Zimbra Collaboration Performing a Single-Server Installation

v8.8.9, July, 2018

Table of Contents

License

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

http://www.synacor.com

Introduction

Zimbra Collaboration includes the Zimbra *MTA*, the Zimbra *LDAP* server, and the Zimbra *mailbox* server. In a single-server installation, all components are installed on one server and require no additional manual configuration.

This installation guide is a quick start guide that describes the basic steps needed to install and configure Zimbra Collaboration in a direct network connect environment. In this environment, the Zimbra server is assigned a domain for which it receives mail, and a direct network connection to the Internet. When Zimbra Collaboration is installed, you will be able to log on to the Zimbra administration console to manage the domain and provision accounts. The accounts you create are able to send and receive external email.

Important Notice About Single Server Installations

Zimbra Collaboration is designed to be the only application suite installed on the server. As part of the installation process, Zimbra Collaboration bundles and installs various other third party and open source software, including Eclipse Jetty, Postfix, and OpenLDAP®. The versions installed have been tested and configured to work with Zimbra software. See the Zimbra Collaboration Administrator Guide for a complete list of software.

A Zimbra license is required in order to create accounts on servers running Zimbra Collaboration Network Edition. You cannot install Zimbra Collaboration Network Edition without a license.

The following table shows the default port settings when Zimbra Collaboration is installed.

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); zimbraMailBindAddress
8443	https	mailbox	Backend HTTPS (if proxy configured on same host); zimbraMailSSLBindAddress
8465	milter	mta/opendkim	OpenDKIM milter service; localhost
8735	zextras	mailbox	internal mailbox to mailbox communication.

8736	zextras	mailbox	distributed configuration
10024	smtp	mta/amavisd	to amavis from postfix; localhost
10025	smtp	mta/master	opendkim; localhost
10026	smtp	mta/amavisd	"ORIGINATING" policy; localhost
10027	smtp	mta/master	postjournal
10028	smtp	mta/master	content_filter=scan via opendkim; 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); zimbraMemcachedBindAddress

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 & zmrcd): 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; zimbraConvertdURL
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.

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.

ℹ 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.

Overview of the Installation Process

When you run the install script, the process verifies that the correct prerequisite Zimbra application packages are available to be installed.

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 Convertd** is installed.
- **Zimbra Convertd:** This package should be installed on at least one **Zimbra-Store** server. Only one **Zimbra-Convertd** package needs to be present in the Zimbra Collaboration environment. The default is to install one **Zimbra-Convertd** 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 docu- ments 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.

Downloading the Zimbra Software

Obtain the Zimbra Collaboration software download and save to the computer from which you will install the software.

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.

Basic 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 (optional) on one server.

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		

Server Configured	Menu Item	Description
	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.
	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 config 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	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. ℹ This option is displayed only if the zimbra-proxy package is installed.
	LDAP Bes Searcher password	This password is automatically generated and is used by the ldap BES user.

Zimbra Logger

Server Configured	Menu Item	Description
Zimbra mailbox server	**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.

Server Configured	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	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. 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.
	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		
Zimbra Mailbox Server	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		
Zimbra Mailbox Server	**SMTP host**	Defaults to current server name
	Web server HTTP port:	default **80**
	Web server HTTPS port:	default **443**
	Web server mode	Can be **HTTP**, **HTTPS**, **Mixed**, **Both** or **Redirect**. • **Mixed** mode uses HTTPS for logging in and HTTP for normal session traffic • **Both** mode means that an HTTP session stays HTTP, including during the login phase, and an HTTPS session remains HTTPS throughout, including the login phase. • **Redirect** mode redirects any users connecting via HTTP to 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	http://<example.com>:7780/aspell.php
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`.		

zimbra-store		
Zimbra Mailbox Server	*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.	This enables automatic notification when updates are available when this is set to **TRUE**. ℹ The software update information can be viewed from the Administration Console Tools Overview pane.
	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.

Server Configured	**Menu Item**	**Description**
zimbra-proxy		

Server Configured	Menu Item	Description
mailbox server, MTA server 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?	default **no**. If **yes**, the following global config settings will be applied: - This server will be added to the list of `zimbraReverseProxyUpstreamImapServers` - Embedded IMAP[S] servers will be disabled.

Installing Zimbra Collaboration Software

Important: Before you begin, make sure to:

- (Network Edition Only) Store your license in a directory folder on your server as it is needed to complete your installation of Zimbra Collaboration
- Confirm you have the latest system requirements and prerequisites for installing Zimbra Collaboration.

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

1. Log in as root to the Zimbra server and cd to the directory where the Zimbra Collaboration archive tar file is saved (cd /var/<tmp>). Type the following commands:
   - Unpack the file: `tar xvzf [zcsfullfilename.tgz]`
   - Change to the correct directory: `cd [zcsfullfilename]`
   - Begin the installation: `./install.sh`

   ```
   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
   ```

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/# 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

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.
   Important: 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. Zimbra IMAPD is meant to be installed on a multi-server environment, with hundreds of thousands of users, and it's still a Beta Release. Zimbra recommends to only install it for demo and evaluation purposes.*

   - If installing **Zimbra Network Edition**, you will have the modules Archiving and Convertd as an option to add to your Zimbra installation.

   - It is recommended to only install Zimbra-dnscache on the MTA Servers when there are no other DNS servers (for example dnsmasq or bind) already installed and running on the same server.

   ```
   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

Use internal development repo [N] n
Configuring package repository

Install zimbra-ldap [Y] y

Install zimbra-logger [Y] y

Install zimbra-mta [Y] y

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] y

Install zimbra-proxy [Y] y

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
     MISSING: libreoffice

###WARNING###

One or more suggested packages for zimbra-store are missing.
Some features may be disabled due to the missing package(s).


Installing:
    zimbra-core
    zimbra-ldap
    zimbra-logger
    zimbra-mta
    zimbra-snmp
    zimbra-store
    zimbra-apache
    zimbra-spell
    zimbra-convertd
    zimbra-memcached
    zimbra-proxy
    zimbra-archiving
    zimbra-chat
    zimbra-drive
    zimbra-network-modules-ng


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

Also select the services to be installed on this server. To install Zimbra Collaboration on a single server, enter `Y` for the ldap, logger, mta, snmp, store, and spell packages. If you use IMAP/POP Proxy, enter `Y` for the Zimbra proxy package and the Zimbra Memcached package.

Note: Ensure that the `zimbra-memcached` package is installed on at least one of the nodes in the system if the Proxy is installed.

Note: 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.

5. Next, type `Y` and press *Enter* to modify the system.

    - Selected packages are installed on the server.
    - Checks to see if MX record is configured in DNS. The installer checks to see if the hostname is resolvable via DNS. If there is an error, the installer asks if you would like to change the hostname. We recommend that the domain name have an MX record configured in DNS.
    - Checks for port conflict.

6. At this point, the Main menu displays showing the default entries for the Zimbra components 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 packages being installed. Values that require further configuration are marked with asterisks (******) to their left. To navigate the Main menu, select the menu item to change. You can modify any of the defaults. For a quick installation, accepting all the defaults, you only need to do the following:
7. To set the appropriate time zone, enter `1` to select Common Configuration and then enter `7` for TimeZone. Set the correct time zone.

```
Main menu

   1) Common Configuration:
   2) zimbra-ldap:                             Enabled
   3) zimbra-logger:                           Enabled
   4) zimbra-mta:                              Enabled
   5) zimbra-snmp:                             Enabled
   6) zimbra-store:                            Enabled
        +Create Admin User:                    yes
        +Admin user to create:                 admin@zimbra.io
******* +Admin Password                        UNSET
        +Anti-virus quarantine user:           virus-
quarantine.bcsk28oyoe@zimbra.io
        +Enable automated spam training:       yes
        +Spam training user:                   spam.dqxmkmf5tv@zimbra.io
        +Non-spam(Ham) training user:          ham.pcq8excwph@zimbra.io
        +SMTP host:                            z883.zimbra.io
        +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://z883.zimbra.io:7780/aspell.php
        +Enable version update checks:         TRUE
        +Enable version update notifications:  TRUE
        +Version update notification email:    admin@zimbra.io
        +Version update source email:          admin@zimbra.io
        +Install mailstore (service webapp):   yes
        +Install UI (zimbra,zimbraAdmin webapps): yes
******* +License filename:                     UNSET

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

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

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

9. Type `r` to return to the Main menu.

10. Enter `7` to select **zimbra-store** from the Main menu. The store configuration menu displays.

11. Select the following from the store configuration menu:
    - Type 4 to set the Admin Password. The password must be six or more characters. Press *Enter*.
    - (Network Edition only) Type 33 for **License filename** and type the directory and file name for the Zimbra license. For example, if you saved to the `/tmp` directory, you would type `/tmp/ZimbraLicense.xml`. If you do not have the license, you cannot proceed. See the section on Zimbra License Requirements
    - Enable version update checks and Enable version update notifications.
      If these 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.
12. Type `r` to return to the Main menu.
13. If you want to change the default Class of Service settings for new features that are listed here, type 12 for Default Class of Service Configuration.
    Then type the appropriate number for the feature to be enabled or disabled. Changes you make here are reflected in the default COS configuration.
14. If no other defaults need to be changed, type `a` to apply the configuration changes. Press *Enter*

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

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

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

16. 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.
    ```

17. 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. Components that are installed include spam training and documents, (wiki) accounts, time zone preferences, backup schedules, licenses, as well as common Zimlets.

    ```
    The system will be modified - continue? [No] y
    Operations logged to /tmp/zmsetup.20160711-234517.log
    Setting local config values...done.
    Initializing core config...Setting up CA...done.
    Deploying CA to /opt/zimbra/conf/ca ...done.
    Creating SSL zimbra-store certificate...done.
    ```

```
Creating new zimbra-ldap SSL certificate...done.
Creating new zimbra-mta SSL certificate...done.
Creating new zimbra-proxy SSL certificate...done.
Installing mailboxd SSL certificates...done.
Installing MTA SSL certificates...done.
Installing LDAP SSL certificate...done.
Installing Proxy SSL certificate...done.
Initializing ldap...done.
.
.
Checking current setting of zimbraReverseProxyAvailableLookupTargets
Querying LDAP for other mailstores
Searching LDAP for reverseProxyLookupTargets...done.
Adding zmail.example.com to zimbraReverseProxyAvailableLookupTargets
Setting convertd URL...done.
.
.
Granting group zimbraDomainAdmins@zmail.example.com domain right
+domainAdminConsoleRights on zmail.example.com...done.
Granting group zimbraDomainAdmins@zmail.example.com global right
+domainAdminZimletRights...done.
Setting up global distribution list admin UI components..done.
Granting group zimbraDLAdmins@zmail.example.com global right
+adminConsoleDLRights...done.
.
.
Setting default backup schedule...Done
Looking for valid license to install...license installed.
Starting servers...done.
Installing common zimlets...
        com_zimbra_attachmail...done.
        com_zimbra_phone...done.
        com_zimbra_proxy_config...done.
          .
          .
        com_zimbra_ymemoticons...done.
        com_zimbra_date...done.
Finished installing common zimlets.
Installing network zimlets...
        com_zimbra_mobilesync...done.
         .
         .
        com_zimbra_license...done.
Finished installing network zimlets.
Restarting mailboxd...done.
Creating galsync account for default domain...done.
Setting up zimbra crontab...done.


Moving /tmp/zmsetup.20160711-234517.log to /opt/zimbra/log
```

```
Configuration complete - press return to exit
```

Final Set-Up (required)

After the Zimbra Collaboration servers are configured, the following functions must be configured.

> ❗ 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.

If **zimbra-logger** is installed, set up the **syslog** configuration files to enable server statistics to display on the administration console, and enable the logger monitor host. The server statistics includes information about the message count, message volume, and anti-spam and anti-virus activity.

Access to the 'zimbra' user

Zimbra Collaboration ships a default `zimbra` user with a disabled password. Zimbra Collaboration requires access to this account via **ssh public key authentication**. On most operating systems this combination is okay, but if you have modified pam rules to disallow any ssh access to disabled accounts then you must define a password for the `zimbra` UNIX account. This will allow ssh key authentication for checking remote queues. See the Zimbra wiki article, Mail Queue Monitoring.

Set up the ssh keys. To populate the ssh keys

```
sudo -u zimbra -i # if not already logged in as the zimbra user
zmupdateauthkeys
```

The key is updated on `/opt/zimbra/.ssh/authorized_keys`

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

> ℹ Note, your system may use a different provider for the syslog service. See the Wiki article Configuring Logger Host for more information

1. As **root**, type the following command to enable the server to display statistics - `/opt/zimbra/libexec/zmsyslogsetup`
2. You must enable syslog to log statistics from remote machines.

   RedHat Systems

   - Edit the `/etc/sysconfig/syslog` file to add -r to the SYSLOGD_OPTIONS setting, `SYSLOGD_options="-r -m 0"`
   - Stop the syslog daemon - `/etc/init.d/syslog stop`
   - Start the syslog daemon - `/etc/init.d/syslog start`

Debian and Ubuntu Systems

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

Final Set-Up (optional)

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 respository 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 that `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_GA_1231;
         zmauth;
     }
     ```

   - 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 `zmproxyctl 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 `zmproxyctl 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;
    }
```

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 using a single node:

```
zmprov mcf zimbraAttachmentsScanURL clam://localhost:3310/
zmprov mcf zimbraAttachmentsScanEnabled TRUE
```

Provisioning Accounts

Once the mailbox server is running, open your browser, enter the administration console URL and log on to the console to provision email accounts. The administration console URL is entered as:

```
https://[mailhost.example.com]:7071
```

> To go to the administration console, you must type **https**, even if you configured the Web server mode as HTTP.

The first time you log on, a warning may be displayed stating the connection is untrusted. This only applies the first time you log in. Click **I understand the Risks** to be able to connect to the Zimbra administration console. Then click `OK`.

Enter the admin user name and password configured during the installation process. Enter the name as `admin@mailhost.example.com`

Activate the Zimbra Collaboration license (Network Edition Only)

Admin Console:

After you log on, a dialog displays stating your license is not activated.

Go to:

Home > **Configure** > **Global Settings** > **License**

click `Activate License` on the toolbar then Click `OK` to continue.

Provision 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

Admin Console:

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

1. From the administration console **Home** page’s Content pane, go to `Add Accounts`.

   > Four accounts will already be listed - the admin account, two spam training accounts, and a global Documents account. These accounts do not need any additional configuration.

2. Click `Add Account`. 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 is 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, you can send and receive emails.

Importing Content from User Mailboxes

Zimbra developed different applications to facilitate moving a user's 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. Use one of the Zimbra Collaboration utilities to move user mail to Zimbra Collaboration to guarantee that all information is imported correctly.

The following applications can be accessed from the administration console **Download page**, and instruction guides are available from the Help Desk page or from the Zimbra Website, Documentation page.

Alternatively, you can download the following applications from https://example.com/downloads/index.html (with "example.com" being your Zimbra server name).

- **Zimbra Collaboration Migration Wizard for Exchange**. Format is an .exe file. You can migrate users from Microsoft® Exchange server email accounts to Zimbra server accounts.
- **Zimbra Collaboration Migration Wizard for Domino**. Format is an .exe file. You can migrate users from Lotus Domino server email accounts to Zimbra server accounts.
- **PST Import Wizard** (User Instructions). Format is an .exe file. Users download the Import Wizard to their computers and run the executable file to import their Outlook .pst files to the Zimbra server. Before users run this utility, Zimbra recommends that they run the Outlook Inbox Repair tool, `scanpst.exe`, on their .pst files, to clean up any errors in their file. For more information about this tool, go to http://support.microsoft.com/kb/287497.

Administrator Account

Initial administrative tasks when you log on for the first time may include setting up the admin mailbox to include features, aliases, and forwarding addresses needed for the administrator's working environment.

Two aliases for the admin account are created during install:

- **Postmaster**. The postmaster address is displayed in emails that are automatically generated from Postfix when messages cannot be sent. If users reply to this address, the message is forwarded to the admin mailbox.
- **Root**. This address is where notification messages from the operating system are sent.

If you entered a notification address for AV alerts when you configured the MTA, that is different from the default, you need to create that account in the administration console. If you didn’t change the default during installation, the anti-virus notification is sent directly to the admin account.

Uninstalling Zimbra Collaboration

To uninstall servers, run the install script -u, delete the Zimbra Collaboration directory, and remove the zcs.tgz file on the servers.

1. cd to the original install directory for the Zimbra Collaboration files.
2. Type `sudo ./install.sh -u`
3. When `Completely remove existing installation?` is displayed, type `Yes`. The Zimbra servers are stopped, the existing packages, webapp directories, and most of the contents of the `/opt/zimbra` directory are removed.
4. Type `rm -rf [zcsfullfilename]` to delete the Zimbra Collaboration directory.
5. Delete the zcs.tgz file.

System Requirements for Zimbra Collaboration

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

Operating System (Network Edition)	The following operating systems are supported: - Red Hat® Enterprise Linux® 7 (64-bit) - CentOS Linux® 7 (64-bit) - Red Hat Enterprise Linux 6 (64-bit), **patch level 4 or later is required** - CentOS Linux 6 (64-bit), **patch level 4 or later is required** - 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. Deprecated starting Zimbra Collaboration 8.8**. ℹ 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.
Operating System (Open Source Edition)	In addition to supporting the operating systems listed above for the Network Edition, other operating system versions are available for the Open Source Edition. Check the Zimbra Open Source Downloads page on https://www.zimbra.com.
Virtualization (Network Edition)	The following hypervisors are supported: - VMware vSphere 5.x - VMware vSphere 4.x - XenServer 6.5 - XenServer 6.2 - KVM
File Systems	The following file systems are supported: - **XFS** - **ext3** or **ext4** file systems for Linux deployments - **NFS** for backup only

Other Dependencies	Netcat (nc) is required on all operating systems using Zimbra Collaboration. The `nc` utility must be installed prior to installation or upgrading. For SUSE and Ubuntu systems, disable **AppArmor** and verify that the AppArmor service is not running before installing Zimbra Collaboration. For Red Hat Enterprise, Fedora Core and SUSE operating systems, the server must also have the following installed: • **NPTL**. Native POSIX Thread Library • **Sudo**. Superuser, required to delegate admins. • **libidn**. For internationalizing domain names in applications (IDNA) • **GMP**. GNU Multiple-Precision Library. For Ubuntu 14 and Ubuntu 12: • Sudo • libidn11 • libpcre3 • libexpat1 • libgmp3c2
Miscellaneous	• SSH client software to transfer and install the Zimbra Collaboration software. • Valid DNS configured with an A record and MX record. • Servers should be configured to run Network Time Protocol (NTP) on a scheduled basis.

Administrator Computers NOTE: Other configurations may work.	The following operating system/browser combinations are supported: Windows 7 SP1, Windows 8 or Windows 10 with one of the following: • Microsoft support is only available for Internet Explorer 11 or Microsoft Edge ◦ 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: ◦ Firefox ◦ Safari ◦ Google Chrome Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10, or 10.11 with one of the following: • The latest stable release of: ◦ Firefox ◦ Safari ◦ Google Chrome Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following: • The latest stable release of: ◦ Firefox ◦ Google Chrome
Administrator Console Monitor	Display minimum resolution 1024 x 768

End User Computers using Zimbra Web Client NOTE: Other configurations may work.	**For Zimbra Web Client - Advanced & Standard version** Minimum • Intel/AMD/Power PC CPU 750MHz • 256MB RAM Recommended • Intel/AMD/Power PC CPU 1.5GHz • 512MB RAM The following operating system/browser combinations are supported: Windows 7 SP1, Windows 8 or Windows 10 with one of the following: • Microsoft support is only available for Internet Explorer 11 or Microsoft Edge ◦ 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: ◦ Firefox ◦ Safari ◦ Google Chrome Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10, or 10.11 with one of the following: • The latest stable release of: ◦ Firefox ◦ Safari ◦ Google Chrome Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following: • The latest stable release of: ◦ Firefox ◦ Google Chrome

End User Computers Using Other Clients	Minimum • Intel/AMD/Power PC CPU 750MHz • 256MB RAM Recommended • Intel/AMD/Power PC CPU 1.5GHz • 512MB RAM Operating system POP/IMAP combinations • Windows 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 **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. 💡 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.
Exchange Web Services	EWS Clients • Outlook 2011/2016 (MAC only) • Apple Desktop Clients (OS X, 10.8+) EWS Interoperability • Exchange 2010+
Monitor	Display minimum resolution: 1024 x 768
Internet Connection Speed	128 kbps or higher

Zimbra Connector for Outlook (Network Edition Only)

Operating System	• Windows 10 • Windows 8 • Windows 7 SP1 ❗ 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.
Microsoft Outlook	• 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) ❗ 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.

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

Galaxy S® 4, Galaxy Nexus™

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-synchonise 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.