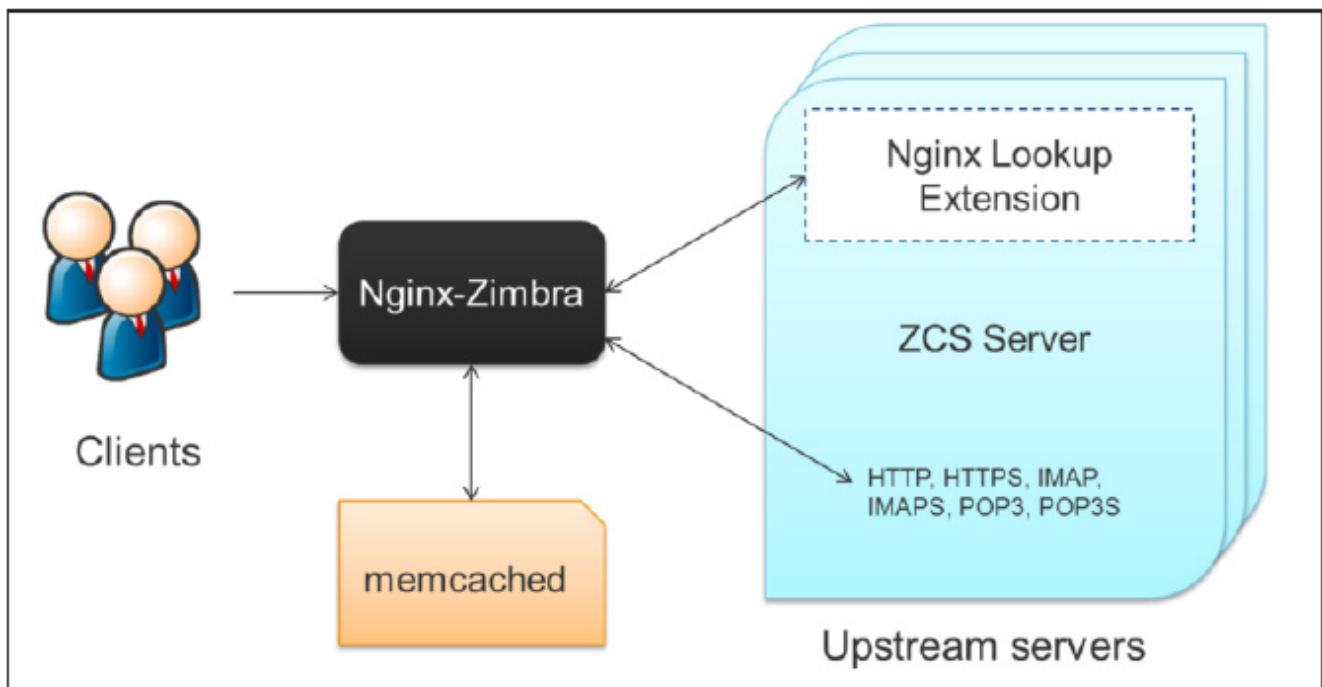
1. End clients connect to Zimbra Proxy using HTTP[S]/POP[S]/IMAP[S] ports.
2. Proxy attempts to contact a memcached server (elected from the available memcached servers, using a round-robin algorithm) if available and with caching enabled to query the upstream route information for this particular client.
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 Zimbra Collaboration Runtime

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



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.



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. The proxy also optionally connects to the IMAPD service on the Zimbra IMAPD ports if IMAPD is installed and configured at the global level or on a specific set of mailbox servers.

Zimbra Proxy Port Mapping

Zimbra Proxy Ports (External to Zimbra Collaboration)	
HTTP	80
HTTPS	443
POP3	110
POP3S (Secure POP3)	995
IMAP	143
IMAPS (Secure IMAP)	993

Zimbra Mailbox Ports (Internal to Zimbra Collaboration)	
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

Zimbra IMAPD Ports (Internal to Zimbra Collaboration)	
IMAP Backend (if Proxy configured)	8143
IMAPS Backend (if Proxy configured)	8993

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 having 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.

Preparing Your Server Environment

In order to successfully install and run Zimbra Collaboration, ensure your system meets the requirements described in this section. System administrators should be familiar with installing and managing email systems.



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 Zimbra Collaboration system requirements see [System Requirements for Zimbra Collaboration](#) at the end of this guide.

Modifying Operating System Configurations

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

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



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

Configuring High-Fidelity Document Preview (Network Edition Only)

The high-fidelity document preview feature requires the installation of LibreOffice or the LibreOffice-headless package, depending on the operating system you are running.

If LibreOffice is installed, the system is automatically configured to use high-fidelity document preview. If LibreOffice is not installed, the preview engine from prior Zimbra Collaboration releases is used.

This can be accomplished with the appropriate Linux distribution's package management systems:

- For RHEL, install the libreoffice-headless package:

```
yum install libreoffice
yum install libreoffice-headless
```

- For Ubuntu, install libreoffice:

```
apt-get install libreoffice
```

Install Language and Font Packages

Confirm you have the appropriate language packs or fonts installed for LibreOffice to properly view documents and attachments. For example:

- If using Ubuntu 12.04 (**deprecated**) and viewing East Asian languages, be sure to install:

```
apt-get install libreoffice-l10n-*  
apt-get install ttf-vlgothic
```

- If using Ubuntu 14.04 or 16.04 and viewing East Asian languages, be sure to install:

```
apt-get install libreoffice-l10n-*  
apt-get install fonts-vlgothic
```

- If using RHEL, be sure to install:

```
yum install libreoffice-langpack-xx
```

DNS Configuration Requirement

When you create a domain during the installation process, Zimbra Collaboration checks to see if you have an MX record correctly configured for that domain. 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.

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

You must configure a relay host if you do not enable DNS. After Zimbra Collaboration is installed, go to the **administration console's Global Settings>MTA** tab and:

- Uncheck **Enable DNS lookups**.
- Enter the **relay MTA address** to use for external delivery.



Even if a relay host is configured, an MX record is still required if the Zimbra Collaboration server is going to receive email from the Internet.

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.

Order of Installation

1. ZCS LDAP server(s)
2. ZCS MTA server(s)
3. ZCS Proxy server(s)
4. ZCS Mailbox server(s) options:
 - Zimbra Mailbox Server, which includes the mailstore services and webapp services (mailstore server + UI server)
 - Zimbra Web Application Server Split mode, which includes:
 - a Zimbra mailstore server (mailstore server)
 - a Zimbra webapp server (UI server)
5. ZCS IMAPD server(s)
 - Optional standalone IMAP server



Zimbra-proxy is normally installed on the MTA server or you can install it on its own server.



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



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

Starting the Installation Process

Before you begin, make sure to:



- Store your license in a directory folder on your server as it is needed to complete your installation of Zimbra Collaboration. For more information about licenses, see [Zimbra Collaboration License](#) and [Zimbra License Requirements](#) (Network Edition only)
- Confirm you have the latest system requirements and prerequisites for installing Zimbra Collaboration, as described in [System Requirements for Zimbra Collaboration](#)

For the latest Zimbra Collaboration software downloads, go to <https://www.zimbra.com>.

Save the Zimbra Collaboration **tar** file to the computer from which you are installing the software.



The screen shots are examples of the Zimbra Collaboration installation script. The actual script may be different.

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

Open an SSH session to the Zimbra server and follow the steps below:

1. Log in as **root** to the Zimbra Collaboration 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.



*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-8.8.5_GA_1894.UBUNTU16_64.20171026035615/
zcs-NETWORK-8.8.5_GA_1894.UBUNTU16_64.20171026035615/packages/
.
.
.
zcs-NETWORK-8.8.5_GA_1894.UBUNTU16_64.20171026035615/install.sh
zcs-NETWORK-8.8.5_GA_1894.UBUNTU16_64.20171026035615/README.txt

root@zimbraiop:/tmp/# cd zcs-NETWORK-8.8.5_GA_1894.UBUNTU16_64.20171026035615/
root@zimbraiop:/tmp/zcs-NETWORK-8.8.5_GA_1894.UBUNTU16_64.20171026035615#
./install.sh

Operations logged to /tmp/install.log.y1YeCSI5
.
.
.
```

2. The **install.sh** script reviews the installation software to verify that the Zimbra packages are available.

The installation process checks to see whether any of the applications **Sendmail**, **Postfix**, **MySQL** or **MariaDB** are running.

If any of these applications are running, you are asked to disable them.

Disabling **MySQL** and **MariaDB** is **optional** but highly recommended.

Sendmail and **Postfix** **MUST** be disabled for Zimbra Collaboration to start correctly.

```
root@zimbraiop:/tmp/zcs-NETWORK-8.8.5_GA_1894.UBUNTU16_64.20171026035615#  
./install.sh
```

```
Operations logged to /tmp/install.log.y1YeCSI5
```

```
Checking for existing installation...
```

```
zimbra-chat...NOT FOUND  
zimbra-drive...NOT FOUND  
zimbra-imapd...NOT FOUND  
zimbra-network-modules-ng...NOT FOUND  
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-convertd...NOT FOUND  
zimbra-memcached...NOT FOUND  
zimbra-proxy...NOT FOUND  
zimbra-archiving...NOT FOUND  
zimbra-core...NOT FOUND
```

```
.  
.  
.
```

3. The Zimbra software agreement displays. Read the agreement and when

Do you agree with the terms of the software license agreement? [N]

displays, enter **Y** to continue.



The license agreement displays in multiple sections, and you must accept each section of the license agreement.

4. Use Zimbra's package repository [Y]

displays, press **enter** to continue. Your system will be configured to add the Zimbra packaging repository for **yum** or **apt-get** as appropriate so it can install the Zimbra 3rd party packages.

Checking for installable packages

```
Found zimbra-core (local)
Found zimbra-ldap (local)
Found zimbra-logger (local)
Found zimbra-mta (local)
Found zimbra-dnscache (local)
Found zimbra-snmp (local)
Found zimbra-store (local)
Found zimbra-apache (local)
Found zimbra-spell (local)
Found zimbra-convertd (local)
Found zimbra-memcached (repo)
Found zimbra-proxy (local)
Found zimbra-archiving (local)
Found zimbra-chat (repo)
Found zimbra-drive (repo)
Found zimbra-imapd (local)
Found zimbra-network-modules-ng (local)
```

```
Use Zimbra's package repository [Y] y
Configuring package repository
```

5. Next, select the packages to be installed on this server.



For the cross mailbox search feature, install the Zimbra Archive package. To use the archiving and discovery feature, contact Zimbra sales.

The installer verifies that there is enough room to install Zimbra.

6. 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](#)



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 ZCS LDAP Master server before you can install other ZCS 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 Zimbra Collaboration servers. See the section on [Configuring LDAP Replication](#)

1. Follow steps 1 through 4 in [Starting the Installation Process](#) to open an SSH session to the LDAP server, log on to the server as **root**, and unpack the ZCS software.

2. Type **y** and press *Enter* to install the **zimbra-ldap** package.
The **zimbra-mta**, **zimbra-store** and **zimbra-logger** packages should be marked **n**.

```
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
Install zimbra-convertd [Y] N
Install zimbra-memcached [Y] N
Install zimbra-proxy [Y] N
Install zimbra-archiving [N] N
Install zimbra-chat [Y] N
Install zimbra-drive [Y] N
Install zimbra-imapd [Y] N
Install zimbra-network-modules-ng [Y] N
Checking required space for zimbra-core
Installing:
  zimbra-core
  zimbra-ldap
The system will be modified. Continue? [N]
```

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 the section [Main Menu options](#) 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** submenu.

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) Store ephemeral attributes outside Ldap: no
- 6) Secure interprocess communications: yes
- 7) TimeZone: America/Mexico_City
- 8) IP Mode: ipv4
- 9) Default SSL digest: sha256

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

5. Type **4** to display the automatically generated LDAP admin password.

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

Password for ldap admin user (min 6 characters): [bEyMZxNxq]

You can change this password.

Write down the LDAP password, the LDAP host name and the LDAP port.

LDAP Admin Password _____
LDAP Host name _____
LDAP Port _____



You must configure this information when you install the mailbox servers and the MTA servers.

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

```
1 Africa/Algiers
.
.
.
94 Europe/London
.
.
.
109 Pacific/Tongatapu
110 UTC
Enter the number for the local timezone: [110] 94
```

7. Type **r** to return to the Main menu.
8. From the Main menu, type **2** for **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]
```

9. Type **3** for **Domain to create** to change the default domain name to the main domain name you want to use for your network, (e.g. **example.com**).
10. The passwords listed in the **LDAP configuration** menu are automatically generated.

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      _____
```



You need these passwords when configuring the MTA and the LDAP replica servers. Write them down.

11. When changes to the LDAP configuration menu are complete:

```
*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes]
Save config in file: [/opt/zimbra/config.8381]
Saving config in /opt/zimbra/config.8381...done
```

- enter **r** to return to the main menu.
- Type **a** to apply the configuration changes.
- When **Save configuration data to file** appears, type **Yes** and press *Enter*.
- 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? [No]** 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]
Save config in file: [/opt/zimbra/config.8381]
Saving config in /opt/zimbra/config.8381...done.
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.20170302-133132.log
Setting local config values...done.
.
.
.
Starting servers...done.
Skipping creation of default domain GAL sync account - not a service node.
Setting up zimbra crontab...done.

Moving /tmp/zmsetup.20170302-133132.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.



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

The Zimbra license file can be installed on one of the mailbox servers during the installation. If you do not have a license file, you can install it from the administration console when the Zimbra

Collaboration install is complete. See [Zimbra License Requirements](#)

Install Zimbra Mailbox Services

1. Follow steps 1 through 4 in [Starting the Installation Process](#) to open an SSH session to the Mailbox server, log on to the server as **root**, and unpack the ZCS software.
2. Type **y** and press *Enter* to install the **zimbra-logger** package (optional and only on one mail server) and **zimbra-store**. In the following screen shot example, the packages to be installed are emphasized.



*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
Install zimbra-convertd [Y] Y
Install zimbra-memcached [Y] N
Install zimbra-proxy [Y] N
Install zimbra-archiving [N] Y
Install zimbra-chat [Y] Y
Install zimbra-drive [Y] Y
Install zimbra-imapd [Y] N
Install zimbra-network-modules-ng [Y] y
```

###WARNING###

Network Modules NG needs to bind on TCP ports 8735 and 8736 in order to operate, for inter-instance communication.

Please verify no other service listens on these ports and that ports 8735 and 8736 are properly filtered from public access by your firewall.

Please remember that the Backup NG module needs to be initialized in order to be functional. This is a one-time operation only that can be performed by clicking the 'Initialize' button within the Backup section of the Network NG Modules in the Administration Console or by running ``zxsuite backup doSmartScan`` as the zimbra user.

```
Checking required space for zimbra-core
Checking space for zimbra-store
Checking required packages for zimbra-store
    FOUND: libreoffice-1:4.2.8-0ubuntu4
zimbra-store package check complete.
```

Installing:

```
zimbra-core
zimbra-logger
zimbra-snmp
zimbra-store
zimbra-apache
zimbra-spell
zimbra-convertd
zimbra-archiving
zimbra-chat
zimbra-drive
zimbra-network-modules-ng
```

The system will be modified. Continue? [N]

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 the section [Main Menu options](#) for a description of the Main menu.

Main menu

```
1) Common Configuration:
    +Hostname:                               mailstore-1.example.com
***** +Ldap master host:                   UNSET
    +Ldap port:                             389
***** +Ldap Admin password:                UNSET
    +LDAP Base DN:                          cn=zimbra
```



```

+Store ephemeral attributes outside Ldap: no
+Secure interprocess communications:    yes
+TimeZone:                             UTC
+IP Mode:                              ipv4
+Default SSL digest:                   sha256

2) zimbra-logger:                      Enabled
3) zimbra-snmp:                        Enabled
4) 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.mgpgruxx@mailstore-
1.example.com
    +Enable automated spam training:     yes
    +Spam training user:                 spam.qgku2xsq@mailstore-
1.example.com
    +Non-spam(Ham) training user:        ham.y49bbzuis@mailstore-
1.example.com
***** +SMTP host:                      UNSET
    +Web server HTTP port:               8080
    +Web server HTTPS port:              8443
    +Web server mode:                    https
    +IMAP server port:                   7143
    +IMAP server SSL port:                7993
    +POP server port:                    7110
    +POP server SSL port:                 7995
    +Use spell check server:              yes
    +Spell server URL:                   http://mailstore-
1.example.com:7780/aspell.php
    +Enable version update checks:        TRUE
    +Enable version update notifications: TRUE
    +Version update notification email:   admin@mailstore-1.example.com
    +Version update source email:         admin@mailstore-1.example.com
    +Install mailstore (service webapp):  yes
    +Install UI (zimbra,zimbraAdmin webapps): yes
***** +License filename:                UNSET

5) zimbra-spell:                        Enabled
6) zimbra-convertd:                     Enabled
7) Default Class of Service Configuration:
8) Enable default backup schedule:       yes
s) Save config to file
x) Expand menu
q) Quit

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

```

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

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) Store ephemeral attributes outside Ldap:	no
7) Secure interprocess communications:	yes
8) TimeZone:	UTC
9) IP Mode:	ipv4
10) 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.

5. Type **8** to set the correct time zone.

```
1 Africa/Algiers
.
.
.
94 Europe/London
.
.
.
109 Pacific/Tongatapu
110 UTC
Enter the number for the local timezone: [110] 94
```

6. Type **r** to return to the Main menu.
7. From the Main menu, type **4** for **zimbra-store** to view the **Store configuration** settings.

Store configuration

```
1) Status: Enabled
2) Create Admin User: yes
3) Admin user to create: admin@mailstore-1.example.com
** 4) Admin Password UNSET
5) Anti-virus quarantine user: virus-
quarantine.orulkdewtz@mailstore-1.example.com
6) Enable automated spam training: yes
7) Spam training user: spam.udbnonsavi@mailstore-
1.example.com
8) Non-spam(Ham) training user: ham.3ptgqja0f@mailstore-
1.example.com
** 9) SMTP host: UNSET
10) Web server HTTP port: 8080
11) Web server HTTPS port: 8443
12) HTTP proxy port: 80
13) HTTPS proxy port: 443
14) Web server mode: https
15) IMAP server port: 7143
16) IMAP server SSL port: 7993
17) IMAP proxy port: 143
18) IMAP SSL proxy port: 993
19) POP server port: 7110
20) POP server SSL port: 7995
21) POP proxy port: 110
22) POP SSL proxy port: 995
23) Use spell check server: yes
24) Spell server URL: http://mailstore-
1.example.com:7780/aspell.php
25) Configure for use with mail proxy: TRUE
26) Configure for use with web proxy: TRUE
27) Enable version update checks: TRUE
28) Enable version update notifications: TRUE
29) Version update notification email: admin@mailstore-1.example.com
30) Version update source email: admin@mailstore-1.example.com
31) Install mailstore (service webapp): yes
32) Install UI (zimbra,zimbraAdmin webapps): yes
**33) License filename: UNSET

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

8. 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.



*By default, the domain name portions of the email addresses for the Admin user, Anti-virus quarantine user, Spam training user and Non-spam(Ham) training user, are set to be the zimbra mailstore server address. You may want to change these to be the Zimbra Collaboration primary domain address instead. (**example.com** in this example)*

9. Type the corresponding number to set the **SMTP host**. This is the mta-server host name.
10. 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 an HTTPS connection.

All modes use SSL encryption for back-end administrative traffic.

11. If you are configuring proxy servers, type the corresponding number to enable the servers. When you enable these, the mail server port and proxy port numbers are automatically changed. See [Configuration during installation](#).
12. If you install the **Zimbra-spell** package, it should be installed on every mailstore. The hostname portion of the http address for each should be the hostname of the mailstore server it is installed on.
13. **Enable version update checks** and **Enable version update notifications** are set to TRUE. Zimbra Collaboration automatically checks for the latest Zimbra Collaboration software updates and notifies the account that is configured in Version update notification email. You can modify this later from the administration console.
14. 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.

15. **(Network Edition only)**. Type the corresponding menu number to install the Zimbra license file.
Enter the location of the Zimbra 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.
16. 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)** value to **no**, which will exclude mailstore services.
- To install both the mailstore and UI services on the same server, confirm the values for **Install mailstore (service webapp)** and **Install UI (zimbra,zimbraAdmin webapps)** are both set to **yes**. The default is **yes**.



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

17. Type **r** to return to the Main menu.
18. Review the Default Class of Service Configuration settings. If you want to change the COS default configuration of these features, type the number 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.
19. 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.
20. When Save Configuration data to file appears, type **Yes** and press *Enter*.

```
Save configuration data to a file? [Yes]
```

21. 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*.

```
Save config in file: [/opt/zimbra/config.16039]
Saving config in /opt/zimbra/config.16039...done.
```

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

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

```
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.20160711-234517.log
Setting local config values...done.
.
.
.
Configuration complete - press return to exit
```

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

The installation of the mailbox server is complete.

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](#) to open an SSH session to the MTA server, log on to the server as **root**, and unpack the ZCS 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 packages to be installed are emphasized.



*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] 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
```

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

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

```
Checking required space for zimbra-core
```

```
Installing:
```

```
  zimbra-core
```

```
  zimbra-mta
```

```
  zimbra-dnscache
```

```
The system will be modified. Continue? [N] y
```

```
Installing packages
```

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 the section [Main Menu options](#) for a description of the Main menu.

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
   +Store ephemeral attributes outside Ldap: no
   +Secure interprocess communications:     yes
   +TimeZone:                              Africa/Monrovia
   +IP Mode:                               ipv4
   +Default SSL digest:                     sha256

2) zimbra-mta:                             Enabled
   +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
s) Save config to file
x) Expand menu
q) Quit

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

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

Common configuration

1) Hostname:	mta-1.example.com
** 2) Ldap master host:	UNSET
3) Ldap port:	389
** 4) Ldap Admin password:	UNSET
5) LDAP Base DN:	cn=zimbra
6) Store ephemeral attributes outside Ldap:	no
7) Secure interprocess communications:	yes
8) TimeZone:	Africa/Monrovia
9) IP Mode:	ipv4
10) Default SSL digest:	sha256

The mta 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.

5. Type **8** to set the correct time zone.

```
1 Africa/Algiers
.
.
.
94 Europe/London
.
.
.
109 Pacific/Tongatapu
110 UTC
Enter the number for the local timezone: [110] 94
```

6. Type **r** to return to the **Main** menu.
7. Type **2** to go to the **Mta configuration** menu.

Mta configuration

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

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

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



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

9. Select the menu number for **Bind password for postfix ldap user**.
You must use the same value for this as is configured on the LDAP master server.
10. Select the menu number for **Bind password for amavis ldap user**.
You must use the same value for this as is configured on the LDAP master server.
11. Type **r** to return to the **Main** menu.



If you are installing the Zimbra-proxy package, see [Installing Zimbra Proxy](#) before continuing.

12. 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.
13. When **Save configuration data to file** appears,
type **Yes** and press *Enter*.
14. The next request asks where to save the file. To accept the default, press *Enter*. To save the files to another directory, enter the directory and then press *Enter*.
15. When **The system will be modified - continue?** appears,
type **Yes** 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.

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

The installation of the MTA server is complete.

Installing Zimbra Proxy

Installing the `zimbra-proxy` package is optional, but recommended for scalable multi-server deployment. Zimbra proxy is normally installed on the MTA server or can be configured on a separate server. Zimbra proxy can be installed on more than one server. At least one instance of `zimbra-memcached` must be installed to cache the route information (upstream mailbox server for each endclient).



If you are moving from a non-proxy environment (for example, single server to multi-server environment), additional steps are necessary for the mailbox server and proxy configuration. After you complete the proxy installation, reconfigure the mailbox server as described in the Zimbra Collaboration Administration Guide, *Zimbra Proxy* chapter.



Memcached is shipped as the caching layer to cache LDAP lookups. Memcache does not have authentication and security features so the servers should have a firewall set up appropriately. The default port is `11211` and is controlled by the `zimbraMemcacheBindPort` conf setting.

Installing on the MTA Server

If you are installing `zimbra-proxy` on the MTA server, select the `zimbra-proxy` package and the `zimbra-memcached` package. Follow the installation process for [Installing Zimbra MTA on a Server](#). After Step 11, configure the Zimbra-proxy.

1. On the MTA server, select to install the `zimbra-proxy` and `zimbra-memcached` packages, type `y` and press **Enter** to install the selected package.
2. The *Main* menu displays the default entries for the Zimbra component you are installing. Select **Proxy Configuration** menu. You can modify any of the values.

The **Bind password for Nginx ldap user** was configured when the LDAP server was installed. This is set when the MTA connected to the LDAP server. This is not used unless the Kerberos5 authenticating mechanism is enabled.



Setting the password even though GSSAPI auth/proxy is not set up does not cause any issues.

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

Return to [Installing Zimbra MTA on a Server](#), step 12, to continue the MTA server installation.

Installing 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](#) 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.



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

Select the packages to install

```
Install zimbra-ldap [Y] N
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 [N] Y
Install zimbra-proxy [N] Y
Install zimbra-archiving [N] N
Installing:
    zimbra-memcached
    zimbra-proxy
```

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

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**.

Main menu

1) Common Configuration:

+Hostname: localhost
+Ldap master host: ldap-1.example.com
+Ldap port: 389
+Ldap Admin password: set
+LDAP Base DN: cn=zimbra
+Store ephemeral attributes outside Ldap: no
+Secure interprocess communications: yes
+TimeZone: (GMT-08.00) Pacific Time (US &

Canada)

+IP Mode: ipv4
+Default SSL digest: sha256

2) zimbra-proxy: Enabled

+Enable POP/IMAP Proxy: TRUE
+IMAP server port: 7143
+IMAP server SSL port: 7993
+IMAP proxy port: 143
+IMAP SSL proxy port: 993
+POP server port: 7110
+POP server SSL port: 7995
+POP proxy port: 110
+POP SSL proxy port: 995

***** +Bind password for nginx ldap user: Not Verified
+Enable HTTP[S] Proxy: TRUE
+Web server HTTP port: 8080
+Web server HTTPS port: 8443
+HTTP proxy port: 80
+HTTPS proxy port: 443
+Proxy server mode: https

3) Enable default backup schedule: yes

s) Save config to file

x) Expand menu

q) Quit

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

7. The **Proxy Configuration** menu displays. You can modify any of the values.

The **Bind password for Nginx ldap user** is configured when the LDAP server was installed. This is set when the MTA connected to the LDAP server. This is not used unless the Kerberos5 authenticating mechanism is enabled.



Setting the password even though GSSAPI auth/proxy is not set up does not cause any issues.

Proxy configuration

1) Status:	Enabled
2) Enable POP/IMAP Proxy:	TRUE
3) IMAP server port:	7143
4) IMAP server SSL port:	7993
5) IMAP proxy port:	143
6) IMAP SSL proxy port:	993
7) POP server port:	7110
8) POP server SSL port:	7995
9) POP proxy port:	110
10) POP SSL proxy port:	995
11) Bind password for nginx ldap user:	set
12) Enable HTTP[S] Proxy:	TRUE
13) Web server HTTP port:	8080
14) Web server HTTPS port:	8443
15) HTTP proxy port:	80
16) HTTPS proxy port:	443
17) Proxy server mode:	https

8. Type **r** to return to the *Main* menu.
9. When the proxy server is configured, return to the *Main* menu and type **a** to apply the configuration changes. Press *Enter* to save the configuration data.
10. When **Save Configuration data to a file** appears, 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 then press *Enter*.
12. When **The system will be modified - continue?** appears, type **y** and press *Enter*.
13. When **Installation complete - press return to exit** displays, press *Enter*.

The installation of the proxy server is complete.

Installing Zimbra IMAPD

Installing the new **zimbra-imapd** package is optional, and is available as an unsupported beta if you want to test this beta product targeted for scalable multi-server deployment. Zimbra imapd is normally installed on the mailbox server or can be configured on a separate server. Zimbra imapd can be installed on more than one server.

Installing on the Mailbox Server

If you are installing **zimbra-imapd** on the mailbox server, select the **zimbra-imapd** package. Follow the installation process for [Install Zimbra Mailbox Services](#). After Step 11, configure the Zimbra-imapd.

1. On the mailbox server, select to install the **zimbra-imapd** packages, type **y** and press **Enter** to install the selected package.
2. The *Main* menu displays the default entries for the Zimbra component you are installing. Select

IMAPD Configuration menu. You can modify any of the values.

IMAPD configuration

1) Status:	Enabled
2) Add to upstream IMAP Servers?:	no

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

1. Type **1** to disable the IMAPD process on this machine.
2. Type **2** to add the server to the upstream IMAP Servers list.



If you are installing new IMAPD nodes into a running cluster be sure and upgrade all of the mailbox nodes to the same version of Zimbra prior to installing the IMAPD nodes.

Return to [Install Zimbra Mailbox Services](#), step 12, to continue the server installation.

Installing on a separate server

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

1. Follow steps 1 through 4 in [Starting the Installation Process](#) 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-imapd** package as shown in the following screen shot example. The other packages should be marked **N**.



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

Select the packages to install

```
Install zimbra-ldap [Y] N
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 [N] N
Install zimbra-proxy [N] N
Install zimbra-archiving [N] N
Install zimbra-imapd [N] Y
Checking required space for zimbra-core
```

Installing:

```
zimbra-core
zimbra-imapd
```

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

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-imapd**.

Main menu

1) Common Configuration:

```
+Hostname:                localhost
+Ldap master host:        ldap-1.example.com
+Ldap port:               389
+Ldap Admin password:     set
+LDAP Base DN:            cn=zimbra
+Store ephemeral attributes outside Ldap: no
+Secure interprocess communications: yes
+TimeZone:                (GMT-08.00) Pacific Time (US &
```

Canada)

```
+IP Mode:                 ipv4
+Default SSL digest:      sha256
```

2) zimbra-imapd: Enabled

s) Save config to file

x) Expand menu

q) Quit

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

7. The **IMAPD Configuration** menu displays. You can modify any of the values.

By default the IMAPD service is enabled when it is selected for installation.



No IMAP sessions will be routed to the IMAPD server unless it is added to the multi-valued `zimbraReverseProxyUpstreamImapServers` LDAP attribute. This can be done using the `zmprov` command at any time after the server is installed and does not have to be done during installation. After adding the new IMAPD node to `zimbraReverseProxyUpstreamImapServers`, the globalconfig LDAP cache must be flushed on all servers acting as lookup targets in order for them to pick up the change. This can be done with the command `zmprov flushCache -a config`. To verify that this has taken effect, make sure that the new IMAPD node is listed in the output of `zmprov gacf zimbraReverseProxyUpstreamImapServers`, when run from a lookup target server.



If you are installing new IMAPD nodes into a running cluster be sure and upgrade all of the mailbox nodes to the same version of Zimbra prior to enabling routing to the IMAPD nodes.

IMAPD configuration

```
1) Status:                Enabled
2) Add to upstream IMAP Servers?: no
```

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

9. When the `imapd` server is configured, return to the *Main* menu and type `a` to apply the configuration changes. Press *Enter* to save the configuration data.
10. When **Save Configuration data to a file** appears, 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 then press *Enter*.
12. When **The system will be modified - continue?** appears, type `y` and press *Enter*.
13. When **Installation complete - press return to exit** displays, press *Enter*.

The installation of the `imapd` server is complete.

Installing zimbra-archiving Package

Installing the `zimbra-archiving` package is optional. This package enables Zimbra Collaboration Archiving and Discovery, which offers:

- Archiving, the ability to archive messages that were delivered to or sent by ZCS.
- Discovery, the ability to search across mailboxes.

The prerequisite to enabling archiving and discovery is the installation and configuration of the `zimbra-archiving` package on at least one mailbox server. The installation of this package provides the ZCS discovery (also known as cross mailbox) search tool and sets the attributes that allow archiving to be enabled on the Zimbra MTAs.

To enable archiving and discovery, select the `zimbra-store` and `zimbra-archiving` packages during your installation process. The `zimbra-core` package is installed by default.

```
Select the packages to install
Install zimbra-ldap [Y] N
Install zimbra-logger [Y] N
Install zimbra-mta [Y] N
Install zimbra-dnscache [N] N
Install zimbra-snmp [Y] N
Install zimbra-store [Y] Y
Install zimbra-apache [Y] N
Install zimbra-spell [Y] N
Install zimbra-convertd [N] N
Install zimbra-memcached [N] N
Install zimbra-proxy [N] N
Install zimbra-archiving [N] Y
Install zimbra-chat [Y] N
Install zimbra-drive [Y] N
Install zimbra-imapd [Y] N
```

Installing:

```
zimbra-core
zimbra-store
zimbra-archiving
```

This system will be modified. Continue [N] Y

See the *Zimbra Archiving and Discovery* chapter in the Zimbra Collaboration Administration Guide for more information about configuring and archiving.

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 question is 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 [Mail queue monitoring](#).

Set Up the SSH Keys

To populate the SSH keys, perform the following as the **zimbra** user (`sudo su - zimbra`) on each server:

```
zmupdateauthkeys
```

The key is updated in `/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.



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/syslogd stop`.
- c. Start the syslog daemon. Type `/etc/init.d/syslogd 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
```

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 `zmtrainasa --cleanup`. To do this, set `zmlocalconfig -e zmtrainasa_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. Perform the following on each server in your Zimbra Collaboration environment.

1. Log on as `root`.
2. Type `su - zimbra`.

3. Type `zmcontrol status`. The services status information is displayed. All services should be running.



If services are not started, you can type `zmcontrol start`. See the CLI command appendix in the Zimbra Collaboration 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>`. The 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. The default value of `zimbraAdminProxyPort` is `9071`.



- The administration console address must be typed with `https`, even if you configured only `http`.
- The first time you log on, a certificate authority (CA) alert may be displayed. Click **Accept this certificate permanently** to accept the certificate and be able connect to the Zimbra administration console. Then click **OK**.

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 Zimbra Collaboration is installed, if you installed the Zimbra license, you can log on to the administration console and configure additional domains, create Classes of Service, and provision accounts. See the Zimbra Collaboration Administration 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 section.

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**.



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 Zimbra Collaboration 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

Ephemeral Data Migration

Versions of Zimbra prior to 8.8.9 stored *ephemeral data* in *LDAP*. Examples of *ephemeral data* include:

- `zimbraAuthTokens`
- `zimbraCsrfTokenData`
- `zimbraLastLogonTimestamp`

Zimbra Collaboration version 8.8.9 introduced the ability to store *ephemeral data* in an external service such as [SSDB](#). This is an optional feature; however, it can improve *LDAP* performance and stability.

Please refer to the *Zimbra Collaboration Administration Guide* for more information. Migration of *ephemeral data* out of *LDAP* and into *SSDB* must be performed after an install or upgrade has been completed.

Installing Zimbra X Webclient

Optionally you can install Zimbra X Webclient, which is currently in beta stage and you can provide early feedback to Zimbra. Below are the steps to setup Zimbra X Webclient on Zimbra

1. Run Zimbra X Webclient on any of the mailbox servers
 - Make sure latest version of **NodeJS** and **NPM** is installed
 - In case of multinode environment make sure you are selecting a node which is currently working as a mailbox node
 - Clone repository of Zimbra X Webclient by executing `git clone https://github.com/Zimbra/zm-x-web.git`
 - If you want to do any customizations on top of Zimbra X Webclient then you can do as shown here [Customising-Zimbra-X-Webclient](#)
 - Install npm modules by executing `npm install`
 - Create a production build by executing `npm run build`. If customisations were made in a client directory other than `default`, e.g. in the `client/foo` directory, then specify the client directory name as an environment variable on the command line like `CLIENT=foo npm run build`
 - `PORT=9090 npm run serve` (We are specifying port 9090 to make sure it doesn't conflict with other used ports in Zimbra)
2. Configure nginx to route requests properly on proxy server
 - add below line in `/opt/zimbra/conf/nginx/templates/nginx.conf.web.template` file at the end of file where other files are getting included

```
${web.https.enabled}include  
${core.includes}/${core.cprefix}.web.zimbrax.default;
```


- add below block as an extra upstream block, this should contain hostname of mailbox node which contains zm-x-web, make sure to give correct port which was used when executing `npm run serve` command above

```
upstream zimbra_x_webclient
{
    server    <hostname_of_mailbox_which_hosts_zimbra_x_webclient>:9090
    fail_timeout=10s version=8.8.8_6A_1231;
    zmath;
}
```

- Navigate to the `/opt/zimbra/conf/nginx/includes/` directory
- Copy `nginx.conf.web.admin.default` to same directory and name it as `nginx.conf.web.zimbrax.default`
- Remove all location blocks from `nginx.conf.web.zimbrax.default` file, and add location blocks shown in [\[location_blocks\]](#)

3. There are two ways from which Zimbra X Webclient can be configured for access

- Use PORT number to access Zimbra X Webclient
 - make sure selected port is not conflicting with proxy's open ports as described in [Proxy Ports Wiki](#)), to be on safer side it is recommended to use `9090` port
 - Update port number in listen block on second line of server block to `9090` (or any selected port)
 - Restart proxy by `zmpoxyctl restart`
 - Check if Zimbra X Webclient is working on https://<hostname_of_proxy>:9090/
- Use subdomain to access Zimbra X Webclient
 - Update port number in listen block on second line of server block to `443`, this will make sure subdomain is listening on default ssl port
 - add `server_name` directive under listen directive and specify subdomain which we need to use to listen to requests `server_name <subdomain>.<hostname_of_proxy>`
 - Restart proxy by `zmpoxyctl restart`
 - Check if Zimbra X Webclient is working on https://<subdomain>.<hostname_of_proxy>/



Do not access Zimbra X Webclient using mailbox node url, as it will not work. Users should access it using proxy url only.

```
location /
{
    # Rewrite url for favicon icon
    rewrite ^/favicon.ico$ /assets/favicon.ico break;

    # Proxy to Zimbra X Webclient Upstream
    proxy_pass      https://zimbra_x_webclient;
```

```

# Cache only specific files listed below
expires off;

# Cache assets for 10 mins
location /assets/**
{
    expires 10m;
}

# Cache chunks for max time as chunk number changes on every new build
location /**/*.chunk.*
{
    expires max;
}

# For audit
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

set $relhost $host;
if ($host = '') {
    set $relhost $server_addr;
}
proxy_set_header Host          $relhost:9090;
}

location ^~ /@zimbra
{
    # Rewrite url to remove @zimbra token
    rewrite ^/@zimbra/(.*)$ /$1 break;

    # Proxy to Zimbra Upstream
    proxy_pass          https://zimbra_ssl;

    # Don't cache data requests
    expires off;

    # For audit
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

    # Remove referer header, as csrf check fails with different referer
    proxy_set_header Referer "";

    set $relhost $host;
    if ($host = '') {
        set $relhost $server_addr;
    }
    proxy_set_header Host          $relhost;
}

```

Uninstalling Zimbra Collaboration

To uninstall servers, run the install script with the `-u` option. Then delete the `/opt/zimbra` 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 deleted. See [Uninstall Zimbra on Linux](#).

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.
- 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 [Installing Zimbra Proxy](#).

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 are the same as 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
```

If you are installing the Zimbra proxy or *MTA* on the new node, you will also need to record the following:



- Bind password for postfix ldap user
- Bind password for amavis ldap user
- Bind password for nginx ldap user

```
zmlocalconfig -s | grep -E '(amavis|nginx|postfix)_password'
```



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

1. Follow steps 1 through 4 in [Starting the Installation Process](#) 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.



If SNMP is being used, type **Y** for **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 **2** to set **Create Admin User** to **No**.
 - 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
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*.



Set either or both of these to TRUE if you are going to set up **zimbra-proxy**.



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 Administration 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](#).

Move Mailboxes

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

You can set global options to exclude items from the mailbox move. See the Zimbra Collaboration Administration Guide 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 Collaboration Web Client.
- Spam and ham mailboxes.



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	zmpov -l ms <singleserver.com> -- -zimbraServiceEnabled mailbox
logger	zmpov -l ms <singleserver.com> -- -zimbraServiceEnabled logger
stats	zmpov -l ms <singleserver.com> -- -zimbraServiceEnabled stats
spell	zmpov -l ms <singleserver.com> -- -zimbraServiceEnabled spell
converted	zmpov -l ms <singleserver.com> -- -zimbraServiceEnabled converted

If archiving was installed, disable it as well:

```
zmpov -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.

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


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 a 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.

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-mm` 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-mm
```

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 *master-1* by default. If LDAP *master-1* is down, writes move to ldap *master-2*.
 - a. To enable the feature run:

```
./libexec/zmldapenable-mmrc -s 1 -m ldap://<<master-2.example.com>>:389/
```

- b. Once the feature is enabled use the **zmlocalconfig** command to add the LDAP servers to a group.

```
zmlocalconfig -e ldap_master_url="ldap://<<master-1.example.com>>:389  
ldap://<<master-2.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 LDAP 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](#) 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* submenu.
 - a. Type **2** to change the **LDAP Master host** name to the name of the primary master's hostname; e.g., *master-1.example.com*.
 - b. Type **4** to change the **LDAP admin password** to the Zimbra admin password of the primary master.
 - c. 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**.



Item **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 accordingly.

The next four steps are to change the default passwords on this server to match the passwords on the *master-1* LDAP server.

b. Type **7** to change the *LDAP replication password*.

c. Type **8** to change the *LDAP postfix password*.

d. Type **9** to change the *LDAP amavis password*.

e. Type **10** to change the *LDAP NGINX password*.

f. 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://<master-2.example.com>:389
ldap://<master-1.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-mmrm -s 3
```

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

```
zmlocalconfig -e ldap_master_url="ldap://<master-1.example.com>:389 \
ldap://<master-2.example.com>:389 ldap://<master-3.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.



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, `ldap-1.example.com`, `ldap-2.example.com`, `ldap-3.example.com`, with `ldap-3.example.com` being shut down.

```
zimbra@ldap-1:/tmp/mmr$ ./zmldapmmrtool -q
Master replication information
Master replica 1
rid: 100 URI: ldap://ldap-2.example.com:389/ TLS: critical Master replica 2
rid: 101 URI: ldap://ldap-3.example.com:389/ TLS: critical
```

2. The RID being used by `ldap-3.example.com` is `101`. This agreement can be deleted with:

```
zimbra@ldap-1:/tmp/mmr$ ./zmldapmmrtool -d -o 101
```

3. Confirm the deletion.

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



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
0	In Sync	The servers are currently in sync.
1	No contact	No connection to the master server and the system exits.

Error Code	Status	Description
2	Stand-alone	The master server has no replica servers and is considered a standalone master server.
3	Could not execute StartTLS	The replica server requires StartTLS and fails.
4	Server down	The replica server is currently down.
5	Unable to search	Searching the replica server for the context CSN fails.
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, `ldap-2.example.com` is the master server, and `ldap-3.example.com` and `ldap-4.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@ldap-2.example.com
Master: ldap://ldap-3.example.com:389 Code: 0 Status: In Sync CSN:
20120528123456.123456Z#000000#001#000000
Master: ldap://ldap-4.example.com:389 Code: 0 Status: In Sync CSN:
20120528123456.123456Z#000000#001#000000
Master: ldap://ldap-5.example.com:389 Code: 4 Status: Server down

```

Configuring LDAP Replication

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](#) for master LDAP server installation instructions. After the installation of the master LDAP server has completed, continue to [Enable Replication on the LDAP Master](#).

Enable Replication on the LDAP Master

On the master LDAP server, as the `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](#) 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
```

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) Store ephemeral attributes outside Ldap:	no
6) Secure interprocess communications:	Yes
7) 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 **Ldap port** to the same port as configured for the Master LDAP server.
6. Type **4** and change the **Ldap Admin password** to the Master LDAP admin password, then 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

- a. Type **2** and change **Create Domain** to **no**.
- b. Type **4** for **LDAP replication password** and enter the same password to match the value on the Master LDAP Admin user password for this local config variable.



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



If you have installed Zimbra MTA on the LDAP server, configure the Amavis and the Postfix passwords. To find these values, issue the following commands:

```
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.



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

Remove LDAP Replica from All Active Servers

1. On each member server, including the replica, verify the `ldap_url` value. Type `zmlocalconfig [ldap_url]`.
2. Remove the disabled LDAP replica server URL from `zmlocalconfig`. Do this by modifying the `ldap_url` to only include enabled ZCS LDAP servers.



The master LDAP server should always be at the end of the `ldap_url` string value.

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

Disable LDAP on the Replica

To disable LDAP on the replica server:

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

```
zmprov -l ms <zhostname> -zimbraServiceEnabled ldap
```

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



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

Monitoring LDAP Replication Status

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

Feature Requirement

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



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

Error Codes and Status Explanations

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

Error Code	Status	Description
0	In Sync	The servers are currently in sync.
1	No contact	No connection to the master server and the system exits.

Error Code	Status	Description
2	Stand-alone	The master server has no replica servers and is considered a standalone master server.
3	Could not execute StartTLS	The replica server requires StartTLS and fails.
4	Server down	The replica server is currently down.
5	Unable to search	Searching the replica server for the context CSN fails.
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, `ldap-2.example.com` is the master server, and `ldap-3.example.com` and `ldap-4.example.com` are replicas servers. The following screen-shot shows that replica server `ldap-3` is in sync with the master server, as indicated by the `Code:0` and `Status: In Sync`, and replica server `ldap-4` is currently down, as indicated by `Code: 4` and `Status: Server down`.


```
zimbra@ldap-2.example.com
Replica: ldap://ldap-3.example.com:389 Code: 0 Status: In Sync
Replica: ldap://ldap-4.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://ldap-3.example.com:389 Code: 0 Status: In Sync
Replica: ldap://ldap-4.example.com:389 Code: 6 Status: 0w 0d 0h 14m 42s behind
```

System Requirements for Zimbra Collaboration


Servers	<p>Evaluation and Testing</p> <ul style="list-style-type: none"> • Intel/AMD 64-bit CPU 1.5 GHz • RAM requirements: <ul style="list-style-type: none"> ◦ 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 <p>Production environments</p> <ul style="list-style-type: none"> • Intel/AMD 2.0 GHZ+ 64-bit CPU • RAM requirements: <ul style="list-style-type: none"> ◦ 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 <code>/opt/zimbra</code>, plus additional space for mail storage. The other nodes require 100MB. <p>General Requirements</p> <ul style="list-style-type: none"> • Firewall Configuration should be set to “No firewall”. • RAID-5 is not recommended for installations with more than 100 accounts.
Network Edition and Open Source supported Cloud platforms	<p>The following Cloud Platforms are supported:</p> <ul style="list-style-type: none"> • Oracle Cloud • VMware vCloud Director • VMware vCloud Air

Operating System (Network Edition)	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> • 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 • Oracle Linux 7.2 • Oracle Linux 6.6 • Ubuntu 16.04 LTS Server Edition (64-bit), starting from Zimbra Collaboration 8.7.1 and above • 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. Depreciated starting Zimbra Collaboration 8.8. <div>  <p>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.</p> </div>
Operating System (Open Source Edition)	<p>In addition to supporting the operating systems listed above for the Network Edition, other operating system versions are available for the Open Source Edition. Check the Zimbra Open Source Downloads page on https://www.zimbra.com.</p>
Virtualization (Network Edition)	<p>The following hypervisors are supported:</p> <ul style="list-style-type: none"> • VMware vSphere 5.x • VMware vSphere 4.x • XenServer 6.5 • XenServer 6.2 • KVM
File Systems	<p>The following file systems are supported:</p> <ul style="list-style-type: none"> • XFS • ext3 or ext4 file systems for Linux deployments • NFS for backup only



Other Dependencies	<p>Netcat (nc) is required on all operating systems using Zimbra Collaboration. The nc utility must be installed prior to installation or upgrading.</p> <p>For SUSE and Ubuntu systems, disable AppArmor and verify that the AppArmor service is not running before installing Zimbra Collaboration.</p> <p>For Red Hat Enterprise, Fedora Core and SUSE operating systems, the server must also have the following installed:</p> <ul style="list-style-type: none"> • NPTL. Native POSIX Thread Library • Sudo. Superuser, required to delegate admins. • libidn. For internationalizing domain names in applications (IDNA) • GMP. GNU Multiple-Precision Library. <p>For Ubuntu 14 and Ubuntu 12:</p> <ul style="list-style-type: none"> • Sudo • libidn11 • libpcre3 • libexpat1 • libgmp3c2
Miscellaneous	<ul style="list-style-type: none"> • 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.

<p>Administrator Computers</p> <p>NOTE: Other configurations may work.</p>	<p>The following operating system/browser combinations are supported:</p> <p>Windows 7 SP1, Windows 8 or Windows 10 with one of the following:</p> <ul style="list-style-type: none"> • Microsoft support is only available for Internet Explorer 11 or Microsoft Edge <ul style="list-style-type: none"> ◦ IE11 and higher for Windows 7 SP1 ◦ IE11 and higher for Windows 8 ◦ IE11 or Microsoft Edge (Supported since ZCS 8.6 P4 and above) for Windows 10 • The latest stable release of: <ul style="list-style-type: none"> ◦ Firefox ◦ Safari ◦ Google Chrome <p>Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10, or 10.11 with one of the following:</p> <ul style="list-style-type: none"> • The latest stable release of: <ul style="list-style-type: none"> ◦ Firefox ◦ Safari ◦ Google Chrome <p>Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following:</p> <ul style="list-style-type: none"> • The latest stable release of: <ul style="list-style-type: none"> ◦ Firefox ◦ Google Chrome
<p>Administrator Console Monitor</p>	<p>Display minimum resolution 1024 x 768</p>

End Computers Zimbra Client	User using Web	<p>For Zimbra Web Client - Advanced & Standard version</p> <p>Minimum</p> <ul style="list-style-type: none"> • Intel/AMD/Power PC CPU 750MHz • 256MB RAM <p>Recommended</p> <ul style="list-style-type: none"> • Intel/AMD/Power PC CPU 1.5GHz • 512MB RAM <p>The following operating system/browser combinations are supported:</p> <p>Windows 7 SP1, Windows 8 or Windows 10 with one of the following:</p> <ul style="list-style-type: none"> • Microsoft support is only available for Internet Explorer 11 or Microsoft Edge <ul style="list-style-type: none"> ◦ IE11 and higher for Windows 7 SP1 ◦ IE11 and higher for Windows 8 ◦ IE11 or Microsoft Edge (Supported since ZCS 8.6 P4 and above) for Windows 10 • The latest stable release of: <ul style="list-style-type: none"> ◦ Firefox ◦ Safari ◦ Google Chrome <p>Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10, or 10.11 with one of the following:</p> <ul style="list-style-type: none"> • The latest stable release of: <ul style="list-style-type: none"> ◦ Firefox ◦ Safari ◦ Google Chrome <p>Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following:</p> <ul style="list-style-type: none"> • The latest stable release of: <ul style="list-style-type: none"> ◦ Firefox ◦ Google Chrome
NOTE: configurations may work.	Other	

End User Computers Using Other Clients	<p>Minimum</p> <ul style="list-style-type: none"> • Intel/AMD/Power PC CPU 750MHz • 256MB RAM <p>Recommended</p> <ul style="list-style-type: none"> • Intel/AMD/Power PC CPU 1.5GHz • 512MB RAM <p>Operating system POP/IMAP combinations</p> <ul style="list-style-type: none"> • Windows 7 SP1 with Outlook Express 6, Outlook 2007 and above (MAPI), Thunderbird • Fedora Core 4 or later with Thunderbird • Mac OS X 10.6 or later with Apple Mail <p>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.</p> <div>  <p>If users are presently using IE 10 or older, Zimbra strongly recommends that they upgrade to the latest version of Internet Explorer for optimal performance with ZWC.</p> </div>
Exchange Web Services	<p>EWS Clients</p> <ul style="list-style-type: none"> • Outlook 2011/2016 (MAC only) • Apple Desktop Clients (OS X, 10.8+) <p>EWS Interoperability</p> <ul style="list-style-type: none"> • Exchange 2010+
Monitor	<p>Display minimum resolution: 1024 x 768</p>
Internet Connection Speed	<p>128 kbps or higher</p>

Zimbra Connector for Outlook (Network Edition Only)

Operating System	<ul style="list-style-type: none"> • Windows 10 • Windows 8 • Windows 7 SP1 <div>  <p>Windows 7 SP1 is in its Extended Support period until January 14, 2020. Zimbra Collaboration 8.8.x is the last release to support Microsoft Outlook 2010 and Microsoft Windows 7 SP1.</p> </div>
Microsoft Outlook	<ul style="list-style-type: none"> • Outlook 2016: 32-bit and 64-bit editions of Microsoft Outlook are supported. • 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. • Office365: Click-to-run versions of Microsoft Outlook are supported. (BETA) <div>  <p>Outlook 2007 is deprecated. The 8.6 series of Zimbra Collaboration is the last release to support Microsoft Outlook 2007. Support for 8.6 ends in September 2018.</p> </div>

Zimbra Mobile (Network Edition Only)

Network Edition 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, iOS9
- Android 2.3 and above
- Windows Mobile 6.0 and above
- Microsoft Outlook using the Exchange ActiveSync (EAS)

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

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

Note: To find SSH client software, go to Download.com at <http://www.download.com/> and search for SSH. The list displays software that can be purchased or downloaded for free. An example of a free SSH client software is PuTTY, a software implementation of SSH for Win32 and Unix platforms. To download a copy go to <http://putty.nl>

Zimbra Network NG Modules: First Steps

This Guide contains all information needed to switch to the new Zimbra Network NG modules from their legacy counterparts after upgrading to Zimbra 8.8.

Switching to Backup NG

Switching to the new Backup NG is a simple process that will initialize the new backup system on a dedicated path. Until the initialization is completed, the old backup engine will be active. Old backup files will not be removed and the old backup and restore tools are still available via the usual CLI commands.

Backup Path Limitations

To hold Backup NG data, a storage must comply to the following:

- The storage must have a mountpoint on the system.
 - The "zimbra" user must of course have r/w permission on the path.
- The data must be stored on a case-sensitive filesystem.



Backup NG features a built-in scheduling system and does not rely on the system's cron service. At the end of the initialisation process, old backup-related crontab lines will be automatically removed.

Backup NG Initialization

Before initializing the Backup NG module, make sure you have enough space on the storage where you will store the backup. The average size of the backup is 50-70% of the nominal total quota of all mailboxes.

To initialize the Backup NG module:

- Access the Zimbra Administration Console.
- Enter the "Network Modules NG" section on the left menu.
- Enter the "Backup" section.
- Set the "Backup Path" to the directory where you will store your backup.
- Click the "Initialize" button - this will trigger a SmartScan to initialize the Backup Path

Switching to Mobile NG

Switching to the new Mobile NG is a simple process that will activate the new mobile handlers and deactivate the old ones. This will also switch the synchronization control over to Mobile NG from the legacy Zimbra Mobile. Until the initialization is complete, the old mobile engine will be active.

What Happens after the Switch

After switching to Mobile NG, all existing syncstates will be invalidated, and all connected devices will automatically re-synchronise all of their data through the new engine.



Since the switch will force all connected devices to re-synchronise all of their data, make sure to alert your users beforehand to make sure that they have wifi coverage or enough traffic on their mobile data plans.

Furthermore, the switch might lead to an abrupt increase in the number of connections to the server, and consequently its load, due to the resynchronisation of all devices.

The switch is completely transparent to end users, and no user interaction should be prompted or required, but being the Exchange ActiveSync protocol mostly client-driven different behaviours might be experienced, such as:

- Device not synchronising until user's action (e.g. opening the email client).
- Device requiring a restart.
- Device not synchronising until the user re-enters their username and password in the account's settings.

Albeit sporadic, such behaviours and the load impact on the system should be taken into account when planning to switch to Mobile NG.

Mobile NG Initialization

To initialize Mobile NG:

- Access the Zimbra Administration Console.
- Enter the "Network Modules NG" section on the left menu.
- Enter the "Mobile" section.
- Click the "Activate" button.

Switching to HSM NG

The HSM NG module will become active as soon as the upgrade to Zimbra 8.8 is complete, and does not require any interaction.

Any old HSM policy, volume and volume configuration will be maintained.



HSM NG features a built-in scheduling system and does not rely on the system's cron service. At the first start after the upgrade, old HSM-related crontab lines will be automatically removed.

Switching to Admin NG

Switching to the new Admin NG is a simple process that will migrate any relevant ACL information to the module's own configuration manager, clearing existing ACLs and ACEs from the system.

Admin NG is significantly different than the old Delegated Administration engine. Please read the product's documentation and only migrate to Admin NG if its feature set meets your needs.



Switching to Admin NG will remove all existing ACLs and ACEs from the server. This new module is extremely different from its legacy counterpart, so after the migration will not be able to recreate the very same admin roles and settings.

This is a one way only process.

Once Admin NG is initialized it's not possible to go back to the old engine, so if you have customized or complex ACLs/ACEs carefully consider whether or not to switch.

Admin NG Initialization

Admin NG is not enabled by default during upgrades from a version earlier than 8.8, so it must be enabled manually before migrating to it.

To enable Admin NG:

- Run the following command as the "zimbra" user on any mailbox server:

```
zmprov mcf zimbraNetworkAdminNGEnabled TRUE
```

To initialize Admin NG:

- Access the Zimbra Administration Console.
- Enter the "Network Modules NG" section on the left menu.
- Enter the "Admin" section.
- Click on the "Migrate" button.