



Zimbra™ Collaboration Suite Single Server Installation

Open Source Edition 7.0

February 2011

Legal

Copyright ©2005-2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

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

Zimbra, a division of VMware, Inc.

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

February 2011- ZCS 7.0

2/7/11

Zimbra™ Collaboration Suite Single Server Installation - Open Source

The Zimbra Collaboration Suite 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 the Zimbra Collaboration Suite 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 the Zimbra Collaboration Suite 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 will be able to send and receive external email.

Topics in this chapter include:

- ◆ [Important Notice About Single Server Installations](#)
- ◆ [Installation Prerequisites](#)
- ◆ [Modifying Operating System Configurations](#)
- ◆ [Configure DNS](#)
- ◆ [Overview of Installation Process](#)
- ◆ [Downloading the Zimbra Software](#)
- ◆ [Basic Configuration](#)
- ◆ [Installing Zimbra Software](#)
- ◆ [Provisioning Accounts](#)
- ◆ [Support and Contact Information](#)

Important Notice About Single Server Installations

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

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

Table Zimbra Port Mapping

	Port
Remote Queue Manager	22
Postfix	25
HTTP	80
POP3	110
IMAP	143
LDAP	389
HTTPS	443
Mailboxd IMAP SSL	993
Mailboxd POP SSL	995
Mailboxd LMTP	7025

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

Installation Prerequisites

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

System Requirements

For the ZCS system requirements see Other Dependencies in [System Requirements for Zimbra Collaboration Suite 7.0](#).

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>

Modifying Operating System Configurations

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

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

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

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

Configure 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, ZCS checks to see if you have an MX record correctly configured. If it is not, an error is displayed suggesting that the domain name have an MX record configured in DNS.

You must configure a relay host if you do not enable DNS. After ZCS is installed, go to the **Global Settings>MTA** tab on the administration console and uncheck **Enable DNS lookups**. Enter the relay MTA address to use for external delivery.

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

Overview of Installation Process

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

- **Zimbra Core** installs the libraries, utilities, and monitoring tools.
- **Zimbra LDAP** installs the OpenLDAP software, which provides open source LDAP directory services.
- **Zimbra Store** installs the mailbox server, including Jetty, the servlet container for the Zimbra server.
- **Zimbra MTA** installs the Postfix open source MTA, the Clam AntiVirus antivirus engine, the SpamAssassin junk mail filter, and the Amavisd-New content filter.
- **Zimbra SNMP** installs the SNMP package for monitoring. This package is optional.
- **Zimbra Logger** installs tools for syslog aggregation and reporting. If you do not install Logger the server statistics are not captured, and the server statistics section of the administration console does not display.
- **Zimbra Spell** installs the Aspell open source spelling checker.
- **Zimbra Apache** is installed automatically when Zimbra Spell is installed.

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.

Downloading the Zimbra Software

For the latest Zimbra software download, go to www.zimbra.com. Save the Zimbra Collaboration Suite archive file to the computer from which you will install the software.

Zimbra Sales by contacting sales@zimbra.com or calling 1-650-427-5701 sales@zimbra.com or by calling 1-650-427-5701

Basic Configuration

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

Table Main Menu Options

Main Menu	Description
1) Common Configuration - These are common settings for all servers	
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.
LDAP port	The default port is 389
LDAP Admin password	This is the master LDAP password.
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).
2) zimbra-ldap	
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	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 now. In most cases, you will accept the default.
LDAP Root password	The root LDAP password for internal LDAP operations.

Table Main Menu Options

Main Menu	Description
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 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 password on the LDAP server.
3) zimbra-store	
Create Admin User	The administrator account is created during installation. This account is the first account provisioned on the Zimbra server and allows you to log on to the administration console.
Admin user to create	The default is admin@[mailhost.example.com].
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.

Table Main Menu Options

Main Menu	Description
Enable automated spam training	<p>By default, the automated spam training filter is enabled and two mail accounts are created.</p> <ol style="list-style-type: none"> 1. Spam Training User to receive mail notification about mail that was not marked as junk, but should have been. 2. Non-spam (HAM) Training User to receive mail notification about mail that was marked as junk, but should not have been. <p>These addresses are automatically configured to work with the spam training filter. The accounts created have a randomly selected name. To recognize what the account is used for, you may want to change this name.</p>
The default port configurations are shown	<ul style="list-style-type: none"> • SMTP host • Web server HTTP port: 80 • Web server HTTPS port: 443 • Web server mode — Can be HTTP, HTTPS, Mixed, Both or Redirect. <p>Mixed mode uses HTTPS for logging in and HTTP for normal session traffic</p> <p>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.</p> <p>Redirect mode redirects any users connecting via HTTP to an HTTPS connection.</p> <p>All modes use SSL encryption for back-end administrative traffic.</p> <ul style="list-style-type: none"> • IMAP server port: 143 • IMAP server SSL port: 993 • POP server port: 110 • POP server SSL port: 995 • Use spell checker server, default Yes (if installed) • Spell server URL: http://<example.com>:7780/aspell.php

Table Main Menu Options

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

Table Main Menu Options

Main Menu	Description
4) zimbra-mta	
	<ul style="list-style-type: none"> • MTA Auth host — This is configured automatically if the MTA authentication server host is on the same server, but must be configured if the authentication server is not on the MTA. • Enable Spamassassin — Default is enabled. • Enable ClamAV — Default is enabled. • Notification address for AV alerts — Sets the notification address for AV alerts. You can either accept the default or create a new address. If you create a new address, remember to provision this address from the admin console. <hr/> <p><i>Note: If the virus notification address does not exist and your host name is the same as the domain name on the Zimbra server, the virus notifications queue in the Zimbra MTA server cannot be delivered.</i></p> <hr/> <ul style="list-style-type: none"> • 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 password on the LDAP server.
5) zimbra-snmp (optional)	
	<ul style="list-style-type: none"> • Enable SNMP notifications — The default is Yes. • SNMP Trap hostname • Enable SMTP notification — The default is Yes. • SMTP Source email address • SMTP Destination email address

Table Main Menu Options

Main Menu	Description
6) zimbra-logger	When installed, it is automatically enabled. Logs from the hosts are sent to the mailbox server where zimbra-logger is installed and the information is used to generate the statistics graphs and for message tracing.
7) zimbra-spell	(optional) When installed, it is automatically enabled.
9) Default Class of Service Configuration	This menu section lists major new features for the ZCS release and whether the feature is enabled or not. When you change the feature setting during ZCS installation, you change the default COS settings Having this control, lets you decide when to introduce new features to your users.
c) Collapse menu	Allows you to expand or collapse the menu.
r) Start servers after configuration	When the installation and configuration is complete, if this is set to Yes , the Zimbra server is automatically started.
s) Save config to file	At any time during the installation, you can save the configuration to file.
x) Expand menu	Expand menus to see the underlying options
q) Quit	Quit can be used at any time to quit the installation.

Installing Zimbra Software

Important: Before you begin, make sure to:

- Confirm you have the latest system requirements and prerequisites for installing ZCS, as described in [System Requirements for Zimbra Collaboration Suite 7.0 on page 27](#).

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 Suite archive tar file is saved (**cd /var/<tmp>**). Type the following commands:

- **tar xzvf [zcsfullfilename.tgz]**, to unpack the file.
- **cd [zcsfullfilename]** to change to the correct directory.
- **./install.sh** to begin the installation.

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

```
[root@mailhost tmp]# tar xzvf zcs.tgz
zcs-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20100916012803/
zcs-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20100916012803/packages/
zcs-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20100916012803/packages/zimbra-
apache_7.0.0_GA_2834.UBUNTU10_64_amd64.deb
.
.
zcs-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20101015012627/install.sh
zcs-NETWORK-7.0.0_GA_2834.UBUNTU10_64.20101015012627/README.txt
.
.
[root@mailhost tmp]# cd zcs-NETWORK-
7.0.0_GA_2834.UBUNTU10_64.20101015012627
[root@mailhost tmp/zcs-NETWORK-
7.0.0_GA_2834.UBUNTU10_64.20101015012627# ./install.sh
.
.
Operations logged to /tmp/install.log.3833
Checking for existing installation...
  zimbra-ldap...NOT FOUND
  zimbra-logger...NOT FOUND
  zimbra-mta...NOT FOUND
  zimbra-snmp...NOT FOUND
  zimbra-store...NOT FOUND
  zimbra-apache...NOT FOUND
  zimbra-spell...NOT FOUND
  zimbra-core...NOT FOUND
```

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

2. The installation process checks to see if Sendmail, Postfix, and MySQL software are running. If any of these applications are running, you are asked to disable them. Disabling MySQL is optional but highly recommended. Sendmail and Postfix must be disabled for the Zimbra Collaboration Suite to start correctly.
3. Next, the installer checks to see that the prerequisite software is installed. If the prerequisite software packages are not installed, the installation process stops. You must fix the problem and start the installation over. See Other Dependencies in [System Requirements for Zimbra Collaboration Suite 7.0](#).

```
Checking for prerequisites...
FOUND: NPTL
FOUND: sudo-1.7.2pl-1ubuntu5.2
FOUND: libidn11-1.15-2
FOUND: libpcre3-7.8-3build1
FOUND: libgmp3c2-2:4.3.2+dfsg-1ubuntu1
FOUND: libexpat1-2.0.1-7ubuntu1
FOUND: libstdc++6-4.4.3-4ubuntu5
FOUND: libperl5.10-5.10.1-8ubuntu2
Checking for suggested prerequisites...
FOUND: perl-5.10.1
FOUND: sysstat
Prerequisite check complete.
```

Select the services to be installed on this server. To install Zimbra Collaboration Suite on a single server, enter **Y** for the ldap, logger, mta, snmp, store, and spell packages. The installer verifies that there is enough room to install ZCS. If there is not, the installation stops.

```
Checking for installable packages

Found zimbra-core
Found zimbra-ldap
Found zimbra-logger
Found zimbra-mta
Found zimbra-snmp
Found zimbra-store
Found zimbra-apache
Found zimbra-spell

Select the packages to install

Install zimbra-ldap [Y]
Install zimbra-logger [Y]
Install zimbra-mta [Y]
Install zimbra-snmp [Y]
Install zimbra-store [Y]
Install zimbra-apache [Y]
Install zimbra-spell [Y]
Checking required space for zimbra-core
checking space for zimbra-store

Installing:
  zimbra-core
  zimbra-ldap
  zimbra-logger
  zimbra-mta
  zimbra-snmp
  zimbra-store
  zimbra-apache
  zimbra-spell
```

4. 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.

```
The system will be modified. Continue? [N] y
Installing packages
  zimbra-core.....zimbra-
core_7.0.0_GA_2729.UBUNTU10_64_amd64.deb...done
  zimbra-ldap.....zimbra-
ldap_7.0.0_GA_2729.UBUNTU10_64_amd64.deb...done
  zimbra-logger.....zimbra-
logger_7.0.0_GA_2729.UBUNTU10_64_amd64.deb...done
  zimbra-mta.....zimbra-
mta_7.0.0_GA_2729.UBUNTU10_64_amd64.deb...done
  zimbra-snmp.....zimbra-
snmp_7.0.0_GA_2729.UBUNTU10_64_amd64.deb...done
.
.
.
Operations logged to /tmp/zmsetup.09162010-120613.log
Installing LDAP configuration database...done.
Setting defaults...

DNS ERROR - resolving MX records for mailhost.example.com
It is suggested that the domain name have an MX record configured in
DNS
Change domain name? [Yes] n
done.
Checking for port conflicts
```

5. At this point, the **Main menu** displays showing the default entries for the Zimbra component you are installing. To expand the menu to see the configuration values, type **X** and press **Enter**. The Main menu expands to display configuration details for the package being installed. Values that require further configuration are marked with asterisks (****) to their left.

To navigate the Main menu, select the menu item to change. You can modify any of the defaults. See “Main Menu Options,” on page 7, for a description of the Main menu.

For a quick installation, accepting all the defaults, you only need to do the following:

6. If your time zone is not Pacific time, enter **1** to select **Main menu 1, Common Configuration** and then enter **6** for **TimeZone**. Set the correct time zone.


```

Main menu
  1) Common Configuration:
      +Hostname: mailhost.example.com
      +Ldap master host: mailhost.example.com
      +Ldap port: 389
      +Ldap Admin password: set
      +Secure interprocess communications: yes
      +TimeZone: America/Los_Angeles
  2) zimbra-ldap: Enabled
      +Status Enabled
      +Create Domain: yes
      +Domain to create: mailhost.example.com
      +Ldap root password: set
      +Ldap replication password: set
      +Ldap postfix password: set
      +Ldap amavis password: set
      +Ldap nginx password: set
  3) zimbra-store: Enabled
      +Status Enabled
      +Create Admin User: yes
      +Admin user to create: admin@mailhost.example.com
  ***** +Admin Password UNSET
      +Anti-virus quarantine user: virus-
quarantine.zodi72xmm6@mailhost.example.com
      +Enable automated spam training: yes
      +Spam training user spam.vviwu_izoj@mailhost.example.com
      +Non-spam(Ham) training user: ham.unsbogyzer@mailhost.example.com
      +SMTP host: mailhost.example.com
      +Web server HTTP port: 80
      +Web server HTTPS port: 443
      +Web server mode: http
      +IMAP server port: 143
      +IMAP server SSL port: 993
      +POP server port: 110
      +POP server SSL port: 995
      +Use spell check server: yes
      +Spell server URL: http://mailhost.example.com
:7780/aspell.php
      +Configure for use with mail proxy: FALSE
      +Configure for use with web proxy: FALSE
      +Enable version update checks: TRUE
      +Enable version update notifications: TRUE
      +Version update notification email: admin@mailhost.example.com
      +Version update source email: admin@mailhost.example.com

  4) zimbra-mta: Enabled
  5) zimbra-snmp: Enabled
  6) zimbra-logger: Enabled
  7) zimbra-spell: Enabled
  8) zimbra-convertd: Enabled
  9) Default Class of Service Configuration:
  10) Enable default backup schedule: yes
  c) Collapse menu
  r) Start servers after configuration yes
  s) Save config to file
  q) Quit

```

7. Type **r** to return to the Main menu.
8. Enter **3** to select **zimbra-store** from the Main menu. The Store configuration menu displays.
9. Select the following from the store configuration menu:
 - Type **4** and type the admin password. The password must be six or more characters. Press **Enter**.
 - **Enable version update checks** and **Enable version update notifications** are set to **TRUE**. ZCS automatically checks for the latest ZCS software updates and notifies the account that is configured in **Version update notification email**. You can modify this later from the administration console.

```

Store configuration

  1) Status:                               Enabled
  2) Create Admin User:                     yes
  3) Admin user to create:                   admin@mailhost.example.com
** 4) Admin Password                       UNSET
  5) Anti-virus quarantine user:             virus-
quarantine.zodi72xmm6@mailhost.example.com
  6) Enable automated spam training:         yes
  7) Spam training user: spam.vviwu_izoj@mailhost.example.com
  8) Non-spam(Ham) training user: ham.unsbogyzer@mailhost.example.com
  9) SMTP host:                             mailhost.example.com
10) Web server HTTP port:                   80
11) Web server HTTPS port:                  443
12) Web server mode:                        http
13) IMAP server port:                       143
14) IMAP server SSL port:                   993
15) POP server port:                        110
16) POP server SSL port:                    995
17) Use spell check server:                 yes
18) Spell server URL:                       http://mailhost.example.com :7780/aspell.php
19) Configure for use with mail proxy:      FALSE
20) Configure for use with web proxy:       FALSE
21) Enable version update checks:           TRUE
22) Enable version update notifications:    TRUE

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

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

```

10. Type **r** to return to the Main menu.
11. If you want to change the default Class of Service settings for new features that are listed here, type **9** for **Default Class of Service Configuration**. Then type the number for the feature to be enabled or disabled. Changes you make here are reflected in the default COS configuration.

12. 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
Save configuration data to a file? [Yes] y
Save config in file: [/opt/zimbra/config.6585]
Saving config in /opt/zimbra/config.6585...done.
```

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

```
Save configuration data to a file? [Yes] y
Save config in file: [/opt/zimbra/config.6585]
Saving config in /opt/zimbra/config.6585...done.
```

14. 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.6585]
Saving config in /opt/zimbra/config.6585...done.
```

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 server can take several minutes. Components that are installed include spam training and documents (wiki) accounts, time zone preferences, backup schedules, as well as common zimlets.

```
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.10152010-084228.log
Setting local config values...done.
Setting up CA...done.
Deploying CA to /opt/zimbra/conf/ca ...done.
.
.
Installing webclient skins...
    hotrod...done.
    lavender...done.
    carbon...done.
    tree...done.
    smoke...done.
.
.
Finished installing webclient skins.
Setting zimbraFeatureIMEnabled=FALSE...done.
Setting zimbraFeatureTasksEnabled=TRUE...done.
.
.
Starting servers...done.
Installing common zimlets...
    com_zimbra_email...done.
    com_zimbra_url...done.
.
.
Finished installing common zimlets.
Installing network zimlets...
    com_zimbra_mobilesync...done.
    com_zimbra_hsm...done.
.
.
Finished installing network zimlets.
Restarting mailboxd...done.
Setting up zimbra crontab...done.

Moving /tmp/zmsetup.09162010-120613.log to /opt/zimbra/log
```

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

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

Verify Zimbra Server Operation

When **Configuration complete!** appears, the installation is finished and the server has been started.

To verify that the server is running:

1. Type `su - zimbra`.
2. Type `zmcontrol status`. The services status information is displayed. All services should be running.

```
[zimbra@example ~]$ zmcontrol status
Host example.com
      antispam           Running
      antivirus          Running
      converttd          Running
      ldap               Running
      logger             Running
      mailbox            Running
      mta                Running
      snmp               Running
      spell              Running
      stats              Running
[zimbra@example ~]$
```

Note: If services are not running, type `zmcontrol start`.

See the [Administration Guide](#), Appendix A: Command-Line Utilities for more `zmcontrol` commands.

The installation is complete and the servers are started. You can start adding accounts.

Final Set-Up

After the Zimbra servers are configured, the following functions must be configured:

- If 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.
- ZCS ships a default zimbra user with a disabled password. ZCS requires access to this account via ssh public key authentication. On most operating systems this combination is okay, but if you have modified pam rules to

disallow any ssh access to disabled accounts then you must define a password for the zimbra UNIX account. This will allow ssh key authentication for checking remote queues. See the Zimbra wiki article, Mail Queue Monitoring.

Set up the ssh keys. To populate the ssh keys, as Zimbra user (`su-zimbra`). Type `zmupdateauthkeys` and press **Enter**. The key is updated on `/opt/zimbra/.ssh/authorized_keys`.

Enabling Server Statistics Display. 1. In order for the server statistics to display on the administration console, the syslog configuration files must be modified. As root, type `/opt/zimbra/libexec/zmsyslogsetup`. This enables the server to display statistics.

2. You must enable **syslog** to log statistics from remote machines.
 - a. Edit the `/etc/sysconfig/syslog` file, add `-r` to the `SYSLOGD_OPTIONS` setting, `SYSLOGD_options="-r -m 0"`
 - b. Stop the syslog daemon. Type `/etc/init.d/syslog stop`
 - c. Start the syslog daemon. Type `/etc/init.d/syslog start`

Note: On *DEBIAN AND UBUNTU*, step 2 is as follows

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

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`

Note: 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`.

To 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 Bulk Provisioning Wizard.

Configuring One Account

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

1. From the administration console Navigation pane, click **Accounts**.

Note: Four accounts are listed: admin account, two spam training accounts, and a global Documents account. These accounts do not need any additional configuration.

2. Click **New**. The first page of the **New Account Wizard** opens.
3. Enter the account name to be used as the email address and the last name. This the only required information to create an account.
4. You can click **Finish** at this point, and the account is configured with the default COS and global features.

To configure aliases, forwarding addresses, and specific features for this account, proceed through the dialog before you click **Finish**.

When the accounts are provisioned, you can send and receive emails.

Configuring Many Accounts at Once

You can provision multiple accounts at once using the Account Migration tool from the administration console. The wizard guides you through the steps to import accounts from an external directory server, either Active Directory or an LDAP server. The wizard downloads account information from your directory and creates the accounts in ZCS.

Refer to the administration guide to learn more about provisioning accounts.

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 ZCS utilities to move user mail to ZCS 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, Documents page.

Alternatively, you can download the following applications from **<http://{example.com/downloads}/index.html>** (with “example” being your Zimbra server name).

- **ZCS Migration Wizard for Exchange.** Format is an .exe file. You can migrate users from Microsoft® Exchange server email accounts to Zimbra server accounts.
- **ZCS Migration Wizard for Lotus® Domino®.** Format is an .exe file. You can migrate users from Lotus Domino server email accounts to Zimbra server accounts.
- **Zimbra Collaboration Suite Import Wizard for Outlook®.** 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>.
- **Zimbra Collaboration Suite Import Wizard for Lotus® Domino.** Format is an .exe file. Users download the Import Wizard to their computers and run the executable file to import their Lotus Domino files to the Zimbra server.

Administrator's 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 admin console. If you didn't change the default during installation, the anti-virus notification is sent directly to the admin account.

Uninstalling Zimbra Collaboration Suite

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

1. `cd` to the original install directory for the `zcs` files.

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

Additional Information

To learn more about the Zimbra Collaboration Suite, read the Administrator's Guide and Help. The Zimbra guides and release notes in .pdf format can be found in the `opt/zimbra/docs` directory and is also available from the administration console Help button and from the Zimbra Website.

- **Administrator's Guide.** This guide describes product architecture, server functionality, administration tasks, configuration options, and backup and restore procedures. The guide is available in pdf format from the administrator's console, and in HTML format on the Zimbra Website.
- **Administrator Help.** The administrator Help provides detailed instructions about how to add and maintain your servers, domains, and user accounts from the admin console.

Support and Contact Information

Visit www.zimbra.com to join the community and to be a part of building the best open source messaging solution. We appreciate your feedback and suggestions.

- Contact sales@zimbra.com to purchase the Zimbra Collaboration Suite.
- 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 Forums](#), to participate and learn more about the Zimbra Collaboration Suite.
- Send an email to feedback@zimbra.com to let us know what you like about the product and what you would like to see in the product. Or, if you prefer, post your ideas to the Zimbra Forums.

If you encounter problems with this software, visit www.zimbra.com and submit a bug report. Make sure you provide enough detail so that the bug can be easily duplicated.

System Requirements for Zimbra Collaboration Suite 7.0

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

	Requirements
Servers	<p>Evaluation and Testing</p> <ul style="list-style-type: none">• Intel/AMD 32-bit or 64-bit CPU 1.5 GHz• 1 GB RAM• 5 GB free disk space for software and logs• Temp file space for installs and upgrades*• Additional disk space for mail storage <p>Production environments</p> <ul style="list-style-type: none">• Minimum - 32-bit OS with Intel/AMD 2.0 GHZ+ CPU Recommended - 64-bit OS• Minimum - 2 GB RAM Recommend minimum - 4 GB RAM• Temp file space for installs and upgrades*• 10 GB free disk space for software and logs (SATA or SCSI for performance, and RAID/Mirroring for redundancy)• Additional disk space for mail storage <p>*Temp files space- The zimbra-store requires 5GB for /opt/zimbra, plus additional space for mail storage. The other nodes require 100MB.</p> <p>General Requirements</p> <ul style="list-style-type: none">• Firewall Configuration should be set to “No firewall”, and the Security Enhanced Linux (SELinux) should be disabled• RAID-5 is not recommended for installations with more than 100 accounts.

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

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

**Administrator
Computers**

Note: Other configurations may work.

The following operating system/browser combinations are supported:

Windows 2000, XP, Vista, and Windows 7 with one of the following:

- Internet Explorer 7.0 or 8.0
- Firefox 3.0, 3.5 or 3.6
- Safari 4 or 5
- Google Chrome 2.1, 2.2, or 2.3

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

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

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

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

Note: We expect that the 7.0.x series of ZCS will be the last release to support Firefox 3.0. Based on this expectation, we suggest a 3.5 or newer version of Firefox be used.

<p>End User Computers using Zimbra Web Client</p> <p>Note: Other configurations may work.</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>For Zimbra Web Client - Advanced version:</p> <p>The following operating system/browser combinations for the advanced Zimbra Web Client are supported:</p> <p>Windows 2000, XP SP 3, Vista SP 2, or Windows 7 with one of the following:</p> <ul style="list-style-type: none"> • Internet Explorer 7 or 8 • Firefox 3.0, 3.5 or 3.6 • Safari 4 or 5 • Google Chrome 2.1, 2.2, or 2.3 <p>Mac OS X 10.4, 10.5, or 10.6 with one of the following:</p> <ul style="list-style-type: none"> • Firefox 3.0, 3.5 or 3.6 • Safari 4 or 5 • Google Chrome 2.1, 2.2, or 2.3 <p>Linux (Red Hat, Ubuntu, Debian, Fedora, or SUSE) with one of the following:</p> <ul style="list-style-type: none"> • Firefox 3.0, 3.5 or 3.6 • Google Chrome 2.1, 2.2, or 2.3 <p>Note: We expect that the 7.0.x series of ZCS will be the last release to support Firefox 3.0. Based on this expectation, we suggest a newer version of Firefox be used as listed above.</p>
--	---

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

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

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

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

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

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

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

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

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

End User Computers Using Other Clients	<p>Minimum</p> <ul style="list-style-type: none"> • Intel/AMD/Power PC CPU 750MHz • 256MB RAM <p>Recommended</p> <ul style="list-style-type: none"> • Intel/AMD/Power PC CPU 1.5GHz • 512MB RAM <p>Operating system POP/IMAP combinations</p> <ul style="list-style-type: none"> • Windows XP SP 3, Vista SP 2, Windows 7 with Outlook Express 6, Outlook 2003, (MAPI), Thunderbird • Fedora Core 4 or later with Thunderbird • Mac OS X 10.4 or later with Apple Mail <p>Accessibility and Screen Readers</p> <p>Zimbra recommends that customers requiring use of screen readers for accessibility leverage the use of the Standard Zimbra Web Client (HTML).</p> <p>Zimbra continues to invest in improving the accessibility of this interface.</p>
	<p>**Recommendation - If users are presently using IE 6, Zimbra strongly recommends that they upgrade to the latest version of Internet Explorer for optimal performance with ZWC.</p>
Monitor	<p>Display minimum resolution 1024 x 768</p>
Internet Connection Speed	<p>128 kbps or higher</p>

Copyright © 2011 Zimbra and VMware, Inc. All rights reserved.

ZCS 7.0 - February 2011

