
Zimbra™ Collaboration Suite Installation Quick Start

Network Edition or Open Source Edition 4.0

The Zimbra Collaboration Suite includes the Zimbra MTA, the Zimbra LDAP server, and the Zimbra mailbox server. During the installation process all components are installed and require no additional manual configuration.

This quick start guide assumes that all components will be installed on one server and 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.

This quick start guide includes the following sections:

- Installation Prerequisites
- Overview of Installation Process
- Basic Configuration
- Installing Zimbra Software
- Provisioning Accounts
- Installing Zimbra Software on a Mac Server
- Support and Contact Information

Important Notice About Quick Start 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 Tomcat, 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.

Note: A Zimbra license is required in order to create accounts on the Network Edition Zimbra Collaboration Suite server. You can install ZCS without a license but only one account, the administrator account, can be created. See “Configure the Zimbra License for ZCS Network Edition” on page 21.

The following ports are set as defaults when the Zimbra Collaboration Suite is installed.

Table 1 Zimbra Port Mapping

	Port
Postfix	25
HTTP	80
POP3	110
IMAP	143
LDAP	389
HTTPS	443
Tomcat IMAP SSL	993
Tomcat POP SSL	995
Tomcat 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.

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 [System Requirements for Zimbra Collaboration Suite 4.0](#)

Note: To find SSH client software, go to <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

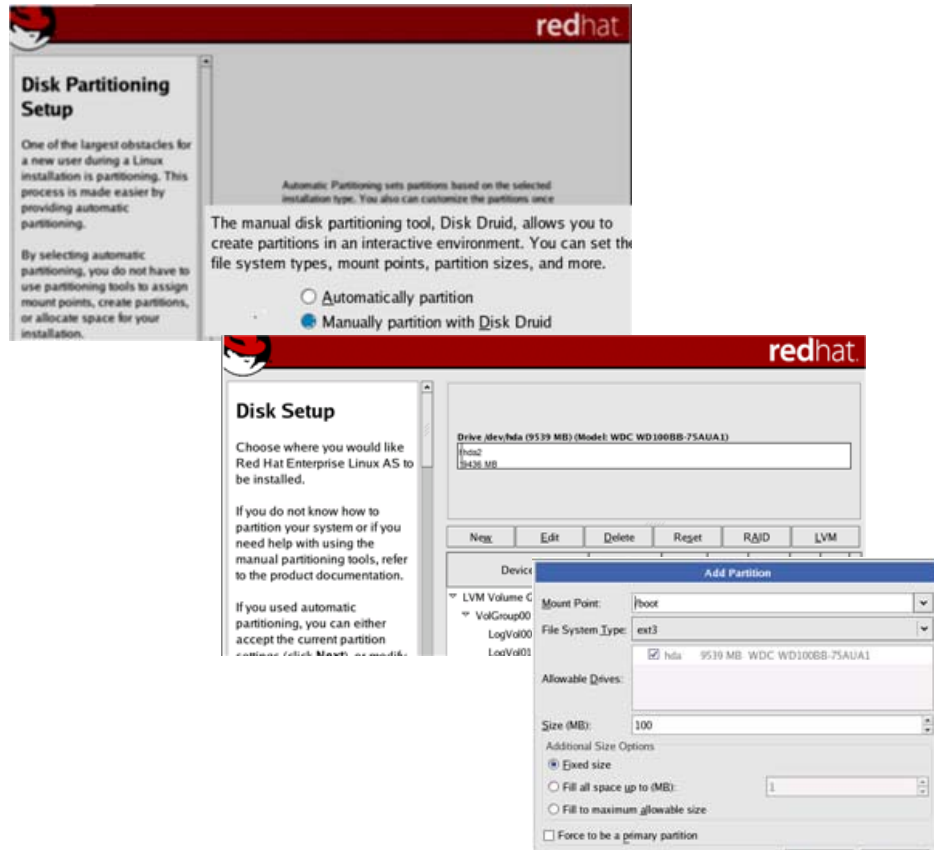
Configuration modifications for two of the most frequently used operating systems, Red Hat Enterprise Linux and Fedora, are described in this guide. The SUSE configuration would be similar to those described for the Red Hat Enterprise Linux. The MAC OS X requires no additional modifications.

Other operating systems may require similar modifications, use this information as a reference to gauge whether your operating system may need to be modified. Also, search the Zimbra forums.

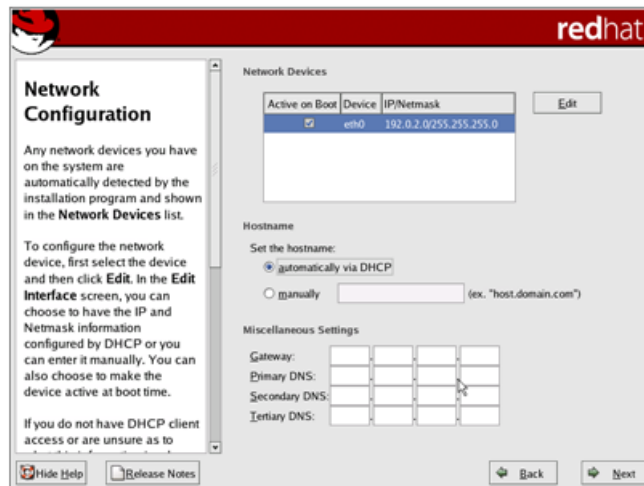
Installation Modifications for Red Hat Enterprise Linux

The Zimbra Collaboration Suite runs on the Red Hat Enterprise Linux, version 4 operating system. When you install the Red Hat software for the Zimbra Collaboration Suite, accept the default setup answers, except for the following steps. Refer to the Red Hat Enterprise Linux installation guide for detailed documentation about installing their software.

- **Disk Partitioning Setup.** Check **Manually partition with DiskDruid**. The disk partition should be set up as follows:
 - The **Mount Point/RAID Volume** size for the **/boot** partition should be 100 MB.
 - The **Swap** partition should be set to twice the size of the RAM on your machine.
 - The **Root** partition (**/**) should be set with the remaining disk space size.

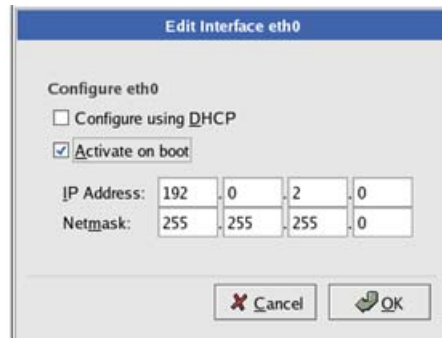


- **Network Configuration>Network Devices>Hostname** should be configured manually with the fully qualified hostname [*mailhost.example.com*] of the Zimbra server.



- Enter the **Gateway** and **Primary DNS** addresses.

- In the **Edit Interface** pop-up screen, check **Activate on Boot**. Enter the **IP Address** and **Netmask** of the device. This allows the interface to start when you boot.



- **Firewall Configuration** should be set to **No firewall**, and the **Security Enhanced Linux (SELinux)** should be disabled.

Important: You will need to disable Sendmail in order to run the Zimbra Collaboration Suite. You can disable the Sendmail service with these command, **chkconfig sendmail off, service sendmail stop.**

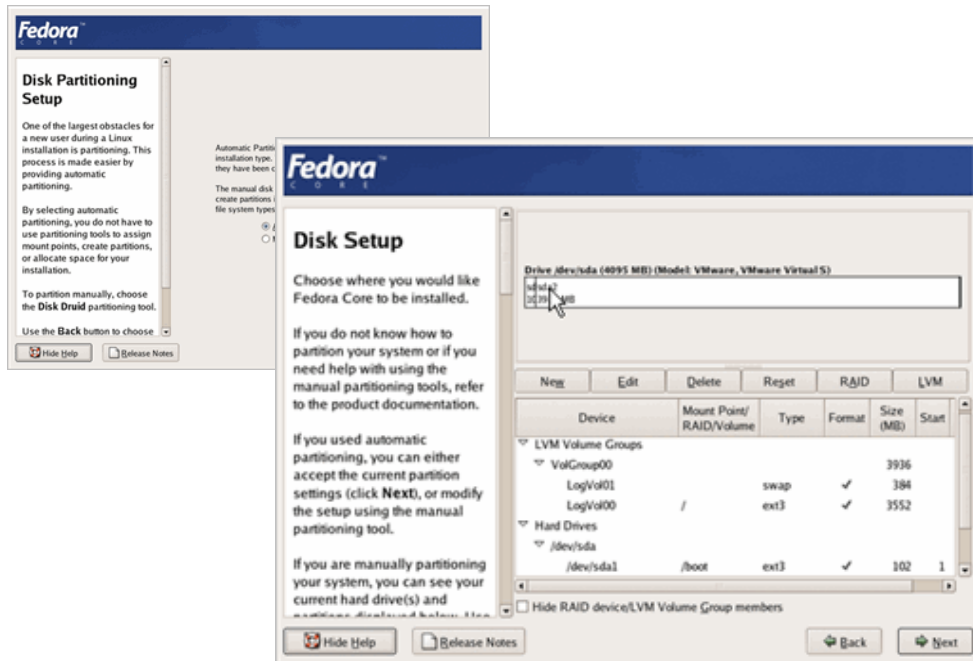
Important: Make sure that FQDN entry in **/etc/hosts** appears before the hostnames. If this is missing, the creation of the Zimbra certificate fails. The FQDN entry should look like this example. See **zmcreatecert** in the Administrator's Guide, CLI Commands appendix.

127.0.0.1	localhost.localdomain localhost
your.ip.address	FQDN yourhostname

Installation Modifications for Fedora

The Zimbra Collaboration Suite runs on the Fedora, Core 4 operating system. When you install the Fedora software for the Zimbra Collaboration Suite, accept the default setup answers, except for the following steps. Refer to the Fedora installation guide for detailed documentation about installing their software.

- **Disk Partitioning Setup.** Check **Manually partition with DiskDruid**. The disk partition should be set up as follows:
 - The **Mount Point/RAID Volume** size for the **/boot** partition should be 100 MB.
 - The **Swap** partition should be set to twice the size of the RAM on your machine.
 - The **Root** partition (**/**) should be set with the remaining disk space size.



- **Network Configuration>Network Devices>Hostname** should be configured manually with the fully qualified hostname name [*mailhost.example.com*] of the Zimbra server.



- Enter the **Gateway** and **Primary DNS** addresses.

- In the **Edit Interface** pop-up screen, check **Activate on Boot**. Enter the **IP Address** and **Netmask** of the device. This allows the interface to start when you boot.

Important: You will need to disable Sendmail in order to run the Zimbra Collaboration Suite. You can disable the Sendmail service with these command, **chkconfig sendmail off, service sendmail stop**.

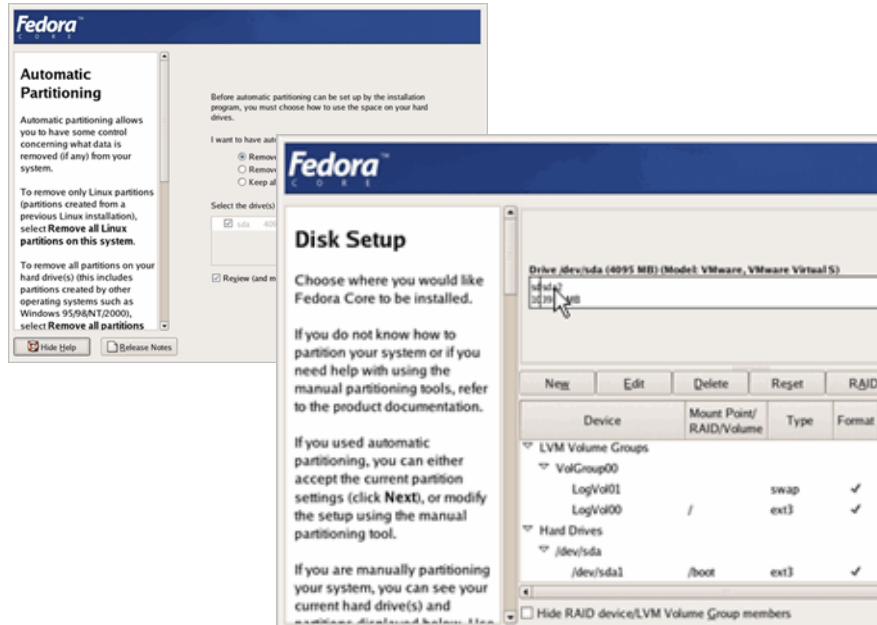
Important: Make sure that FQDN entry in **/etc/hosts** appears before the hostnames. If this is missing, the creation of the Zimbra certificate fails. The FQDN entry should look like this example. See **zmcreatecert** in the Administrator's Guide, CLI Commands appendix.

```
127.0.0.1          localhost.localdomain localhost
your.ip.address   FQDN yourhostname
```

Installation Modifications for Fedora

The Zimbra Collaboration Suite runs on the Fedora, Core 3 operating system. When you install the Fedora software for the Zimbra Collaboration Suite, accept the default setup answers, except for the following steps. Refer to the Fedora installation guide for detailed documentation about installing their software.

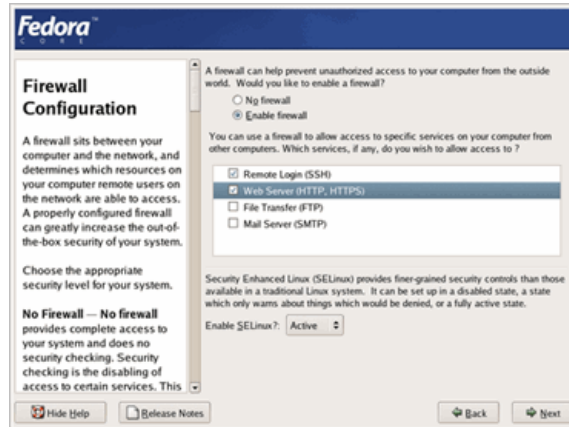
- **Disk Partitioning Setup.** Check **Manually partition with DiskDruid**. The disk partition should be set up as follows:
 - The **Mount Point/RAID Volume** size for the **/boot** partition should be 100 MB.
 - The **Swap** partition should be set to twice the size of the RAM on your machine.
 - The **Root** partition (**/**) should be set with the remaining disk space size.



- **Network Configuration>Network Devices>Hostname** should be configured manually with the hostname name [*mailhost.example.com*] of the Zimbra server.



- Enter the **Gateway** and **Primary DNS** addresses.
- In the **Edit Interface** pop-up screen, check **Activate on Boot**. Enter the **IP Address** and **Netmask** of the device. This allows the interface to start when you boot.
- **Firewall Configuration** should be set to **No firewall**, and the **Security Enhanced Linux (SELinux)** should be disabled.



Important: The following should also be considered before you install the Zimbra Collaboration Suite.

- You must disable Sendmail in order to run the Zimbra Collaboration Suite application. The Sendmail command to stop the service is `/etc/init.d/sendmail stop`, to disable, is `chkconfig sendmail off`. The Postfix command to stop the service is `/etc/init.d/postfix stop`, to disable, is `chkconfig postfix stop`.
- Make sure that FQDN entry in `/etc/hosts` appear before the hostnames. If this is missing, the creation of the Zimbra certificate fails. The FQDN entry should look like this example.

127.0.0.1	localhost.localdomain localhost
your.ip.address	FQDN yourhostname

Installation Modification for Mac Servers

No modifications are required to the MAC server operating system, but Java 1.5 must be set as the default Java.

To set Java 1.5 as the default:

- **su - root**
- **cd /System/Library/Frameworks/JavaVM.Framework/Versions**
- **rm CurrentJDK**
- **ln -s 1.5.0 CurrentJDK**

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 installed.

- **Zimbra Core** installs the libraries, utilities, and monitoring tools.
- **Zimbra LDAP** installs the OpenLDAP software, an open source LDAP directory services.
- **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 Store** installs the mailbox server, including Apache Tomcat, the servlet container for the Zimbra server.
- **Zimbra Spell** installs the Aspell open source spelling checker. When Zimbra spell is installed, Zimbra-Apache is also installed.
- **Zimbra SNMP** installs the SNMP package for monitoring. This package is optional.
- **Zimbra Logger** installs tools for syslog aggregation, reporting, and message tracing.

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, the only value you must define is the administrator's password. The password is used to log on to the Zimbra 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.

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

- **Zimbra Collaboration Suite Connector for Outlook®** (ZCS Network Edition only). Format is a .msi file. This is a MAPI service provider that is installed on users' computers.
- **Zimbra Collaboration Suite Migration Wizard for Exchange.** Format is .exe file. Users can be migrated from Microsoft® Exchange server email accounts to Zimbra server accounts.
- **Zimbra Collaboration Suite Import Wizard for Outlook.** Format is an .exe file. Users can import their Outlook .pst files to the Zimbra server.
- ZCS documents, including administrator's guide, installation guides, Migration Wizard guide, and release notes.

See the Administrator's Guide for information about the ZCS Connector for Outlook and the PST Import Wizard. See the Migration Wizard Guide for information about the Migration Wizard file.

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), and the logger tool (optional), on one server.

The menu driven installation displays the components and their existing default values. During the installation process you can modify the information.

The table below describes the menu options

Table 2 Main Menu Options

Main Menu	Description
1) Hostname	The host name configured in the Red Hat operating system installation.
2) LDAP master host	The LDAP host name. On a single server installation this name is the same as the hostname.
3) LDAP port	The default port is 389.
4) LDAP password	The root LDAP password for the host. This password is automatically generated.

Table 2 Main Menu Options

Main Menu	Description
5) zimbra-ldap	Configuration includes the following: <ul style="list-style-type: none">• Create Domain - Yes. You can create one domain during installation and 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.

Table 2 Main Menu Options

Main Menu	Description
6) zimbra-store	<p>Configuration includes the following.</p> <ul style="list-style-type: none"> • Create Admin User - The administrator account is created during installation. This account is the first account provisioned on the Zimbra server and allows you to log on to the administration console. • Admin user to create - The default is admin@[mailhost.example.com]. • 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. • Enable automated spam training - By default, the automated spam training filter is enabled and two mail accounts are created. <ol style="list-style-type: none"> 1. Spam Training User to receive mail notification about mail that was not marked as junk, but should be. 2. Non-spam (HAM) training user to receive mail notification about mail that was marked as junk, but should not have been. <p>These addresses are automatically configured to work with the spam training filter. The accounts created have a randomly selected name. To recognize what the account is used for you may want to change this name.</p> <p>These default port configurations are shown.</p> <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. Mixed mode uses HTTPS for logging in and HTTP for normal session traffic. All modes use SSL encryption for back-end administrative traffic. Note: selecting both will set it to mixed. • Enable POP/IMAP proxy, default No. For single server installations, this setting should be No. • IMAP server port: 143 • IMAP server SSL port: 993 • POP server port: 110 • POP server SSL port: 995 • Use spell checker server: yes (if installed) • Spell server URL: http://<example.com>:7780/aspell.php

Table 2 Main Menu Options

Main Menu	Description
7) zimbra-mta	<p>The following options can be modified.</p> <ul style="list-style-type: none"> • MTA Auth host. This is configured automatically if the MTA authentication server host is on the same server, but must be configured if the authentication server is not on the MTA. • 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. Note: If the virus notification address does not exist and your host name is the same as the domain name on the Zimbra server, the virus notifications queue in the Zimbra MTA server and cannot be delivered.
8) zimbra-snmp (optional)	<p>You can modify the following options</p> <ul style="list-style-type: none"> • Enable SNMP notifications. The default is No. If you enter yes, you must enter the SNMP Trap hostname. • SNMP Trap hostname • Enable SMTP notification - The default is No. • SMTP Source email address - If you enter yes for SMTP notification, you must enter the SMTP source email address and SMTP Destination email address - destination email address.
9) zimbra-logger	<p>When installed, it is automatically enabled. This information is used to generate the statistics graphs and is used for message tracing.</p>
10) zimbra-spell (optional)	<p>When installed, it is automatically enabled.</p>
11) Enable default backup schedule	<p>For the Network Edition only, sets the schedule for Backup session to run as a full backup every Sunday at 1 a.m. and as incremental on the other days at 1 a.m.</p>
r) Start servers after configuration	<p>When the installation and configuration is complete, if this is set to Yes, the Zimbra server is automatically started.</p>
s) Save config to file	<p>At any time during the installation, you can save the configuration to file.</p>
q) Quit	<p>Quit can be used at any time to quit the installation.</p>

Installing Zimbra Software

For servers other than Mac servers, open an SSH session to the Zimbra server and follow the steps below.

For Macs, see “Installing Zimbra Software on a Mac Server” on page 20.

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 [zcs.tgz]**, to unpack the file
- **cd zcs**, 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.

The screen shots are examples of the Zimbra installation script

```
[root@mailhost. tmp]# tar xzvf zcs.tgz
zcs/
zcs/util/
.
.
.
zcs/packages/
zcs/packages/zimbra-apache-3.0.0_M2_595.RHEL4-20051104060309.i386.rpm
zcs/packages/zimbra-core-3.0.0_M2_595.RHEL4-20051104060309.i386.rpm
zcs/packages/zimbra-mta-3.0.0_M2_595.RHEL4-20051104060309.i386.rpm
zcs/packages/zimbra-spell-3.0.0_M2_595.RHEL4-20051104060309.i386.rpm
zcs/packages/zimbra-store-3.0.0_M2_595.RHEL4-20051104060309.i386.rpm
zcs/packages/zimbra-logger-3.0.0_M2_595.RHEL4-20051104060309.i386.rpm
zcs/packages/zimbra-ldap-3.0.0_M2_595.RHEL4-20051104060309.i386.rpm
zcs/packages/zimbra-snmp-3.0.0_M2_595.RHEL4-20051104060309.i386.rpm
zcs/README.txt
zcs/readme_binary.txt
zcs/docs/
.
.
.
[root@mailhost tmp]# cd zcs
[root@mailhost zcs]# ./install.sh

Operations logged to /tmp/install.log.23354
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 1
```

2. The installation process checks to see if Sendmail, Postfix, and MySQL software are running. If any of these applications is 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. The Zimbra software agreement is displayed and includes the link to the license terms for the Zimbra Collaboration Suite. Please read the agreement and, to continue, press **Enter**.

```
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
ZIMBRA, INC. ("ZIMBRA") WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU
FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR
INSTALLING THE SOFTWARE, OR USING THE PRODUCT, YOU ARE CONSENTING TO
BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS
OF THIS AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.
```

```
License Terms for the Zimbra Collaboration Suite:
  http://www.zimbra.com/license/index.html
```

```
Press Return to continue
```

```
Checking for prerequisites...
  NPTL...found
  sudo -1.6.7p5-30.1.3...found
  libidn...FOUND libidn-0.5.6-1
  curl...FOUND curl-7.12.1-5.rhel4
  fetchmail...FOUND fetchmail-6.2.5-6.el4.2
  gmp...FOUND gmp-4.1.4-3
  /user/lib/libstdc++- FOUND compat-libstdc++-33-3.2.3-47.3
Checking for installable packages
```

4. Next, the installer checks to see that the prerequisite software is installed. If NPTL, sudo, libidn, cURL, fetchmail, GMP or compat-libstdc++- are not installed, the install process quits. You must fix the problem and start the installation over.
5. Select the services to be installed on this server. To install Zimbra Collaboration Suite on a single server, enter **Y** for each package.

6. Type **Y** and press **Enter** to modify the system. The selected packages are installed on the server.

```
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-spell [Y]

Installing:
  zimbra-core
  zimbra-ldap
  zimbra-mta
  zimbra-snmp
  zimbra-store
  zimbra-apache
  zimbra-spell
  zimbra-logger
This system will be modified. Continue [N]Y
Configuration section
```

Note: Before the configuration starts, 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 a MX record configured in DNS.

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

```
Main menu

1) Hostname:                               mailhost.example.com
2) Ldap master host                         mailhost.example.com
3) Ldap port:                               389
4) Ldap password:                           set
5) zimbra-ldap:                             Enabled
   +Create Domain:                           yes
   +Domain to create:                         mailhost.example.com
6) zimbra-store:                             Enabled
   +Create Admin User:                         yes
   +Admin user to create:                      admin@mailhost.example.com
***** +Admin Password                       UNSET
   +Enable automated spam training:           yes
   +Spam training user:                       fdi0j@mailhost.example.com
   +Non-spam(Ham) training user:              s3nnl@mailhost.example.com
   +SMTP host:                                mailhost.example.com
   +Web server HTTP port:                     80
   +Web server HTTPS port:                   443
   +Web server mode:                          http
   +Enable POP/IMAP proxy:                    no
   +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
7) zimbra-mta:                               Enabled
8) zimbra-snmp:                              Enabled
9) zimbra-logger:                            Enabled
10) zimbra-spell:                             Enabled
11) Enable default backup schedule:           yes
r) Start servers after configuration           yes
s) Save config to file
x) Expand menu
q) Quit

Address unconfigured (**) items (? - help) 6
```

To navigate the Main menu, select the menu item to change. You can modify any of the defaults. See [Table 2, Main Menu Options](#), for a description of the Main menu.

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

8. Enter **6** to select **Main menu 6, zimbra-store**.

```

Store configuration

  1) Status:                               Enabled
  2) Create Admin User:                    yes
  3) Admin user to create:                 admin@mailhost.example.com
** 4) Admin Password                        UNSET
  5)+Enable automated spam training:       yes
  6)+Spam training user:                   fdi0j@mailhost.example.com
  7)+Non-spam (Ham)training user:         s3nnl@mailhost.example.com
  8)+SMTP host:                            mailhost.example.com
  9) Web server HTTP port:                 80
 10) Web server HTTPS port:                443
 11) Web server mode:                      http
 12) Enable POP/IMAP proxy:                no
 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

Select, or 'r' for previous menu [r] 6

```

9. Select **4** and type the admin password. The password must be six or more characters. Press **Enter**.

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

11. If no other defaults need to be changed, type **a** to apply the configuration changes. Press **Enter**.

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

13. The next request is 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**.

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

The server is modified. Installing all the components and configuring the server can take a few minutes.

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

The installation is complete and the servers are started.

[Now log on to the administration console and install your Zimbra license. See "Configure the Zimbra License for ZCS Network Edition" on page 21](#)

Installing Zimbra Software on a Mac Server

1. Click on the dmg file to open the file and then click **ZCS.mpkg** to open the Zimbra install package. The Apple installer opens and verifies that the server is ready to install the Zimbra Collaboration Suite. Click **Continue**.
2. Welcome screen appears, click **Continue**.
3. The Zimbra Software License Agreement is displayed. Read the agreement and click **Continue**. A popup screen appears asking that to continue the install you must accept the terms of the license agreement. Click **Agree**.
4. Select the destination volume to install the software. Click **Continue**.
5. The **Easy Install ...** dialog displays. Now you select which services to be installed on this server. To install all service packages on a single server, click **Install**.

To select which services to install, click **Customize**. Deselect those packages you do not want installed. See "Overview of Installation Process" on page 10 for information about the packages. Click **Install** to proceed.

A progress bar shows the Zimbra packages being installed. When **The software was successfully installed** dialog displays, click **Close**.
6. Open the Apple Terminal and log on as **root**. Type **sudo /bin/bash**. Enter your root password, if asked.
7. Type **cd /opt/zimbra/libexec**
8. Type **ls** to see the packages in the directory.
9. Type **./zmsetup.pl**. This starts the ZCS configuration. A temporary log file is created and the server port configurations are checked for conflicts. 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.
10. If no conflicts are found, the Main menu displays the default entries for the Zimbra component you are installing. To expand the menu to see the configuration values type **X** and press **Enter**. The main menu expands to display configuration details for the package being installed. Values that require further configuration are marked with asterisks (*).
11. Go to [Step 6](#) on page -16 to continue the installation steps.

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.

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

See the CLI Command appendix in the Administration Guide for more `zmcontrol` commands.

Configure the Zimbra License for ZCS Network Edition

A Zimbra license is required in order to create accounts in the Network Edition Zimbra Collaboration Suite servers. You can install ZCS without a license but only one account, the administrator account, can be created.

A trial license and a regular license are available:

- **Trial.** You can obtain the trial license from the Zimbra license portal for free. The trial license allows you to create up to 50 users. It expires in 60 days.
- **Regular.** You must purchase the Zimbra Regular license. This license is valid for a specific Zimbra Collaboration Suite system and is encrypted with the number of Zimbra accounts (seats) you have purchased, the effective date, and expiration date of the regular license.

Go to Zimbra's website to obtain a trial license from the Network Downloads area. Also refer to the 4.0 Network Edition Release Notes for the latest information. Contact Zimbra sales to purchase a regular license, email sales@zimbra.com or call 1-650-212-7767, extension 100.

The regular license can only be installed on the ZCS system for which it is purchased. Only one Zimbra license is required for your Zimbra Collaboration Suite environment. This license is installed on the Zimbra LDAP server.

When you purchase, renew, or change the Zimbra license, you must update the Zimbra server with the new license information. Use the **Update License Wizard** from the administration console's Global Settings to upload and install a new license and to update an existing license, or you can install the license using the `zmlicense` CLI commands. See the Administrator's Guide Appendix A, CLI Commands, `zmlicense` to use the CLI command.

Current license information, including the number of accounts purchased, the number of accounts used, and the expiration date, can be viewed from Global Settings, License tab in the administration console.

Installing your Zimbra license after ZCS install is complete

To complete the ZCS installation and create accounts, you must upload and install the license file.

1. When you receive the license, save the license on the computer you use to access the Administration Console.

2. Log on to the administration console, go to **Global Settings>License** tab and on the toolbar, click **Update License**. The License Installation Wizard opens.
3. Use **Browse** to select the ZCS license file you saved. Click **Next**. The license file is uploaded to Zimbra LDAP server.
4. Click **Install** to install the license file.

After the license file is installed, the current license information on the License page is updated to reflect the new information. You can now add new accounts.

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/zimbraAdmin`

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 certificate authority (CA) alert may be displayed. Click **Accept this certificate permanently** to accept the certificate and be able connect to the Zimbra administration console. Then click **OK**.

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

To provision accounts:

1. From the admin 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**, page 1 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 will be configured with the default COS and global features.

If you want 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.

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 alias 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 that address, the message is forwarded to the admin mailbox.
- **Root.** This address is where notification messages from the operating system are sent.

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 you run the install script `-u` and then 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. Delete the `zcs` directory, type `rm -rf zcs`.
5. Delete the `zcs.tgz` file.

Additional Information

To learn more about the Zimbra Collaboration Suite, read the Administrator Reference 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.

- **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.
- **Administrator Help.** The administrator Help provides detailed instructions about how to add and maintain your servers, domains, and user accounts from the admin console.

- **Migration Wizard Guide.** This guide describes how to migrate Microsoft® Exchange clients to the Zimbra Collaboration Suite.

Support and Contact Information

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

- Contact sales@zimbra.com to purchase Zimbra Collaboration Suite.
- Network Edition customers can contact support at support@zimbra.com.
- Explore the Zimbra Forums for answers to installation or configurations problems.
- Join the [Zimbra Community Forum](#), to participate and learn more about the Zimbra Collaboration Suite.
- Send an email to feedback@zimbra.com to let us know what you like about the product and what you would like to see in the product. Or, if you prefer, post your ideas to the Zimbra Forum.

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

Zimbra Inc. Copyright Zimbra, Inc. 2006. All rights reserved. The Zimbra logo and logo type are trademarks of Zimbra, Inc.

All other marks are the property of their respective owners.

092006

System Requirements for Zimbra Collaboration Suite 4.0

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

Requirements	
Servers	<i>Evaluation and Testing</i> <ul style="list-style-type: none">• Intel/AMD 32-bit CPU 1.5 GHz• 1 GB RAM• 5 GB free disk space for software and logs• Additional disk space for mail storage <i>Production environments</i> <ul style="list-style-type: none">• Intel/AMD CPU 32-bit 2.0 GHZ+• Minimum - 2 GB RAM Recommend - 4 GB• 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>Note: RAID-5 is not recommended for installations with more than 100 accounts.</p>
Mac Server	<i>Evaluation and Testing</i> <ul style="list-style-type: none">• PPC Mac (G4 or better), Intel Core Solo, or Intel Core Duo*• 1 GB RAM• 5 GB free disk space for software and logs• Additional disk space for mail storage

<p>Mac Server (continued)</p>	<p><i>Production environments</i></p> <ul style="list-style-type: none"> • PPC Mac (G5 or better), Intel Core Solo, or Intel Core Duo* • Minimum - 2 GB RAM Recommend - 4 GB • 10 GB free disk space for software and logs • Additional disk space for mail storage <p>*There are known issues using ZCS on Macs with the Intel Core Duo. See the Release Note.</p>
<p>Operating System Network Edition</p>	<ul style="list-style-type: none"> • Red Hat® Enterprise Linux®, AS/ES version 4. (32-bit, 64-bit) For clustering, version 4, update 3 is required. The operating system must be configured as described in this guide. • Mac OS® X 10.4.7 <p>Note: Max OS X server installs, the following features are not included: attachment indexing/search, view attachments as HTML, clustering.</p> <ul style="list-style-type: none"> • SUSE ES 9 (32-bit) <p>Note: SUSE server installs, the following features are not included: clustering</p>
<p>Operating System Open Source Edition</p>	<p>In addition to supporting the operating systems listed above for the Network Edition, other OS versions are available for the Open Source Edition. Check the Zimbra Open Source Downloads page on www.zimbra.com.</p>

<p>Other Dependencies</p>	<p>For Red Hat Enterprise, Fedora Core and SuSE operating systems, the server must also have the following installed:</p> <ul style="list-style-type: none"> • NPTL. Native POSIX Thread Library • Sudo. Superuser, required to delegate admins. • libidn. For internationalizing domain names in applications (IDNA) • cURL. A command line tool for transferring files with URL syntax • fetchmail. A remote-mail retrieval and forwarding utility used for on-demand TCIP/IP links. • GMP. GNU Multiple-Precision Library. • compat-libstdc++-33. Compatibility Standard C++ libraries. NOTE: The 32-bit version of the compat-libstdc rpm package is required for both 32-bit or 64-bit servers. • For Red Hat Enterprise only: compat-libstdc++-296
	<p>For Mac servers, Java 1.5 must be installed as the default Java.</p>
<p>Miscellaneous</p>	<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
<p>Administrator Computers *These OS configurations have been tested and are known to work. Other configurations may work.</p>	<ul style="list-style-type: none"> • Windows XP with either Internet Explorer 6.0 SP 2 or Firefox 1.5 • Macintosh OS X 10.4 with Firefox 1.5

End User Computers using Zimbra Web Client *These OS configurations have been tested and are known to work. Other configurations may work.	Minimum <ul style="list-style-type: none">• Intel/AMD/Power PC CPU 750MHz• 256MB RAM Recommended <ul style="list-style-type: none">• Intel/AMD/Power PC CPU 1.5GHz• 512MB RAM Operating system/ browser combinations <ul style="list-style-type: none">• Windows XP with either Internet Explorer 6.0 SP 2 or Firefox 1.5• Fedora Core 4 with Firefox 1.5• Mac OS X 10.4 with Firefox 1.5 or Safari 2.0.4 (Beta)
End User Computers Using Other Clients *These OS configurations have been tested and are known to work. Other configurations may work.	Minimum <ul style="list-style-type: none">• Intel/AMD/Power PC CPU 750MHz• 256MB RAM Recommended <ul style="list-style-type: none">• Intel/AMD/Power PC CPU 1.5GHz• 512MB RAM Operating system POP/IMAP combinations <ul style="list-style-type: none">• Windows XP with either Outlook Express 6 , Outlook 2003 (MAPI), or Thunderbird 1.0.7• Fedora Core 4 with Thunderbird 1.0.7• Mac OS X 10.4 with Apple Mail
Monitor	Display minimum resolution 1024 x 768
Internet Connection Speed	128 kbps or higher

Import Wizard Requirements

Contents of a .pst file from accounts using Microsoft® Outlook® 2003 can be imported to accounts on the Zimbra server.

Rev 9/20/06

Cluster Install for Single-Node Configuration

For Red Hat Cluster Suite Integration

Clustering is available for the Network Edition only

Zimbra Collaboration Suite (ZCS) can be integrated with Red Hat® Enterprise Linux® Cluster Suite version 4, update 3 to provide high availability.

In a single-node cluster implementation, all Zimbra servers are part of a cluster under the control of the Red Hat Cluster Manager.

Note: Red Hat Cluster Suite consists of Red Hat Cluster Manager and Linux Virtual Server Cluster. For ZCS, only Red Hat Cluster Manager is used. In this guide, Red Hat Cluster Suite refers only to Cluster Manager.

This chapter describes configuring one active node and one standby node in a cluster environment. In the example commands in this guide, both the service name and the domain name are **mail.example.com**.

Pre-configuration Requirements

Both servers must meet the requirements described in the Zimbra Collaboration Suite Quick Start Guide, in addition to the requirements described here.

Go to the Red Hat Cluster Suite website, <https://www.redhat.com/software/rha/cluster> to view specific system requirements for cluster configurations using Red Hat Cluster Suite. If you are not familiar with the Red Hat Cluster Suite, read the documentation to understand how each of the components works to provide high availability.

Hardware for the Cluster Environment

For Red Hat Cluster Suite integration, the following hardware is required.

- SAN (shared disk storage device) to store the data for each of the Zimbra servers. The size of the shared storage device depends on your expected site capacity.
- Network power control switch to connect cluster nodes. The power control switch is used as the fence device for I/O fencing during a failover. Use either a APC or a WTI network power switch.

Configure the network power control switch according to the manufacturer's requirements.

Software Requirements For Clustering

- The Red Hat Enterprise Linux 4, Update 3 operating system installed on each server node configured with the same netmask and broadcast address.
- To use the Red Hat Cluster Configuration Tool GUI, install X Window and a desktop environment such as GNOME or KDE.
- Red Hat Cluster Suite, Update 3 on each server node.

Preparing the SAN

Note: You can place all service data on a single volume or choose to place the service data in ten volumes. A more customized volume configuration is possible, but the configurator script only supports single- or ten-volume volume sets. This is a limitation of the configurator script, not of Zimbra Collaboration Suite or of Red Hat Cluster Suite.

Configure the SAN device and create the partitions for the volumes. Refer to the Red Hat Cluster Suite documentation for configuration requirements.

- If you select to configure the SAN in one volume, all service data goes under a single SAN volume.
- If you select to partition the SAN into 10 volumes, the SAN device is partitioned to provide the following volumes for each Zimbra server in the cluster.

- | | |
|-------------------------|---|
| • conf | Volume for the service-specific configuration files |
| • log | Volume for the local logs for Zimbra server |
| • redolog | Volume for the redo logs for the Zimbra server |
| • db/data | Volume for the MySQL data files for the data store |
| • store | Volume for the message files |
| • index | Volume for the search index files |
| • backup | Volume for the backup files |
| • logger/db/data | Volume for the MySQL data files for logger service's MySQL instance |
| • openldap-data | Volume for OpenLDAP data |
| • postfix/spool | Volume for Postfixspool |

Installing the Zimbra Cluster Software

The Zimbra Cluster software consists of **install.pl**, **postinstall.pl**, and **configure-cluster.pl** scripts to automate the cluster configuration process and files that are used during the Zimbra cluster service operation.

Installing and configuring a single server for a cluster environment requires that you configure both servers in a specific sequence.

Flow of Installation:

1. On the Active node
 - Run cluster install.pl to install the necessary files, define users and groups, and create the mount points for the clustered service.
 - Install Zimbra Collaboration Suite. All packages are installed
2. On the Standby node
 - Run cluster install.pl to install the necessary files and define users and groups
 - Install Zimbra Collaboration Suite. All packages are installed
 - Set up syslog and MTA auth
3. On the Active node
 - Set up syslog and MTA auth
4. On the Standby node
 - Run the cluster postinstall.pl program
5. On the Active node
 - Mount the SAN volume(s)
 - Run the cluster postinstall.pl program
 - Run the cluster configurator script, configure-cluster.pl, to prepare the Red Hat Cluster Suite
 - Copy the cluster config. file to the standby node
 - Start Red Hat Cluster Suite daemons
6. On the standby node, start Red Hat Cluster Suite daemons

Installing and Configuring Single-Node Cluster Services

Column one displays the steps performed on the **Active Host**, column two, the steps performed on the **Standby**. The arrow identifies when you must continue the configuration on the other host.

IMPORTANT: These steps must be followed precisely because what you do on one node requires the other node to be in a specific state in order to be correctly configured.

Active

1. Bring up the service IP address on the active node.

```
[root@node1 ~]# ip addr add  
xx.xx.xxx.xx dev eth0
```

2. Run the cluster install.pl:
 - **tar xzvf zcs-cluster.tgz**
to unpack the file
 - **cd zcs-cluster**
to change to the correct directory
 - **./install.pl**
to begin the installationThe necessary files are installed.

Each Zimbra cluster node requires Zimbra and Postfix users and groups. The same user and group IDs must be used on both nodes.

- a. Type the zimbra group ID (GID) to be used. The default is 500.
 - b. Type the postfix group ID. The default is 501.
 - c. Type the postdrop group ID. The default is 502.
 - d. Type the zimbra user ID (UID) to be used. The default is 500.
 - e. Type the postfix user ID. The default is 501.
- The root directory for the mount points is created.
- f. Mount point(s) are created for the cluster service. Type the service name when prompted.
 - g. Type **Done**, when finished.

Standby

Active

3. Install the ZCS software.
All packages should be installed.
SNMP is optional. See the Quick Start Installation Guide for detailed installation instruction.

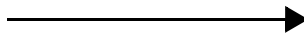
During the installation make the following changes

When the DNS error to resolve MX displays, enter yes to change the domain name. Modify the domain name to the cluster service hostname (not the active node hostname).

On the **Main Menu** make the following changes

- **Host name and LDAP master host name** must be changed from the active node hostname to the cluster service hostname.
- Note the LDAP password. You will need it later.
- Change the admin password.

When the ZCS installation is complete, there should be no reference to the active node hostname.

**Standby**

4. On the Standby host run, run the cluster install.pl:
 - **tar xzvf zcs-cluster.tgz** to unpack the file
 - **cd zcs-cluster** to change to the correct directory
 - **./install.pl** to begin the installationThe necessary files are installed.

Active

Standby

Each Zimbra cluster node requires Zimbra and Postfix users and groups. The same user and group IDs must be used on both nodes.

- a. Type the zimbra group ID (GID) to be used. The default is 500.
- b. Type the postfix group ID. The default is 501.
- c. Type the postdrop group ID. The default is 502.
- d. Type the zimbra user ID (UID) to be used. The default is 500.
- e. Type the postfix user ID. The default is 501.

The root directory for the mount points is created.

- f. Mount point(s) are created for the cluster. Type the service names when prompted. These are the same service names as on the active host.
- g. Type **Done**, when finished.

When you install ZCS on the standby node, you must configure the node as described below.

5. Install the ZCS software. Install the same Zimbra packages as installed on the active host. During the installation make the following changes
 - When the DNS error to resolve MX displays, enter yes to change the domain name. Modify the domain name to the cluster service name (not the server node name).
 - The DNS error appears again. This time when the installer asks "Re-Enter domain name?", type **No**.

Active**Standby**

Make these changes to the following Main Menu sections.

- **LDAP master host name** must be changed to point to the LDAP server running on the active node (mail.example.com). **Note:** this name is the service name, not the active node name.
- Change the **LDAP password** to the password set on the active node.
- **zimbra-ldap.**
Disable LDAP on the standby node.
- **zimbra-store - Admin user to create:**
Type No. An admin account should not be created on the standby node as it is already created on the active node.
- **zimbra-store - SMTP host:** If SMTP is configured, change the SMTP host to the cluster service host. (mail.example.com)
- **zimbra-mta - MTA Auth host:**
Change the MTA's auth host name to the cluster service host (mail.example.com)
- **zimbra-logger**
Disable logger on the standby. It is enabled on the active node.

Complete the ZCS installation on the standby node.

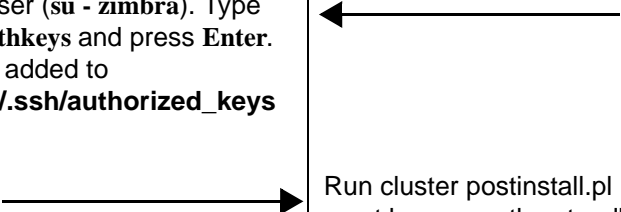
In order for remote management and postfix queue management, the ssh keys must be manually populated on each server.

6. To set up syslog and MTA auth keys, as Zimbra user (**su - zimbra**). Type **zmupdateauthkeys** and press **Enter**. The keys are added to **/opt/zimbra/ssh/authorized_keys**.

Active

7. To set up syslog and MTA auth keys, as Zimbra user (**su - zimbra**). Type **zmupdateauthkeys** and press **Enter**. The key are added to **/opt/zimbra/.ssh/authorized_keys**

Standby



Run cluster **postinstall.pl** . Postinstall must be run on the standby node first because execution of postinstall requires that the LDAP server be running. Zimbra cluster post install script is used after Zimbra Collaboration Suite is installed on the servers to move the data files from the local disk to the volume(s) created on the SAN

8. To start the Zimbra post install cluster configuration script, **cd** to the **zcs-cluster** directory created in step 2.
Type **./postinstall.pl** to begin post install.

The Zimbra processes are stopped, various cluster-specific adjustments are made to the Zimbra Collaboration Suite installation, and unnecessary data files are deleted

9. Mount the SAN volume (s). You can mount one volume for all services or you can mount ten separate volumes. The following command is to mount one volume for all services. To mount by label as root type:
[root@node1 zcs] **mount LABEL=mysanvol /opt/zimbra-cluster/mountpoints/mail.example.com.**
10. Run cluster **postinstall.pl**.
To start the Zimbra post install cluster configuration script, **cd** to the **zcs-cluster** directory created in step 2.
Type **./postinstall.pl** to begin post install.

Active

The Zimbra processes are stopped, various cluster-specific adjustments are made to the Zimbra Collaboration Suite installation, and the data files are moved to the SAN volume(s).

When the postinstall is complete use the Zimbra cluster configurator script to prepare Red Hat Cluster Suite to run the Zimbra Collaboration Suite. **The cluster configurator script is run on only the active mailbox node.**

The cluster configurator asks a series of questions to gather information about the cluster and generate the cluster configuration file, **/etc/cluster/cluster.conf**. This is the main configuration file of Red Hat Cluster Suite.

The cluster configurator installs the generated configuration file on each cluster node as **/etc/cluster/cluster.conf**.

11. To start the Zimbra configuration script, **cd** to the zcs-cluster directory created in step 2.
Type **./configure-cluster.pl**.
The configurator checks to verify that the server installation is correct.
12. When **Is installation finished on all cluster nodes?** displays, type **y** to continue.
13. Enter a name to identify this cluster.
Press **Enter**.

Important: Each cluster on the same network must have a distinct name. Make sure you enter a name that is not in use! Each Red Hat Cluster Suite cluster on the same network must have a distinct name to avoid interfering with another Red Hat Cluster Suite cluster.

Standby

Active

14. Select the network power switch type that is used as the fence device. Configure the fence device host name/IP address, login, and password.

15. Enter the fully-qualified hostname for the nodes in the cluster and the plug number associated with the node's power cord. When the two nodes are identified, type **Done**.

For each service, you need to choose a preferred node to run on and enter the list of volumes to be mounted from the SAN.

16. Select the cluster service. In this cluster configuration, only one service is available. Select **1**.

17. Choose the preferred node on which to run service mail.example.com, node 1

18. A Zimbra cluster service must mount service-specific data volumes. All service data can be placed on a single volume or the different types of data can be distributed over multiple volumes. Choose the volume setup type, single volume or multiple volumes.

19. When "Choose a service...", displays, select **2**. The configuration is complete.

20. Press **Enter** again to view a summary of the configuration.

21. After viewing the summary, save the configuration to a file. You can either accept the default name or rename the configuration file.

22. The configuration file must be copied to the standby node. If you want the script to copy the file to the standby node, enter **Yes**. (Enter the root password, if prompted.)

Standby

Active	Standby
<p>23. When asked, press Enter, to continue.</p> <p>24. Bring down the cluster service IP address. At root@node1 ZCS-cluster]# type ip addr del xx.xx.xx.xx dev eth0. You can now proceed with starting the RHCS daemons, which will bring up ZCS on one of the nodes.</p> <p>25. Start the cluster for the first time on the active node. See “Starting the Red Hat Cluster Suite Daemons” section below.</p> <p>26. When clustat shows the cluster services running on the active node, the cluster configuration is complete.</p>	

Start the Red Hat Cluster Suite Daemons

After the cluster configuration file is copied, you can start the Red Hat Cluster Suite daemons.

Important: *In order to start the cluster daemons correctly, you must be logged on to each node before proceeding, and to see any errors, you should have two sessions open for each node. You enter a command for one node, then enter the same command for the second. You must enter each command on both nodes, before proceeding to the next command.*

- Log on to each node as root.
- Run **tail -f /var/log/messages**, on each node to watch for any errors.
- Open another session for each node.

To start the Red Hat Cluster Service on a member, type the following commands in this order. Remember to enter the command on each node before proceeding to the next command.

1. **service ccsd start**. This is the cluster configuration system daemon that synchronizes configuration between cluster nodes.
2. **service cman start**. This is the cluster heartbeat daemon. It returns when both nodes have established heartbeat with one another.
3. **service fenced start**. This is the cluster I/O fencing system that allows cluster nodes to reboot a failed node during failover.

4. **service rgmanager start**. This manages cluster services and resources.

The **service rgmanager start** command returns immediately, but initializing the cluster and bringing up the Zimbra Collaboration Suite application for the cluster services on the active node may take some time.

After all commands have been issued on both nodes, run **clustat** command on the active node, to verify that the cluster service has been started.

When clustat shows all services are running on the active node, the cluster configuration is complete.

What to do if cluster services does not relocate to preferred node

If the services does not relocate to the active node after several minutes, you can issue Red Hat Cluster Suite utility commands to manually correct the situation.

Note: Not starting correctly on the preferred node usually is an issue that happens only the first time the cluster is started.

For the cluster service that is not running on the active node, run **clusvcadm -d <cluster service name>**, as root on the active node.

```
[root@node1.example.com]#clusvcadm -d mail1.example.com
```

This disables the service by stopping all associated Zimbra processes, releasing the service IP address, and unmounting the service's SAN volumes.

To enable a disabled service, run **clusvcadm -e <service name> -m <node name>**. This command can be run on any cluster node. It instructs the specified node to mount the SAN volumes of the service, bring up the service IP address, and start the Zimbra processes.

```
[root@node1.example.com]#clusvcadm -e mail1.example.com -m node1.example.com
```

Testing the Cluster Set up

To perform a quick test to see if failover works:

1. Log in to the remote power switch and turn off the active node.
2. Run **tail -f /var/log/messages** on the standby node. You will observe the cluster becomes aware of the failed node, I/O fence it, and bring up the failed service on the standby node.

View Zimbra Cluster Status

Go to the Zimbra administration console to check the status of the Zimbra cluster. The **Server Status** page shows the cluster server, the node, the services running on the cluster server, and the time the cluster was last checked. The standby node is displayed as standby. If a service is not running, it is shown as disabled.

