Zimbra™ Collaboration Suite Administrator's Guide

Release 5.0 Beta

Open Source Edition
August 2007

Legal Notice

Building Better Products within the Open Source Community

Zimbra Collaboration Suite leverages many great technologies from the open source community: MySQL, OpenLDAP, Postfix, SpamAssassin, and Apache. Zimbra believes that great products come from contributing to and leveraging open source technologies. We are thankful for the great contributions that led to the creation of MySQL, OpenLDAP, Postfix, SpamAssassin, and Apache.

Trademark and Licensing

Zimbra, Inc.
1500 Fashion Island Boulevard, Suite 100
San Mateo, California 94404 USA
650. 212.0505
www.zimbra.com

Table of Contents

Chapter 1 Introduction

Zimbra™ Collaboration Suite is a full-featured messaging and collaboration solution that includes shared email, address book, calendaring, tasks, and Web document authoring.

Intended Audience

This guide is intended for system administrators responsible for installing, maintaining, and supporting the server deployment of Zimbra.

Readers of this guide should already possess the following recommended knowledge and skill sets:

- Familiarity with the associated technologies and standards, including Red Hat® Enterprise Linux® operating system, SUSE operating systems, and open source concepts
- Industry practices for mail system management

Available Documentation

The following Zimbra documentation is available:

- **Installation Guides**. Installation guides for single server and multi-server installation, include system requirements and server configuration instructions.
- **Administrator Guide**. This guide provides a comprehensive product overview, including architecture, server functionality, administration tasks, configuration options, and monitoring tools.
- **Zimbra Migration Wizard Guides**. The guides provides instructions for running the Migration Wizard to migrate accounts from either Microsoft Exchange servers or Lotus Domino servers.
- **Zimbra administration console Help**. The Help topics describes how to perform tasks required to centrally manage Zimbra servers and mailbox accounts from the administration console.
- **Zimbra Web Client Help**. The Help topics describes how to use the features of the Zimbra Web Client.

- **Release Notes**. Late-breaking news for product releases and upgrade instructions are contained in the release notes. The latest notes can be found on the Zimbra Website, www.zimbra.com.

Support for Recommended Third-Party Components

Where possible, Zimbra adheres to existing industry standards and open source implementations for backup management, user authentications, operating platform, and database management. However, Zimbra only supports the specific implementations described in the Zimbra Collaboration Suite architecture overview in the Product Overview chapter as officially tested and certified for the Zimbra Collaboration Suite. This document may occasionally note when other tools are available in the marketplace, but such mention does not constitute an endorsement or certification.

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
- Explore the Zimbra Forums for answers to installation or configurations problems
- Join the Zimbra 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 Forum.

If you encounter problems with this software, go to http://bugzilla.zimbra.com to submit a bug report. Make sure to provide enough detail so that the bug can be easily duplicated.

Chapter 2 Product Overview

This chapter describes the Zimbra application architecture, integration points, and information flow.

The Zimbra Collaboration Suite is designed to provide an end-to-end mail solution that is scalable and highly reliable. The messaging architecture is built with well-known open-system technology and standards and is composed of a mail server application and a client interface.

The architecture includes the following core advantages:

- **Open source integrations**. Linux®, Apache Jetty, Postfix, MySQL®, OpenLDAP®.
- **Uses industry standard open protocols**. SMTP, LMTP, SOAP, XML, IMAP, POP.
- **Modern technology design**. Java, JavaScript thin client, DHTML.
- **Horizontal scalability**. Because each mailbox server includes its own data store, message store, and set mailbox accounts, you don't change anything on existing servers in order to scale the system. To scale for additional mail accounts, add more servers.
- Browser based client interface.
- Administration console to manage accounts and servers.

Core Functionality

The Zimbra Collaboration Suite provides the following state-of-the-art messaging and collaboration solutions.

- Email messaging
- Calendaring
- Address Books
- Web document authoring

The core functionality within the Suite is as follows:

- Mail delivery and storage
- Indexing of mail messages upon delivery

- Mailbox server logging
- IMAP and POP support
- Directory services
- Anti-spam protection
- Anti-virus protection

Administrators can easily manage domains, servers, and accounts from the browser based administration console.

- Import Microsoft Exchange user accounts
- Add accounts and domains
- Set account restrictions either for an individual account or by COS
- Manage distribution lists
- Set up virtual hosts on a domain
- Manage servers
- Monitor usage

The Zimbra Web Client mail features include the ability to:

- Compose, read, reply, forward, and use other standard mail features
- View mail by conversation threads
- Tag mail to easily group messages for quick reference
- Perform advanced searches
- Save searches
- Use Calendar to schedule appointments
- Share calendars with others
- Create address books and share with others
- Set mailbox usage preferences, including defining mail filtering options
- Use Zimbra Documents to create, organize and share web documents

Zimbra Components

Zimbra architecture includes open-source integrations using industry standard protocols. The third-party software listed below is bundled with Zimbra software and installed as part of the installation process. These components have been tested and configured to work with the software.

- Jetty, the web application server that Zimbra software runs in. Jetty is released under the Apache2.0 license.
- Postfix, an open source message transfer agent (MTA) that routes mail messages to the appropriate Zimbra server.

- OpenLDAP software, an open source implementation of the Lightweight Directory Access Protocol (LDAP) that provides user authentication.
- MySQL database software.
- Lucene, an open-source full featured text index and search engine.
- Anti-virus and anti-spam open source components including:
  - ClamAV, an anti-virus scanner that protects against malicious files.
  - SpamAssassin and DSPAM, mail filters that attempt to identify spam.
  - Amavisd-new, which interfaces between the MTA and one or more content checkers.
- James/Sieve filtering, used to create filters for email.

System Architecture

Figure 1 shows the Zimbra Collaboration Suite architectural design, including the open-source software bundled with the Suite and other recommended third-party applications.

The Zimbra Collaboration Suite includes the following application packages.

Zimbra Core

The Zimbra Core package includes the libraries, utilities, monitoring tools, and basic configuration files.

Zimbra LDAP

The Zimbra Collaboration Suite uses the OpenLDAP software, an open source LDAP directory server. User authentication is provided through OpenLDAP. Each account on the Zimbra server has an unique mailbox ID that is the primary point of reference to identify the account.

The OpenLDAP schema has been customized for the Zimbra Collaboration Suite.

Zimbra MTA (mail routing server)

Postfix is the open source mail transfer agent (MTA) that receives email via SMTP and routes each message to the appropriate Zimbra mailbox server using Local Mail Transfer Protocol (LMTP). The Zimbra MTA also includes the anti-virus and anti-spam components.

Zimbra Store (Zimbra server)

The Zimbra store package installs the components for the mailbox server, including Jetty, which is the servlet container the Zimbra software runs within. Within ZCS, this servlet container is called **mailboxd**.

Each account is configured on one mailbox server, and this account is associated with a mailbox that contains all the mail messages and file attachments for that mail account.

The mailbox server includes the following components:

- Data store
- Message store
- Index store

Each Zimbra server has its own standalone data store, message store and index store for the mailboxes on that server.

As each mail arrives, the Zimbra server schedules a thread to have the message indexed (index store).

Data store. The **data store** is a MySQL database where internal mailbox IDs are linked with user accounts. The data store maps the mailbox IDs to users' OpenLDAP accounts. This database contains each user's set of tag definitions, folders, calendar schedules, and contacts, as well as the status of each mail message - read, unread, tags associated to message, and folder the message resides in.

Message store. The **message store** is where all email messages and file attachments reside. Messages are stored in MIME format. A message that is sent to multiple recipients who have accounts on one mailbox server are stored only once in the file system.

Index store. Index and search technology is provided through Lucene. Index files are maintained for each mailbox.

Zimbra-SNMP

Installing the Zimbra-SNMP package is optional. If you choose to install Zimbra-SNMP for monitoring, the package should be run on every server (Zimbra server, Zimbra LDAP, Zimbra MTA) that is part of the Zimbra configuration. Zimbra uses swatch to watch the syslog output to generate SNMP traps.

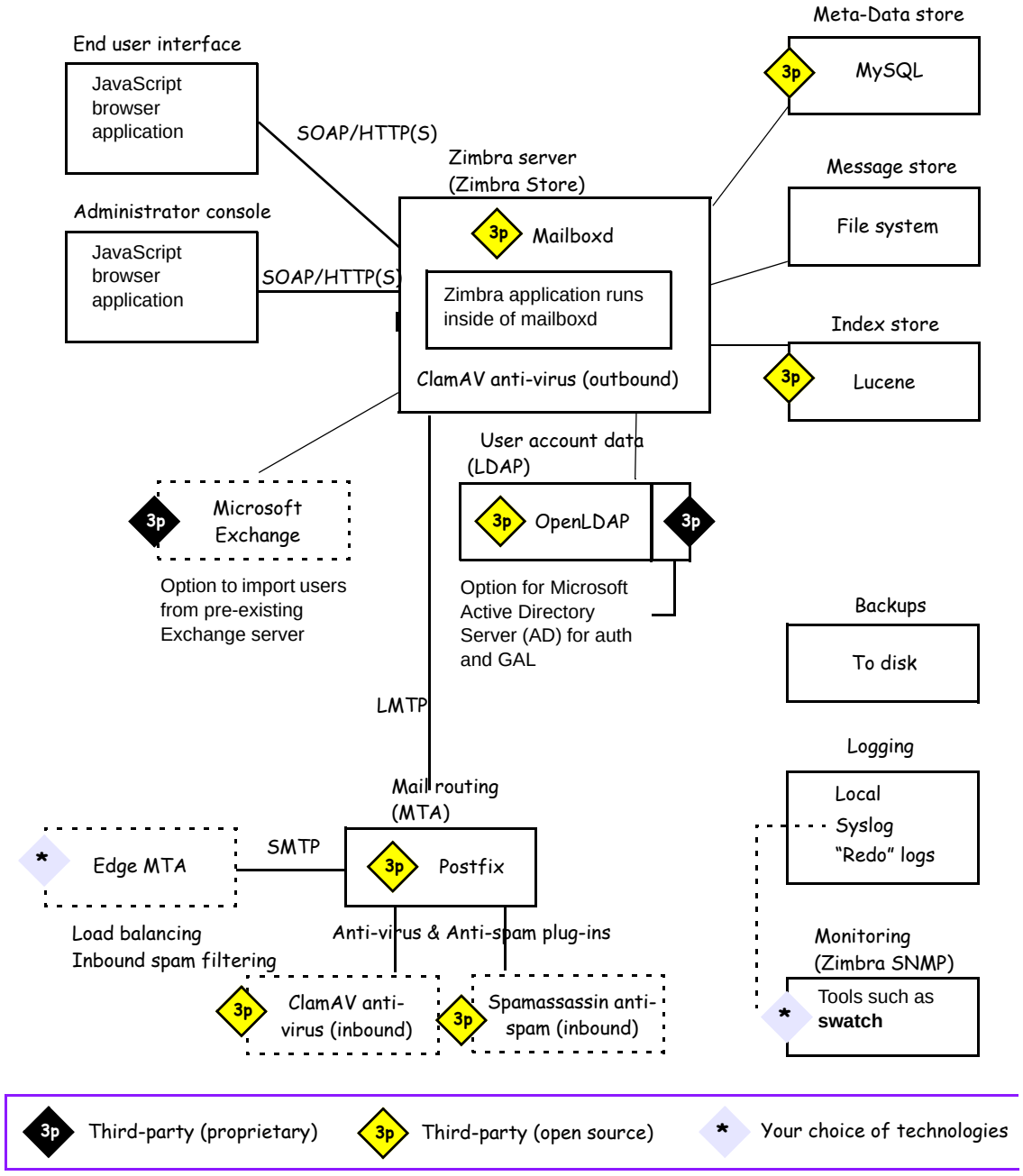
Zimbra Logger

Installing the Zimbra Logger package is optional and is installed on one mailbox server. The Zimbra logger installs tools for syslog aggregation, reporting, and message tracing. If you do not install Logger, you cannot use the message trace feature. In addition, the server statistics are not captured, and the server statistics section of the administration console will not display.

Zimbra Spell

Installing the Zimbra Spell package is optional. Aspell is the open source spell checker used on the Zimbra Web Client. When Zimbra-spell is installed, the Zimbra-apache package is also installed.

Figure 1: Zimbra Collaboration Suite System Architecture



Zimbra System Directory Tree

Table 1 lists the main directories created by the Zimbra installation packages.

Note: *The directory organization is the same for any server in the Zimbra Collaboration Suite, installing under /**opt/zimbra**.*

Table 1 Directory Structure for Zimbra Components

Parent	Directory	Description
/opt/ zimbra/		Created by all Zimbra installation packages
	bin/	Zimbra application files, including the utilities described in Appendix A, Command -Line Utilities
	clamav	Clam AV application files for virus and spam controls
	conf/	Configuration information
	contrib	Third party scripts for conveyance
	convertd	Convert service
	cyrus-sasl	SASL AUTH daemon
	db/	Data Store
	doc/	Zimbra documentation and readme files
	dspam	DSPAM antivirus
	httpd	Spell server
	index/	Index Store
	java/	Contains Java application files
	lib/	Libraries
	libexec/	Internally used executables
	log/	Local logs for Zimbra server application
	logger/	MySQL data files for logger services mySQL instance
	mysql/	MySQL database files
	openldap/	OpenLDAP server installation, pre-configured to work with Zimbra

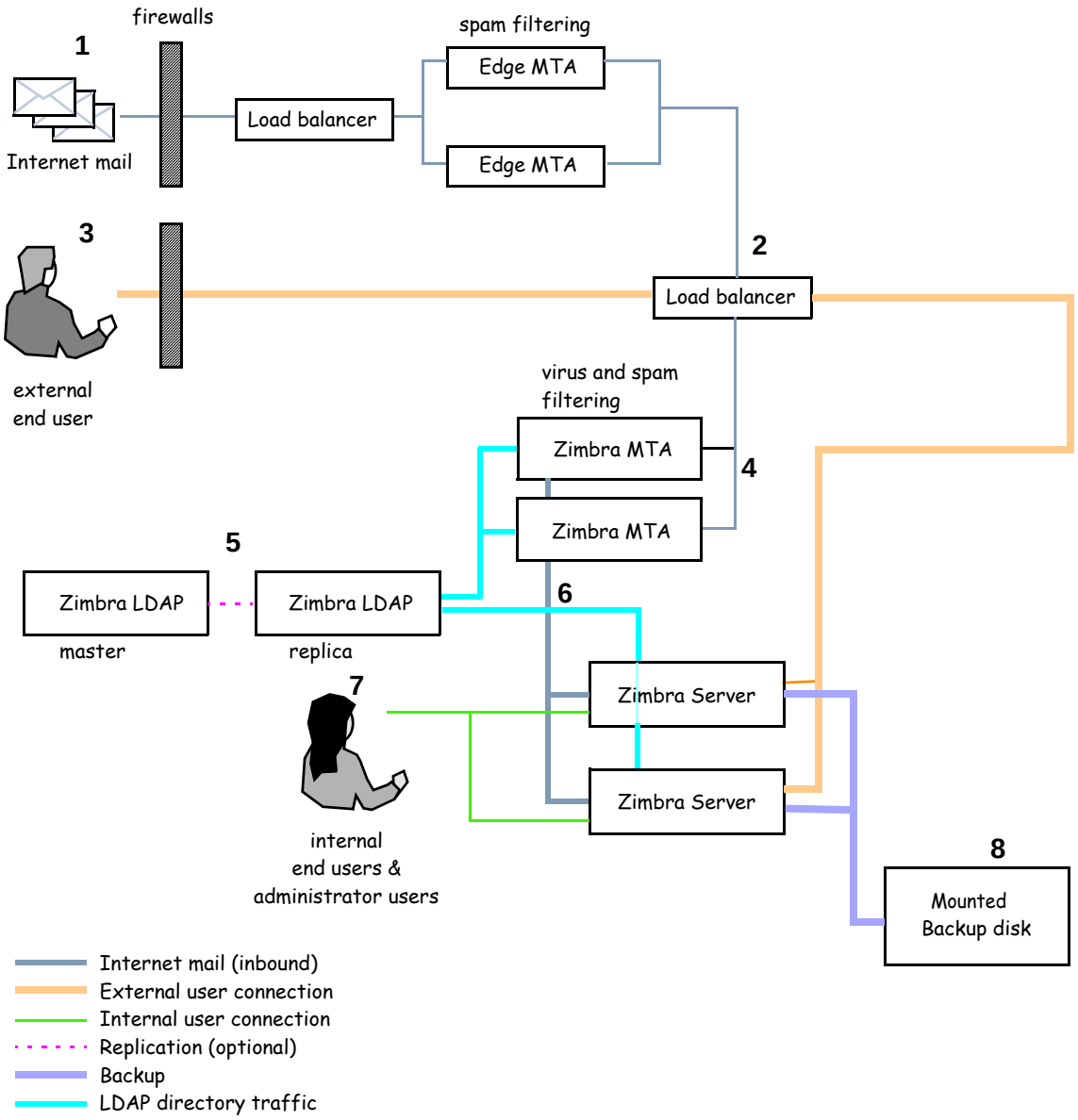
Parent	Directory	Description
	nginx	IMAP proxycd e
	postfix/	Postfix server installation, pre-configured to work with Zimbra
	redolog/	Contains current transaction logs for the Zimbra server
	sleepycat/	Berkeley DB
	snmp/	SNMP monitoring files
	ssl/	Certificates
	store/	Message Store
|||	**jetty/**	mailboxd application server instance. In this directory, the **webapps/zimbra/skins** directory includes the Zimbra UI theme files.
	wiki	Contains the Zimbra Documents global template file
	zimbramon/	Contains the control scripts and Perl modules
	zimlets	Contains Zimlet zip files that are installed with Zimbra
	zimlets-extra	Contains Zimlet zip files that can be installed
	zmstat	

Example of a Typical Multi-Server Configuration

The exact configuration for each deployment is highly dependent on variables including the number of mailboxes, mailbox quotas, performance requirements, existing network infrastructure, IT policies, security methodologies, spam filtering requirements, and so forth.

Figure 2 shows a typical configuration with incoming traffic and user connection. Alternate ways of configuring at many points within the network are possible.

Figure 2: Typical Configuration with Incoming Traffic and User Connections



Explanation of Figure 2 follows:

1. Inbound Internet mail goes through a firewall and load balancing to the edge MTA for spam filtering.
2. The filtered mail then goes through a second load balancer.
3. An external user connecting to the messaging server also goes through a firewall to the second load balancer.
4. The inbound Internet mail goes to any of the Zimbra MTA servers and goes through spam and virus filtering.

5 The designated Zimbra MTA server looks up the addressee's directory information from the Zimbra LDAP replica server.

6 After obtaining the user's information from the Zimbra LDAP server, the MTA server sends the mail to the appropriate Zimbra server.

7 Internal end-user connections are made directly to any Zimbra server which then obtains the user's directory information from Zimbra LDAP and redirects the user as needed.

8 Zimbra servers' backups can be processed to a mounted disk.

Chapter 3 Zimbra Server

The Zimbra server is a dedicated server that manages all of the mailbox contents, including messages, contacts, calendar, Documents notebooks, and attachments. Messages are received from the Zimbra MTA server and then passed through any filters that have been created. Messages are then indexed and deposited into the correct mailbox.

Each Zimbra mailbox server in the system can see only its own storage volumes. Zimbra mailbox servers cannot see, read, or write to another Zimbra server.

In a Zimbra single server environment, all services are on one server, and during installation the computer is configured to partition the disk to accommodate each of the services.

In a Zimbra multi-server environment, the Zimbra LDAP and Zimbra MTA services can be installed on separate servers. See the Multi-Server Installation Guide.

Incoming Mail Routing

The MTA server, receives mail via SMTP and routes each mail message to the appropriate Zimbra mailbox server using LMTP. As each mail message arrives, the Zimbra server schedules a thread to have Lucene index it.

Disk Layout

The mailbox server includes the following volumes:

- **Message Store.** Mail message files are in **opt/zimbra/store**
- **Data Store.** The MySQL Database files are in **opt/zimbra/db**
- **Index Store.** Index files are in **opt/zimbra/index**
- **Log files.** Each component in the Zimbra Collaboration Suite has log files. Local logs are in **/opt/zimbra/log**

Message Store

The Zimbra Message Store is where all email messages reside, including the message body and any file attachments. Messages are stored in MIME format.

The Message Store is located on each Zimbra server under **/opt/zimbra/store**. Each mailbox has a dedicated directory named after its internal Zimbra mailbox ID.

Note: *Mailbox IDs are unique per server, not system-wide.*

Single-Copy Message Storage

"Single copy storage" allows messages with multiple recipients to be stored only once in the file system. On UNIX systems, the mailbox directory for each user contains a hard link to the actual file.

Data Store

The Zimbra Data Store is a MySQL database that contains all the metadata regarding the messages including tags, conversations, and pointers to where the messages are stored in the file system.

Each account (mailbox) resides only on one server. Each Zimbra server has its own standalone data store containing data for the mailboxes on that server.

The Data Store contains:

- Mailbox-account mapping. The primary identifier within the Zimbra database is the mailbox ID, rather than a user name or account name. The mailbox ID is only unique within a single mailbox server. The Data Store maps the Zimbra mailbox IDs to the users' OpenLDAP accounts.
- Each user's set of tag definitions, folders, and contacts, calendar appointments, filter rules.
- Information about each mail message, including whether it is read or unread, and which tags are associated.

Index Store

The index and search technology is provided through Apache Lucene. Each message is automatically indexed as it enters the system. Each mailbox has an index file associated with it.

The tokenizing and indexing process is not configurable by administrators or users.

The process is as follows:

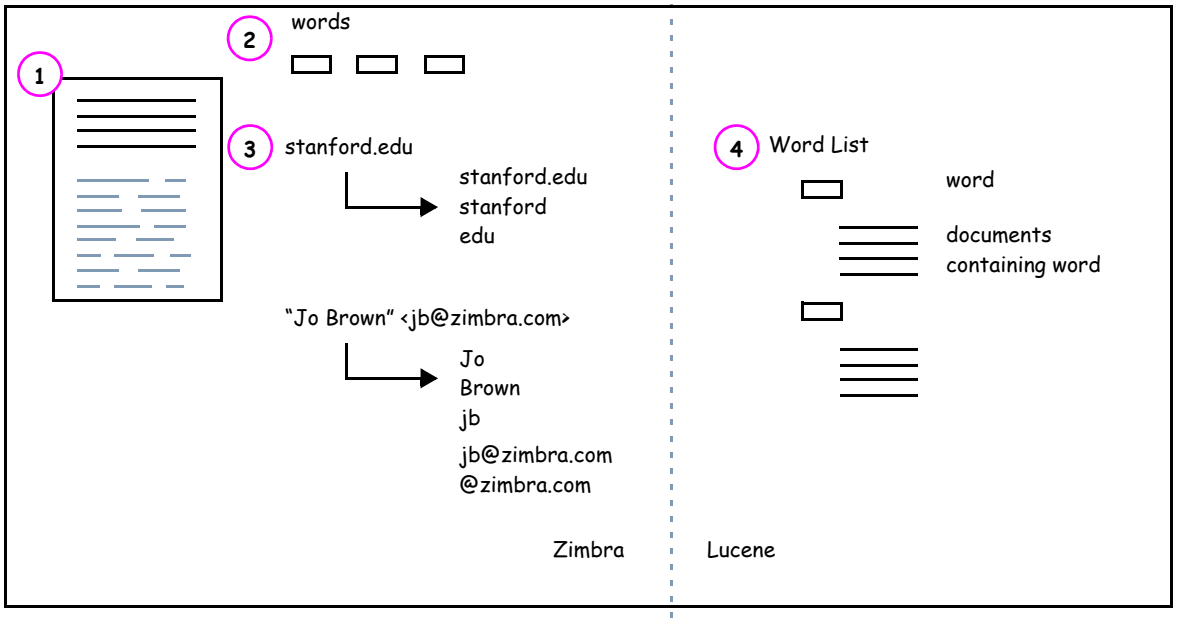
1. The Zimbra MTA routes the incoming email to the Zimbra mailbox server that contains the account's mailbox.

2. The mailbox server parses the message, including the header, the body, and all readable file attachments such as PDF files or Microsoft Word documents, in order to tokenize the words.

3. The mailbox server passes the tokenized information to Lucene to create the index files.

   Note: *Tokenization: The method for indexing is by each word. Certain common patterns, such as phone numbers, email addresses, and domain names are tokenized as shown in Figure 3.*

Figure 3: Message tokenization



Redo Log

Each Zimbra server generates redo logs that contain every transaction processed by that server. If an unexpected shutdown occurs to the server, the redo logs are used for the following:

- To ensure that no uncommitted transactions remain, the server rereads the redo logs upon startup.
- During restore, to recover data written since the last full backup in the event of a server failure.

When the current redo log file size reaches 100MB, the current redo log rolls over to an archive directory. At that point, the server starts a new redo log. All uncommitted transactions from the previous redo log are preserved. In the case of a crash, when the server restarts, the current redo log and the archived logs are read to re-apply any uncommitted transactions.

Log

A Zimbra deployment consists of various third-party components with one or more Zimbra mailbox servers. Each of the components may generate its own logging output.

Selected Zimbra log messages generate SNMP traps, which you can capture using any SNMP monitoring software. See Chapter 10, Monitoring Zimbra Servers

Chapter 4 Zimbra Directory Service

The Zimbra LDAP service is a directory service running a version of the OpenLDAP software that has the Zimbra schema already installed. This chapter describe how the directory service is used for user authentication and account configuration and management.

Note: *Zimbra also supports integration with Microsoft's Active Directory Server. Contact Zimbra support for more detailed information on specific directory implementation scenarios.*

The LDAP server is identified when the Zimbra software is installed. Each server has its own LDAP entry that includes attributes specifying operating parameters. In addition, there is a global configuration object that sets defaults for any server whose entry does not specify every attribute.

A selected subset of these attributes can be modified through the Zimbra administration console; others can be changed through the CLI utility.

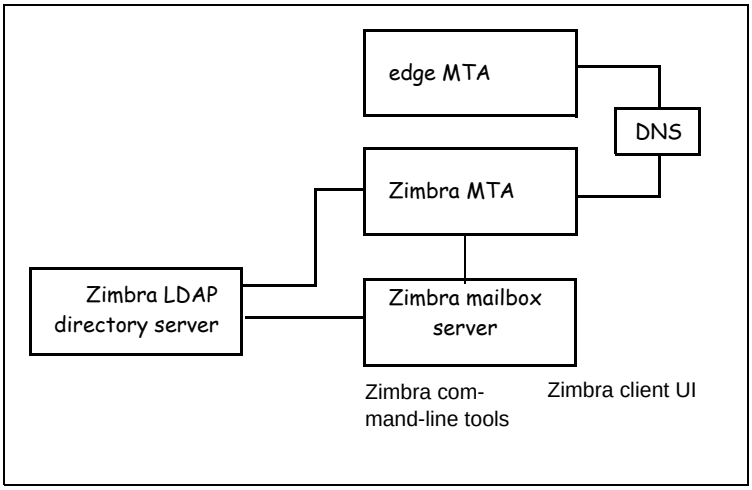
Directory Services Overview

LDAP directory services provide a centralized repository for information about users and devices that are authorized to use your network. The central repository used for Zimbra's LDAP data is the OpenLDAP directory server.

Figure 4 shows traffic between the Zimbra-LDAP directory server and the other servers in the Zimbra system. The Zimbra MTA and the Zimbra mailbox server read from, or write to, the LDAP database on the directory server. The edge MTA does not connect to the LDAP database; instead, it uses the DNS server's MX entry to determine where to direct mail.

The Zimbra clients connect through the Zimbra server, which in turn connects to LDAP.

Figure 4: LDAP Directory Traffic



At the core of every LDAP implementation is a database organized using a *schema*. The schema specifies the types of objects that are stored in the database, and what types of attributes they have.

An LDAP directory entry consists of a collection of attributes and has a globally unique *distinguished name* (DN). The attributes allowed for an entry are determined by the *object classes* associated with that entry. The values of the object class attributes determine the schema rules the entry must follow.

The object classes determine what type of object the entry refers to and what type of data can be stored for that entry. An entry's object classes that determines what kind of entry it is, is called a structural object class and cannot be changed. Other object classes are called auxiliary and may be added to or deleted from the entry.

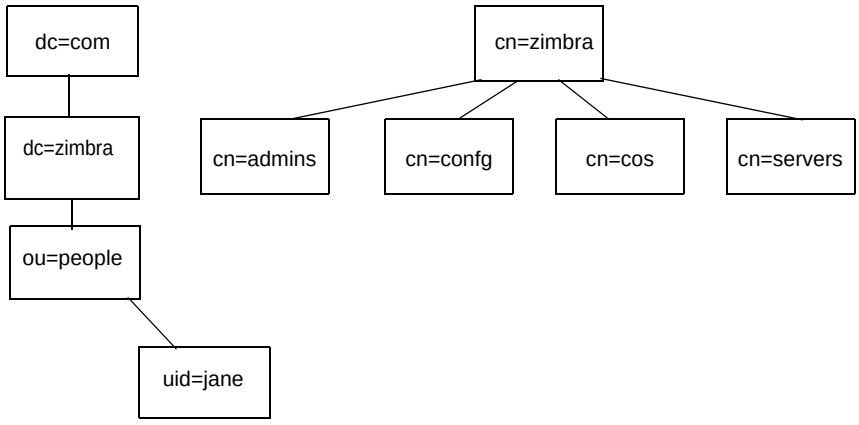
Use of auxiliary object classes in LDAP allows for an object class to be combined with an existing object class. For example, an entry with structural object class **inetOrgPerson,** and auxiliary object class **zimbraAccount,** would be an account, either administrator or end-user. An entry with the object class **zimbraServer** would be a server in the Zimbra system that has one or more Zimbra software packages installed.

LDAP Hierarchy

LDAP directories are arranged in an hierarchal tree-like structure. In the Zimbra system, the structure is arranged based on Internet domain names. LDAP entries typically include items such as user accounts, organizations, or servers.

Figure 5 shows the Zimbra LDAP hierarchy. Each type of entry (object) has certain associated object classes.

Figure 5: Zimbra LDAP Hierarchy



For a complete listing of the Zimbra auxiliary object classes, see the Zimbra LDAP Schema.

Zimbra Schema

Every LDAP implementation has a schema that defines its domain structure, account attributes, and other data structures in use by the organization. Zimbra includes a custom LDAP schema that extends the generic schema included with OpenLDAP software and is designed to potentially coexist with existing directory installations. The Zimbra server, the Zimbra administration console, the command-line account provisioning, and the management utilities require the Zimbra schema.

All attributes and object classes specifically created for Zimbra are prefaced by “zimbra”, as in **zimbraMailRecipient** object class or the **zimbraAttachmentsBlocked** attribute.

The Zimbra schema assumes a baseline schema. In the OpenLDAP installer package included with the Zimbra system, the following schema files are included in the OpenLDAP implementation:

- **core.schema**
- **cosine.schema**
- **inetorgperson.schema**
- **zimbra.schema**

Note: *You cannot modify the Zimbra schema.*

Account Authentication

This section describes the account authentication mechanisms and formatting directives supported:

- **Internal**
- **External LDAP**
- **External Active Directory**

The **Internal** authentication method assumes the Zimbra schema running on the OpenLDAP directory server.

The **External LDAP** and **External Active Directory** authentication methods attempt to bind to the specified LDAP server, using the supplied user name and password. These method can be used if the email environment uses Microsoft Active Directory directory services for authentication and the Zimbra-LDAP directory services for all other Zimbra-related transactions. This requires that users exist in both OpenLDAP and in the Active Directory servers.

The method type is set on a per-domain basis, using the **zimbraAuthMech** attribute, with other information also coming from the domain. If this attribute is not set, the default is to use the internal method as the authentication.

The Internal Authentication Mechanism

For accounts stored in the OpenLDAP server, the **userPassword** attribute stores a salted-SHA1 (SSHA) digest of the user's password. This information is not used to connect to the directory server; it is only used to compare with the information on the OpenLDAP server, using a pool of re-usable administrator LDAP connections.

External LDAP and External Active Directory Authentication Mechanism

Unlike the internal authentication mechanism, the external authentication mechanism attempts to bind to the directory server using the supplied user name and password. If this bind succeeds, the connection is closed and the password is considered valid.

Two additional domain attributes are required for the external mechanism: **zimbraAuthLdapURL** and **zimbraAuthLdapBindDn**.

zimbraAuthLdapURL Attribute and SSL

The **zimbraAuthLdapURL** attribute contains the URL of the Active Directory server to bind to. This should be in the form:

ldap://*ldapserver***:***port*/

where *ldapserver* is the IP address or host name of the Active Directory server, and *port* is the port number. You can also use the fully qualified host name instead of the port number.

Examples include:

ldap://server1:389
ldap://exch1.acme.com

For SSL connection, use **ldaps:** instead of **ldap:**. If the SSL version is used, the SSL certificate used by the server must be configured as a trusted certificate.

zimbraAuthLdapBindDn Attribute

The **zimbraAuthLdapBindDn** attribute is a format string used to determine which user name to use when binding to the Active Directory server.

During the authentication process, the user name starts out in the format:

user@domain.com

The user name may need to be transformed into a valid LDAP bind dn (distinguished name). In the case of Active Directory, that bind dn might be in a different domain

Zimbra Objects

Zimbra uses auxiliary object classes to add Zimbra-specific attributes to existing objects such as an account. The LDAP objects used in Zimbra include the following:

- Accounts
- Class of Service (COS)
- Domains
- Distribution Lists
- Recipients
- Servers
- Global Configurations
- Aliases
- TimeZone
- Zimlet
- CalendarResource

Accounts Object

An account object represents an account on the Zimbra mailbox server that can be logged into. Account entrees are either administrators or user accounts that can be logged into. The object class name is **zimbraAccount**. This object class extends the **zimbraMailRecipient** object class.

The object class **zimbraMailRecipient** is a directory entry that represents an entity that can receives mail. This is a visible external mail address that is expanded through aliases or forwarding into one or more internal/external addresses.

All accounts have the following properties:

- A name in the format of user@some.domain
- A unique ID that never changes and is never reused
- A set of attributes, some of which are user-modifiable (options) and others that are only configurable by the system administrator

All user accounts are associated with a domain, so a domain must be created before creating any accounts.

For more about account provisioning, see the Chapter 8, Managing User Accounts.

Class of Service (COS) Object

Class of Service is a Zimbra-specific object that defines the default attributes an email account has and what features are added or denied. The COS controls features, default preference settings, mailbox quotas, message lifetime, password restrictions, attachment blocking and server pools for creation of new accounts. The object class name is **zimbraCOS.**

Each account is assigned a class of service. COS is used to group accounts and define the feature levels for those accounts. For example, executives can be assigned to a COS that allows the Calendar application. By grouping accounts into specific type of COS, account features can be updated in block.

If the COS is not explicitly set, or if the COS assigned to the user no longer exists, values come from a pre-defined COS called "default".

A COS is not restricted to a particular domain or set of domains.

Domains Object

A Domains object represents an email domain such as *ace.**com*** or *zink.**org**.* A domain must exist before email addressed to users in that domain can be delivered. The object class name is **zimbraDomain**.

Distribution Lists Object

Distribution Lists, also known as mailing lists, are used to send mail to all members of a list by sending a single email to the list address. The object class name is **zimbraDistributionList**.

Recipient Object

Recipient object represents an entity that can receive mail. An external email address exists, and the recipient can be expanded through aliases or forwarding into one or more internal/external addresses. The object class name is **zimbraMailRecipient**. This object class name is only used in conjunction with **zimbraAccount** and **zimbraDistributionlist** classes.

Servers Object

The servers object represents a particular server in the Zimbra system that has one or more of the Zimbra software packages installed. During the installation, the software is automatically registered on the OpenLDAP server. The object class name is **zimbraServer**. Attributes describe server configuration information, such as which services are running on the server.

The server name is used by the Zimbra system to make a request for the server object in the directory. The server requested gets its configuration information and picks up any changes that might have been made by the administrator through the Zimbra Administrator Console.

Global Configuration Object

The Global Configuration object specifies default values for the following objects: server, account, COS, and domain. If the attributes are not set for other objects, the values are inherited from the global settings. The object class name is **zimbraGlobalConfig**.

Global configuration values are required and are set during installation as part of the Zimbra core package. These become the default values for the system.

Alias Object

Alias object is a placeholders in the directory to reserve a name. The object class name is **zimbraAlias**. The attribute points to another entry.

TimeZone Object

TimeZone object is a list of well-known time zones used by the web client. The object class name is zimbraTimeZone.

Zimlet Object

Zimlet Object defines Zimlets that are installed and configured in ZCS. The object class name is zimbraZimletEntry. See the Working with Zimlets chapter for more information about Zimlets.

CalendarResource Object

CalendarResource object defines a calendar resource such as conference rooms or equipment that can be selected for a meeting. The object class name is zimbraCalendarResource.

Company Directory/GAL

A company directory is a company-wide listing of users, usually within the organization itself, that is available to all users of the email system. Sometimes called “white pages” or global address list (GAL), Zimbra uses the company directory to look up user addresses from within the company.

For each domain used in Zimbra, you can choose from the following GAL search options:

- Use an external LDAP server for the GAL
- Use the Zimbra implementation in OpenLDAP
- Include both external LDAP server and OpenLDAP in GAL searches

GAL Searches in Zimbra Client

The Zimbra client can search the GAL. The GAL search returns a list of directory entries that match the user's search.

When the user supplies a name to search for, that name is turned into an LDAP search filter similar to the following example:

```
(|(cn = %s*)(sn=%s*)(gn=%s*)(mail=%s*))
   (zimbraMailDeliveryAddress = %s*)
   (zimbraMailAlias=%s*)
   (zimbraMailAddress = %s*)
```

The string "%s" is replaced with the name the user is searching for.

GAL Attributes in Zimbra

Two possible sources for GAL information are the Zimbra server and the Active Directory server. The relevant LDAP/Active Directory fields are referenced in the Zimbra schema under the same names as listed in the Active Directory schema.

Table 1 maps generic GAL search attributes to their Zimbra contact fields.

Table 1 Attributes Mapped to Zimbra contact

Standard LDAP Attribute	Zimbra Contact Field
co	workCountry
company	Company
givenName/gn	firstName
sn	lastName
cn	fullName
initials	initials
l	workCity
physicalDeliveryOfficeName	office
ou	department
street, streetaddress	workStreet

Table 1 Attributes Mapped to Zimbra contact

Standard LDAP Attribute	Zimbra Contact Field
postalCode	workPostalCode
telephoneNumber	workPhone
st	workState
title	jobTitle
mail	email
objectClass	Not currently mapped

Zimbra GAL Search Parameters

Like authentication, GAL is configured on a per-domain basis. From the administration console, you can run the GAL Configuration Wizard to configure the domain's attributes.

Modifying Attributes

The OpenLDAP directory should not be modified directly. Any additions, changes and deletions are made through the Zimbra administration console or from the CLI utility for provisioning, **zmprov**.

Users modify attributes for their entry (accounts) in the OpenLDAP directory when they change their options from the Zimbra Web Client.

Administrators can also modify LDAP attributes using the command-line tools described in Appendix A: Command-Line Utilities.

Important: *Do not use any LDAP browsers to change the Zimbra LDAP content.*

Chapter 5 Zimbra MTA

The Zimbra MTA (Mail Transfer Agent) receives mail via SMTP and routes each message, using Local Mail Transfer Protocol (LMTP), to the appropriate Zimbra mailbox server.

The Zimbra MTA server includes the following programs:

- Postfix MTA, for mail routing, mail relay, and attachment blocking
- Clam AntiVirus, an antivirus engine used for scanning email messages and attachments in email messages for viruses
- SpamAssassin and DSPAM, mail filters that attempt to identify unsolicited commercial email (spam), using a variety of mechanisms
- Amavisd-New, a Postfix content filter used as an interface between Postfix and ClamAV / SpamAssassin

In the Zimbra Collaboration Suite configuration, mail transfer and delivery are distinct functions. Postfix primarily acts as a Mail Transfer Agent (MTA) and the Zimbra mail server acts as a Mail Delivery agent (MDA).

MTA configuration is stored in LDAP and a configuration script automatically polls the LDAP directory every two minutes for modifications, and updates the Postfix configuration files with the changes.

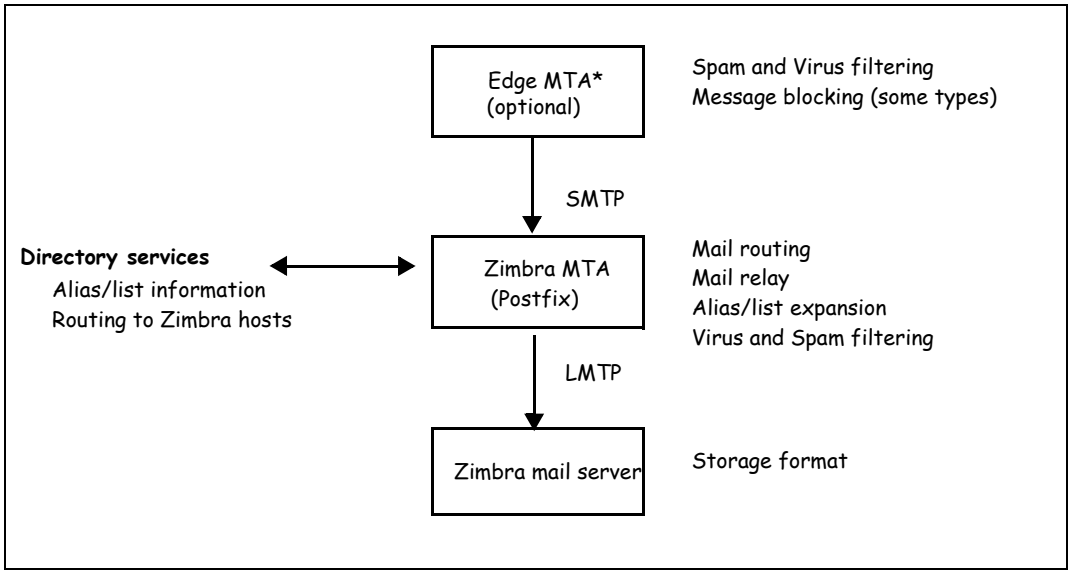
Zimbra MTA Deployment

The Zimbra Collaboration Suite includes a precompiled version of Postfix. This version does not have any changes to the source code, but it does include configuration file modifications, additional scripts, and tools.

Postfix performs the Zimbra mail transfer and relay. It receives inbound messages via SMTP, and hands off the mail messages to the Zimbra server via LMTP, as shown in Figure 6. The Zimbra MTA can also perform anti-virus and anti-spam filtering.

Postfix also plays a role in transfer of outbound messages. Messages composed from the Zimbra web client are sent by the Zimbra server through Postfix, including messages sent to other users on the same Zimbra server.

Figure 6: Postfix in a Zimbra Environment



***Edge MTA** The term "edge MTA" is a generic term referring to any sort of edge security solution for mail. You may already deploy such solutions for functions such as filtering. The edge MTA is optional. Some filtering may be duplicated between an edge MTA and the Zimbra MTA.

Postfix Configuration Files

Zimbra modified the following Postfix files specifically to work with the Zimbra Collaboration Suite:

- **main.cf** - Modified to include the LDAP tables. The configuration script in the Zimbra MTA pulls data from the Zimbra LDAP and modifies the Postfix configuration files.
- **master.cf** - Modified to use Amavisd-New.

Important: *Do not modify the Postfix configuration files directly! Some of the Postfix files are rewritten when changes are made in the administration console. Any changes you make will be overwritten.*

MTA Functionality

Zimbra MTA Postfix functionality includes:

- SMTP authentication
- Attachment blocking
- Relay host configuration
- Postfix-LDAP integration

- Integration with Amavisd-New, ClamAV, and Spam Assassin

SMTP Authentication

SMTP authentication allows authorized mail clients from external networks to relay messages through the Zimbra MTA. The user ID and password is sent to the MTA when the SMTP client sends mail so the MTA can verify if the user is allowed to relay mail.

Note: *User authentication is provided through the Zimbra LDAP directory server, or if implemented, through the Microsoft Active Directory Sever.*

SMTP Restrictions

In the administration console, you can enable restrictions so that messages are not accepted by Postfix when non-standard or other disapproved behavior is exhibited by an incoming SMTP client. These restrictions provide some protection against ill-behaved spam senders. By default, SMTP protocol violators (that is, clients that do not greet with a fully qualified domain name) are restricted. DNS based restrictions are also available.

Important: *Understand the implications of these restrictions before you implement them. You may want to receive mail from people outside of your mail system, but those mail systems may be poorly implemented. You may have to compromise on these checks to accommodate them.*

Relay Host Settings

Postfix can be configured to send all non-local mail to a different SMTP server. Such a destination SMTP server is commonly referred to as a “relay” or “smart” host. You can set this relay host from the administration console.

A common use case for a relay host is when an ISP requires that all your email be relayed through designated host, or if you have some filtering SMTP proxy server.

In the administration console, the relay host setting must not be confused with web mail MTA setting. Relay host is the MTA to which Postfix relays non-local email. Webmail MTA is used by the Zimbra server for composed messages and must be the location of the Postfix server in the Zimbra MTA package.

Important: *Use caution when setting the relay host to prevent mail loops*

MTA-LDAP Integration

The Zimbra LDAP directory service is used to look up email delivery addresses. The version of Postfix included with Zimbra is configured during the installation of the Zimbra Collaboration Suite to use the Zimbra LDAP directory.

Account Quota and the MTA

Account quota is the storage limit allowed for an account. Email messages, contact lists, calendars, and Documents notebook pages contribute to the quota. Account quotas can be set by COS or per account. The MTA attempts to deliver a message, and if a Zimbra user's mailbox exceeds the set quota, the Zimbra mailbox server rejects the message as mailbox is full and the sender gets a bounce message. You can view account quotas from the Administration Console, Monitoring Server Statistics section.

MTA and Amavisd-New Integration

The Amavisd-New utility is the interface between the Zimbra MTA and Clam AV and SpamAssassin scanners.

Anti-Virus Protection

Clam AntiVirus software is bundled with the Zimbra Collaboration Suite as the virus protection engine. The Clam anti-virus software is configured to block encrypted archives, to send notification to administrators when a virus has been found, and to send notification to recipients alerting that a mail message with a virus was not delivered.

The anti-virus protection is enabled during installation. You can also enable or disable virus checking from Global Settings on the administration console. By default, the Zimbra MTA checks every two hours for any new anti-virus updates from ClamAV.

Note: *Updates are obtained via HTTP from the ClamAV website.*

Anti-Spam Protection

SpamAssassin and DSPAM are spam filters bundled with ZCS. When ZCS is installed, spam training is automatically enabled to let users train spam filters when they move messages in and out of their junk folders.

The SpamAssassin default configuration for ZCS is as follows:

- Kill percent at 75%. Mail that is scored at 75% is considered spam and is not delivered. SpamAssassin score of 20 is considered 100%.
- Tag percent at 33%. Mail that is scored at 33% is considered spam and is delivered to the Junk folder.

A Subject Prefix can be configured so messages considered as spam are identified in the subject line as tagged as spam. When a message is tagged as spam, the message is delivered to the recipient's Junk folder.

You can change these settings from the administration console, Global Settings Anti-Spam tab.

Note: *ZCS configures the spam filter to add 0.5 to the Spamassassin score if DSPAM marks the message as spam and deduct 0.1 if DSPAM does not label it as spam.*

Anti-Spam Training Filters

When ZCS is installed, the automated spam training filter is enabled and two feedback system mailboxes are created to receive mail notification.

- Spam Training User to receive mail notification about mail that was not marked as junk, but should be.
- Non-spam (HAM) training user to receive mail notification about mail that was marked as junk, but should not have been.

For these training accounts, the mailbox quota is disabled (i.e. set to 0) and attachment indexing is disabled. Disabling quotas prevents bouncing messages when the mailbox is full.

How well the anti-spam filter works depends on recognizing what is considered spam or not considered spam. The SpamAssassin filter can learn what is spam and what is not spam from messages that users specifically mark as **Junk** from their web client toolbar or **Not Junk** from the web client Junk folder. A copy of these marked messages is sent to the appropriate spam training mailbox.The Zimbra spam training tool, **zmtrainsa,** is configured to automatically retrieve these messages and train the spam filter.

The **zmtrainsa script** is enabled through a cron job to feed mail that has been classified as spam or as non-spam to the SpamAssassin application, allowing SpamAssassin to 'learn' what signs are likely to mean spam or ham. The zmtrainsa script empties these mailboxes each day.

By default all users can give feedback in this way. If you do not want all users to train the spam filter, you can modify the global configuration attributes, **zimbraSpamIsSpamAccount** and **zimbraSpamIsNotSpamAccount**, and remove the account addresses from the attributes. To remove, type as:

zmprov mcf <attribute> ''

When these attributes are modified, messages marked as junk or not junk are not copied to the spam training mailboxes.

Initially, you may want to train the spam filter manually to quickly build a database of spam and non-spam tokens, words, or short character sequences that are commonly found in spam or ham. To do this, you can manually forward messages as message/rfc822 attachments to the spam and non-spam mailboxes. When **zmtrainsa** runs, these messages are used to teach the spam filter. Make sure you add a large enough sampling of messages to these mailboxes. In order to get accurate scores to determine whether to mark messages as spam at least 200 known spams and 200 known hams must be identified.

The zmtrainsa command can be run manually to forward any folder from any mailbox to the spam training mailboxes. If you do not enter a folder name

when you manually run zmtrainsa for an account, for spam the default folder is Junk, for ham, the default foler is Inbox.

To send a specific folder to the spam training mailbox, type the command as:

zmtrainsa <server> <user> spam [foldername]

To send a folder to the non-spam training mailbox, type:

zmtrainsa <server> <user> ham [foldername]

Turning On or Off RBLs

RBL (Real time black-hole lists) can be turned on or off in SpamAssassin from the Zimbra CLI.

The three RBL's that are enabled during installation are the following:

- reject_invalid_hostname
- reject_non_fqdn_hostname
- reject_non_fqdn_sender

You can set the following, in addition to the three above:

- reject_rbl_client dnsbl.njabl.org
- reject_rbl_client cbl.abuseat.org
- reject_rbl_client bl.spamcop.net
- reject_rbl_client dnsbl.sorbs.net
- reject_rbl_client sbl.spamhaus.org
- reject_rbl_client relays.mail-abuse.org

To turn RBL on

1. Log on to the server and go to the Zimbra directory (su - zimbra)
2. Enter **zmprov gacf | grep zimbraMtaRestriction,** to see what RBLs are set.
3. To add any new RBL types, you must list the existing RBLs and the new RBLs all in one command as:

   zmprov mcf zimbraMtaRestriction [RBL type]

   To add all the possible restrictions, the command would be

   zmprov mcf zimbraMtaRestriction reject_invalid_hostname zimbraMtaRestriction reject_non-fqdn_hostname zimbraMtaRestriction reject_non_fqdn_sender zimbraMtaRestriction "reject_rbl_client dnsbl.njabl.org" zimbraMtaRestriction "reject_rbl_client cbl.abuseat.org" zimbraMtaRestriction "reject_rbl_client bl.spamcop.net" zimbraMtaRestriction "reject_rbl_client dnsbl.sorbs.net" zimbraMtaRestriction "reject_rbl_client sbl.spamhaus.org" zimbraMtaRestriction "reject_rbl_client relays.mail-abuse.org"

Note: *Quotes must be added to RBL types that are two words.*

Receiving and Sending Mail through Zimbra MTA

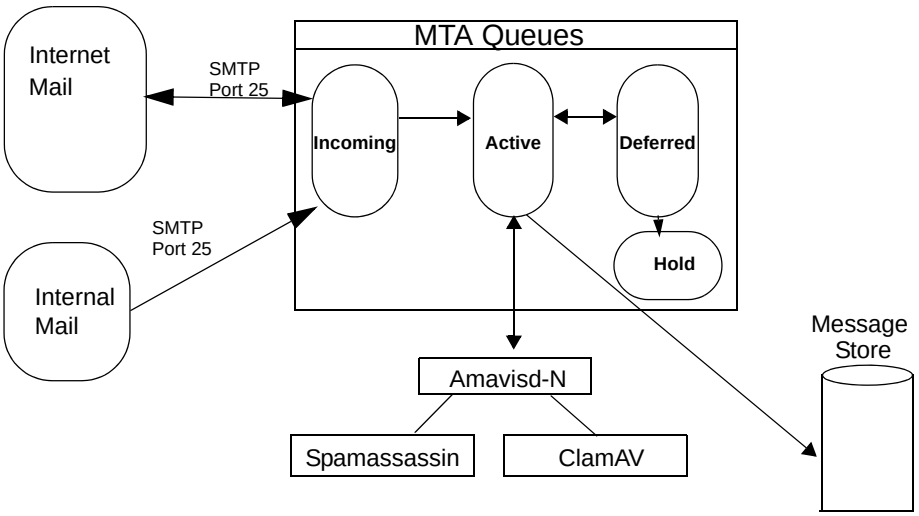
The Zimbra MTA delivers both the incoming and the outgoing mail messages. For outgoing mail, the Zimbra MTA determines the destination of the recipient address. If the destination host is local, the message is passed to the Zimbra server for delivery. If the destination host is a remote mail server, the Zimbra MTA must establish a communication method to transfer the message to the remote host. For incoming messages, the MTA must be able to accept connection requests from remote mail servers and receive messages for the local users.

In order to send and receive email, the Zimbra MTA must be configured in DNS with both an A record and a MX Record. For sending mail, the MTA use DNS to resolve hostnames and email-routing information. To receive mail, the MX record must be configured correctly to route messages to the mail server.

You must configure a relay host if you do not enable DNS. Even if a relay host is configured, an MX record is still required if the server is going to receive email from the internet.

Zimbra MTA Message Queues

When the Zimbra MTA receives mail, it routes the mail through a series of queues to manage delivery. The Zimbra MTA maintains four queues where mail is temporarily placed while being processed: incoming, active, deferred and hold.



Incoming. The incoming message queue holds the new mail that has been received. Each message is identified with a unique file name. Messages in the incoming queue are moved to the active queue when there is room in the

active queue. If there are no problems, message move through this queue very quickly.

Active. The active message queue holds messages that are ready to be sent. The MTA sets a limit to the number of messages that can be in the active queue at any one time. From here, messages are moved to and from the anti-virus and anti-spam filters before being delivered or moved to another queue.

Deferred. Message that cannot be delivered for some reason are placed in the deferred queue. The reasons for the delivery failures is documented in a file in the deferred queue. This queue is scanned frequently to resend the message. If the message cannot be sent after the set number of delivery attempts, the message fails. The message is bounced back to the original sender.

Hold. The hold message queue keeps mail that could not be processed. Messages stay in this queue until the administrator moves them. No periodic delivery attempts are made for messages in the hold queue.

Corrupt. The corrupt queue stores damaged unreadable messages.

You can monitor the mail queues for delivery problems from the administration console. See "Monitoring Mailbox Queues" on page 79.

Chapter 6 Using the Administration Console

The Zimbra administration console is the browser-based user interface used to centrally manage all Zimbra servers and user accounts.

When you install the Zimbra Collaboration Suite, one administrator's user name and password is defined during installation and this admin account is configured. The administrator can use this name and password to log on to the console immediately after the installation is complete.

Administrator Accounts

Only accounts designated as administrator can log into the administration console to manage accounts and server configurations. One administrator account is initially created when the software is installed. Additional administrator accounts can be created. All administrator accounts have equal privileges.

To give administrator privileges to an account, check the Administrator box on the General tab in the user's account.

Logging on

To start the console in a typical installation, use the following URL pattern.

https://server.domain.com:7071/

Where **server.domain.com** is the current running Zimbra server name or IP address and **default** HTTP listen port is 7071.

Enter the complete administrator address, as **admin@domain.com** and then enter the password.The initial password is configured when ZCS is installed.

Changing Administrator Passwords

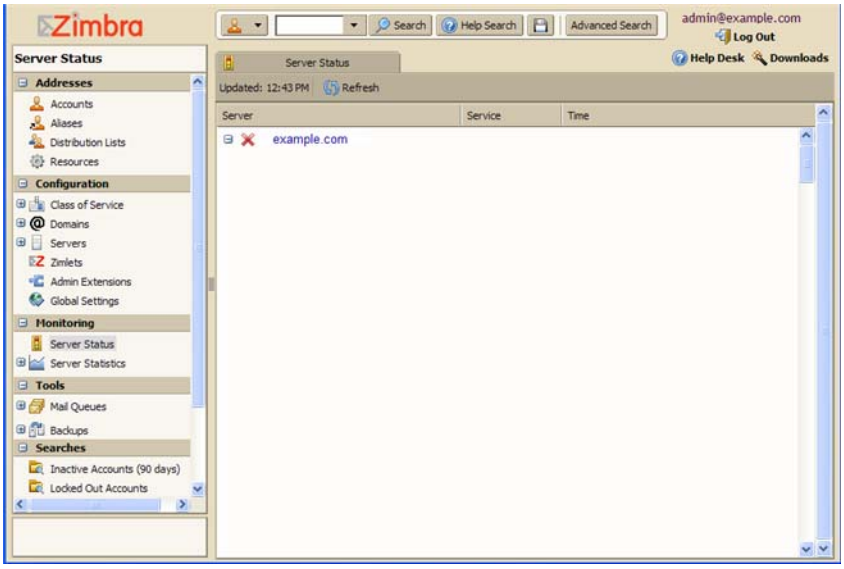
The administrator password is created when the Zimbra software is configured during installation. The password can be changed at any time from the **Accounts** toolbar. Select the account and change the password.

The administration password can also by changed using the command line utility (CLI) **zmprov setpassword**. Enter as **zmprov sp adminname@domain.com password**

About the Administration Console

If you are an administrator, when you log on to the admin console, the right pane displays the Server Status page and the navigation pane, on the left, displays all the functions exposed through the console.

Figure 7: Administration Console - First Page Displayed



The Navigation pane includes the following sections and folders:

Addresses

- **Accounts**. Lists all accounts. In the **Accounts** folder, you create and manage end-user accounts, setting options, class of service, passwords and aliases for an account.
- **Aliases**. Lists all aliases that have been created in Accounts. You can use the Move Alias feature from the toolbar to move an alias from one account to another.
- **Distribution Lists**. Lists all distribution lists. You can create new distribution lists and add or delete members of a distribution list.
- **Resources**. Lists location or equipment that can be scheduled for a meeting. You can create new resources and set the scheduling policy for the resource.

Configuration

- **Class of Service**. Lists classes of service (COS) that have been created. As a minimum, the default COS is displayed. You can create, edit, or delete COS definitions.

- **Domains**. Lists the domain in the Zimbra environment. You can create and manage domains, configure GAL, and configure the authentication mechanism to be used for that domain.
- **Servers**. Lists the servers, the host name and description. You can configure services, MTA, SMTP, IMAP, and POP features for servers.
- **Zimlets**. You can add new Zimlets, set access privileges by COS and by individual accounts and disable and uninstall Zimlets from ZCS.
- **Admin Extensions**. You can create custom modules to add to the Zimbra administration console user interface. You can use the administration console to easily upload and install your modules
- **Global Settings**. From the Global Settings folder, you set the global defaults rules for GAL search results, acceptance of incoming attachments, for MTA, POP, IMAP, anti-spam and anti-virus configuration. These default settings are used when personal options and COS settings are not set.

Monitoring

- **Server Status**. Shows the current status, either **On** or **Off,** for all servers that are running Zimbra MTA, Zimbra LDAP, Zimbra Store, SNMP, and the anti-virus service.
- **Server Statistics**. Shows both system-wide and server specific data about the inbound message volume, inbound message count, and disk usage for messages processed in the last 24 hours, the last three months, and the last year. Server specific data includes a Session tab that shows active session information for the Web Client, Administrators and IMAP, and a Mailbox Quota tab that shows quotas for individual accounts.

Tools

- **Mail Queues**. Shows the number of messages on the Zimbra MTA that are in the Deferred, Incoming, Active, and Hold queues.

Search

- **Searches**. Popular search queries, including search for inactive accounts, search for locked out accounts, search for closed accounts are available from Searches.

When you click on a folder a new tab opens in the Content pane on the right. You can have multiple tabs opened at the same time.

The area above the Content pane includes the Search function, the Help Desk and the Downloads links.

- **Search and Advanced Search** allow you to quickly find accounts, aliases, distribution lists and resources for editing.
- **Help Search** searches Zimbra's wiki, forums, and documentation. This is a powerful unified search to quickly find answers to common questions.
- Help Desk includes the Help, and links to ZCS documentation

- Downloads includes a link to download migration wizards and other migration tools.

Managing Tasks from the Administration Console

From the administration console, the global administrator can do the following:

- Create and manage end-user accounts
- Monitor server status and performance statistics
- Add or remove domains
- Create Classes of Service (COS), which are used to define group policies for accounts
- Create password policies
- Create distribution lists
- Enable or disable optional user-interface features such as conversations and address book in the email client
- Configure various global settings for security, address book, and MTAs
- Easily access the Zimbra migration tools from the administration console's downloads page.

See the Chapter 7, Managing ZCS Configurations, for information about how to configure these functions.

Tasks Not Available from Administration UI

The Zimbra command-line interface (CLI) is another method of configuring and maintaining the Zimbra system. The CLI tool set contains utilities that are not available through the administration console. The CLI options are executed on each server individually.

Use CLI command utilities for the following. See Appendix A, CLI Commands for details about the commands.

- Start and stop services, CLI **zmcontrol**
- Create self-signed certificates, CLI **zmcreatecert**
- Manage local server configuration, CLI **zmlocalconfig**
- Provision accounts in bulk, CLI **zmprov**
- Message tracing, CLI **zmmsgtrace**

Chapter 7 Managing ZCS Configurations

This chapter describes the Zimbra Collaboration Suite component configurations that you manage. The ZCS components are configured during the initial installation of the software. After the installation, you can manage the following components from either the administration console or using the CLI utility:

- Global Settings
- Domains
- Servers
- Zimlets
- Admin Extensions

Help is available from the administration console about how to perform tasks from the administration console. If the task is only available from the CLI, see Appendix A for a description of how to use the CLI utility.

Managing Global Configurations

Global Settings control global rules that apply to accounts in the Zimbra servers. The global settings are set during installation, and the settings can be modified from the administration console. A series of tabs make it easy to manage these settings.

Global settings that can be configured include:

- Defining the default domain.
- Setting the number of results returned for GAL searches.
- Setting how users view email attachments and what type of attachments are not allowed.
- Configuring authentication process, setting the Relay MTA for external delivery, enabling DNS lookup and protocol checks.
- Enabling Pop and IMAP and the port numbers. If IMAP/POP proxy is set up, making sure that the port numbers are configured correctly.
- Set the spam check controls.
- Set anti-virus options for messages received that may have a virus.

- License information, including the account limit and the number of accounts used.
-

Note: *Configurations set in Global Settings define inherited default values for the following objects: server, account, COS, and domain. If these attributes are set in the server. COS or Account set up, they override the global settings.*

General Global Settings

In the General tab configure the following**:**

- **Most results returned by GAL search** field. This sets a global ceiling for the number of GAL results returned from a user search. The default is 100 results per search.
- Default domain. The default domain displays. This is the domain that user logins are authenticated against. ----------
- **Number of threads that can simultaneously process data source imports** field. This.....

Global Attachment Settings

The **Attachments** tab can be configured with global rules to reject mail with files attached and to disable viewing files attached to mail messages in users' mailboxes. When attachment settings are configured in Global Settings, the global rule takes precedence over COS and Account settings.

The attachment settings are as follows:

- **Attachments cannot be viewed regardless of COS**. Users cannot view any attachments. This global setting can be set to prevent a virus outbreak from attachments, as no mail attachments can be opened.
- Attachments are viewed according to COS. This global settings states the COS sets the rules for how email attachments are viewed.

Reject messages with attachment extension lets you select which file types are unauthorized for all accounts. The most common extensions are listed. You can also add different extension types to the list. Messages with those type of files attached are rejected and the sender gets a bounce notice. The recipient does not get the mail message and is not notified.

Note: *Attachments settings can also be set for a Class of Service (COS) and for accounts.*

Global MTA Settings

The MTA tab is used to enable or disable authentication and configure a relay hostname, the maximum message size, enable DNS lookup, protocol checks, and DNS checks. For a description of Zimbra MTA, see Chapter 5, Zimbra MTA.

- **Authentication** should be enabled, to support mobile SMTP authentication users so that their email client can talk to the Zimbra MTA.
- **TLS authentication only** forces all SMTP auth to use Transaction Level Security to avoid passing passwords in the clear.
- **Web mail MTA Host name** and **web mail MTA port**. The MTA that the web server connects to for sending mail. The default port number is 25.
- The **Relay MTA for external delivery** is the relay host name. This is the Zimbra MTA to which Postfix relays non-local email.
- **MTA Trusted Network** is a network where mail is relayed arbitrarily. In general, MTAs must not relay mail to addresses they do not service. This creates an exception to that rule.
- Set the **Maximum messages size** for a message and it's attachments that can be received. You can check to add the **X-Originating-IP header to messages**. The X-Originating-IP header information specifies the original sending IP of the email message the server is forwarding.
- If **Enable DNS lookups** is checked, the Zimbra MTA makes an explicit DNS query for the MX record of the recipient domain. If this option is disabled, set a relay host in the Relay MTA for external delivery.
- The **Protocol** fields are checked to reject unsolicited commercial email (UCE), for SPAM control.
- The **DNS** fields are checked to reject mail, if the client's IP address is unknown, the hostname in the greeting is unknown and/or if the sender's domain is unknown.

Global IMAP and POP Settings

IMAP and POP access can be enabled as a global setting or server setting.

With POP3 (Post Office Protocol) users can retrieve their mail stored on the Zimbra server and download new mail to their computer. The user's POP configuration determines if messages are deleted from the Zimbra server.

With Internet Message Access Protocol (IMAP), users can access their mail from any computer as the mail is stored on the Zimbra server.

Configuring IMAP and POP Proxy Server

Setting up a IMAP/POP proxy server is useful for larger ZCS sites that want to present a single hostname for POP/IMAP. Enabling IMAP/POP proxy servers allows mail retrieval for a domain to be split across multiple Zimbra servers on an account basis.

Note: *An IMAP/POP proxy server should not be configured for ZCS running on a single server.*

The IMAP/POP Proxy server feature can be enabled when ZCS is installed or any time from the administration console. Both SSL and non-SSL connections can be configured.

When an IMAP or POP user enters his email address and password, the IMAP/POP proxy server searches the LDAP directory server to find which Zimbra server host the account is created on and then passes the authentication through to the appropriate mailbox server. The proxy server does not contain any data.

When the proxy server is configured, the default POP and IMAP ports are configured for the proxy server. ZCS designates the Zimbra server port numbers. These port numbers cannot be changed. When you enable a proxy server on any Zimbra server, servers that do not have the proxy server enabled must be configured with appropriate *server* port number listed in the following table.

Table 1 Zimbra IMAP/POP Proxy Server Port Mapping

	Port
IMAP Proxy port	143
IMAP SSL proxy port	993
POP proxy port	110
POP SSL proxy port	995
IMAP server port	7143
IMAP SSL server port	7993
POP server port	7110
POP SSL server port	7995

Anti-Spam Settings

Anti-spam protection can be enabled for each server when the Zimbra software is installed. The following options are configured:

- Kill percent at 75%. Mail that is scored at 75% is considered spam and is not delivered.
- Tag percent at 33%. Mail that is scored at 33% is considered spam and is delivered to the Junk folder.
- Subject prefix field is blank. The prefix entered in this field is added to the subject line for messages tagged as spam.

When a message is tagged as spam, the message is delivered to the recipient's Junk folder. Users can view the number of unread messages that are in their Junk folder and can open the Junk folder to review the messages marked as spam. If you have the anti-spam training filters enabled, when they

add or remove messages in the Junk folder, their action helps train the spam filter. See Anti-Spam Protection on page 36.

RBL (Real time black-hole lists) can be turned on or off in SpamAssassin from the Zimbra CLI. See the section To turn RBL on on page 38.

Anti-Virus Settings

Anti-virus protection is enabled for each server when the Zimbra software is installed. The global settings for the anti-virus protection is configured with these options enabled:

- **Block encrypted archives**, such as password protected zipped files.
- **Send notification to recipient** to alert that a mail message had a virus and was not delivered.

During ZCS installation, the administrator notification address for anti-virus alerts is configured. The default is to set up the admin account to receive the notification. When a virus has been found, a notification is automatically sent to that address.

By default, the Zimbra MTA checks every two hours for any new anti-virus updates from ClamAV. The frequency can be set between 1 and 24 hours.

Note: *Updates are obtained via HTTP from the ClamAV website.*

Managing Domains

One domain is identified during the installation process and additional domains can be easily added to the Zimbra system from the administration console.

For domains, you configure the Global Address List mode, the authentication mode, virtual domains and create a Domain Documents account.

General Configuration

You can configure the maximum number of accounts that the domain can have and assign a default Class of Service (COS) to the domain. This COS is automatically assigned to accounts created on the domain.

Global Address List (GAL) Mode

The Global Address List (GAL) is your company directory.

GAL is configured on a per-domain basis. The GAL mode setting for each domain determines where the GAL lookup is performed. Select one of the following GAL configurations:

- **Internal**. The Zimbra LDAP server is used for directory lookups.

- **External**. External directory servers are used for GAL lookups. You can configure multiple external LDAP hosts for GAL. All other directory services use the Zimbra LDAP service (configuration, mail routing, etc.).
- **Both**. Internal and external directory servers are used for GAL lookups.

A GAL configuration wizard steps you through configuring the GAL mode and to set the maximum number of results returned for a search in GAL.

Authentication Modes

Authentication is the process of identifying a user or a server to the directory server and granting access to legitimate users based on user name and password information provided when users log in. Zimbra Collaboration Suite offers the following three authentication mechanisms:

- **Internal**. The Internal authentication uses the Zimbra directory server for authentication on the domain. When you select Internal, no other configuration is required.
- **External LDAP**. The user name and password is the authentication information supplied in the bind operation to the directory server. You must configure the LDAP URL, LDAP filter, and wither to use DN password to bind to the external server.
- **External Active Directory**. The user name and password is the authentication information supplied to the Active Directory server. You identify the Active Directory domain name and URL.

On the administration console, you use an authentication wizard to configure the authentication settings on your domain.

Virtual Hosts

Virtual hosting allows you to host more than one domain name on a server. The general domain configuration does not change. When you create a virtual host, this becomes the default domain for a user login. Zimbra Web Client users can log in without having to specify the domain name as part of their user name.

Virtual hosts are entered on the **Domains>Virtual Hosts** tab on the administrator's console. The virtual host requires a valid DNS configuration with an A record.

To open the Zimbra Web Client log in page, users enter the virtual host name as the URL address. For example, **https://mail.company.com**.

When the Zimbra login screen displays, users enter only their user name and password. The authentication request searches for a domain with that virtual host name. When the virtual host is found, the authentication is completed against that domain.

Documents

Zimbra Documents is a document sharing and collaboration application. Users can create, organize, and share web documents. Images, spreadsheets, and other rich web content objects can be embedded into Documents via the AJAX Linking and Embedding (ALE) specification.

The Documents application consists of a Global Documents account which holds the templates, one optional domain Documents account per domain, and Documents notebooks. The Global Documents account is automatically created when ZCS is installed. The domain Documents account can be used to collect, organize, and share information with your users.

One Documents account can be created per domain. You can either add the account when you create the domain or and you can add a domain Documents account to an existing domain. When you create the account, you configure who can access this Documents account and what access rights these users can have.

The following users can be selected to access the Documents account:

- All users in the domain
- All users in all domains
- Distribution lists
- Individual accounts
- Public

Except for Public who has view-only permissions, you can select what kind of access these users can have: view , edit, remove, and add pages to the Documents notebook.You can view and change the access permissions from the administration console.

Managing Servers

A server is a machine that has one or more of the Zimbra service packages installed. During the installation, the Zimbra server is automatically registered on the LDAP server.

You can view the current status of all the servers that are configured with Zimbra software, and you can edit or delete existing server records. You cannot add servers directly to LDAP. The Zimbra Installation program must be used to add new servers because the installer packages are designed to register the new host at the time of installation.

The server settings include:

- General information about the service host name, and LMTP advertised name and bind address, and the number of threads that can simultaneously process data source imports.
- A list of enabled services

- Determining how authentication should work for the server, setting a Web mail MTA hostname different from global. Setting relay MTA for external delivery, and enabling DNS lookup if required.
- Enabling POP and IMAP and setting the port numbers for a server. If IMAP/POP proxy is set up, making sure that the port numbers are configured correctly.
- Adding and configuring new index and message volumes

Servers inherit global settings if those values are not set in the server configuration. Settings that can be inherited from the Global configuration include MTA, SMTP, IMAP, POP, anti-virus, and anti-spam configurations.

General Server Settings

The General tab includes the server display name, the server hostname, and LMTP information including advertised name, bind address, and number of threads that can simultaneously process data source imports. The Notes text box can be used to record details you want to save.

Services Settings

The Services tab shows the Zimbra services. A check mark identifies the services that are enabled for the selected server, including LDAP, Mailbox, IMAP and POP proxy, MTA, SNMP, Anti-Virus, Anti-Spam, Spell Checker, and Logger.

MTA Server Settings

From the MTA tab, you can enable or disable authentication, configure the Web mail MTA hostname, set Web mail MTA timeout, the relay MTA for external delivery, MTA trusted networks, and disable DNS lookup for the server.

IMAP and POP Server Settings

From these tabs, you can configure IMAP and POP availability on a per server basis.

Volume Settings

The Volume tab can be used to manage storage volumes on your Zimbra Mailbox server. When Zimbra Collaboration Suite is installed, one index volume and one message volume are configured on each mailbox server. You can add new volumes, set the volume type, and set the compression threshold

Index Volume

Each Zimbra mailbox server is configured with one current index volume. Each mailbox is assigned to a permanent index directory on the current index volume. When an account is created, the current index volume is automatically defined for the account. You cannot change which index volume the account is assigned.

As volumes become full, you can create a new current index volume for new accounts. When a new current index volume is added, the older index volume is no longer assigned new accounts.

Index volumes not marked current are still actively in use as the index volumes for accounts assigned to them. Any index volume that is referenced by a mailbox as it's index volume cannot be deleted.

Message Volume

When a new message is delivered or created, the message is saved in the current message volume. Additional message volumes can be created, but only one is configured as the current volume where new messages are stored. When the volume is full, you can configure a new current message volume. The current message volume receives all new messages. New messages are never stored in the previous volume.

A current volume cannot be deleted. and message volumes that have messages referencing the volume cannot be deleted.

Managing Other Functions

Zimlets

Zimlets can be deployed and undeployed from the administration console. The Zimlets pane lists all the Zimlets that are installed and shows whether the Zimlet is enabled or not. You can configure the COS and individual accounts to allow access to Zimlets. See the Working with Zimlets chapter for information about Zimlets.

Admin Extensions

You can create custom modules to add to the Zimbra administration console user interface. You can use the administration console to easily upload and install your modules.

Note: *Go to the Zimbra wiki, Extending Admin UI for documentation about how to create an extended admin UI module.*

Backing Up the System

Backing up the mailbox server on a regular basis can help you quickly restore your email service if there is an unexpected crash. You should include backing up the Zimbra server in your system-wide backup process. Only full backups of the Zimbra data can be created.

Before backing up the Zimbra data, all servers must be stopped. To stop the servers, use the CLI command, **zmcontrol stop**. After the backup is complete, to restart the servers, use **zmcontrol start**. See Appendix A, for more information about these command.

To restore the Zimbra data, you must delete the existing data and then restore the backup files. The servers must be stopped before restoring the data.

Chapter 8 Customizing Accounts, Setting General Preferences and Password Rules

When an account is provisioned, you create the mailbox, assign the email address, and enable Zimbra applications and features. You also set general preferences, the policy for password usage, and select a theme as the initial appearance of Zimbra Web Client.

This chapter describes the features and user preferences that can be configured for an account either from the assigned COS or in individual accounts.

ZCS offers two Zimbra Web Client options. Both Web clients include mail, calendar, and address book functionality. Users can choose which view when they log in and they can select their preference in their account Options tab.

- Advanced Web Client includes Ajax capability and offers a full set of Web collaboration features. This Web client works best with newer browsers and fast internet connections.
- Standard Web Client is a good option when Internet connections are slow or users prefer HTML-based messaging for navigating with their mailbox.

Note: *Mailbox features are enabled for the Zimbra Web Client users. When IMAP or POP clients are used, users may not have these features available.*

Zimbra Messaging and Collaboration Applications

The Zimbra Collaboration Suite provides the following messaging and collaboration solutions:

- Email messaging
- Calendaring
- Address Books
- Tasks
- Documents for Web document authoring
- Briefcase
- Instant Messenger (Beta)

You can enable and disable these applications by either Class of Server (COS) or by individual accounts.

Configuring the COS and assigning a COS to accounts lets you configure the default settings for account features and restrictions for groups of accounts. Individual accounts can be configured differently and any changes you make override the COS setting. When you update the COS, the changes are not reflected in accounts that have COS overrides.

Email messaging

Zimbra email messaging is a full-featured email application that includes advanced message search capabilities, mail sorted by conversations, tags, user-defined folders, user-defined filters, and more. You configure which email messaging features are enabled.

Messaging features that can be enabled are listed below; the third column is the tab where the feature can be enabled. Many of these features can than be managed from the users' account Options tabs when they log on to the Zimbra Web Client.

Feature Name	Description	COS/ Account Tabs
Mail	Enables the email application. This is enabled by default.	Features
Conversations	Messages can be displayed grouped into conversations or as a message list. Conversations group messages by subject. If this feature is turned on, conversation view is the default. Users can change the default from their account Options tabs.	Features
HTML compose	Users can compose email messages with an HTML editor. They can specify their default font settings for HTML compose in their account Options tabs.	Feature
Email message lifetime	Number of days a message can remain in any folder before it is automatically purged. The default is 0; email messages are not deleted.	Advanced
Trashed message lifetime	Number of days a message remains in the Trash folder before it is automatically purged. The default is 30 days.	Advanced

Spam message lifetime	Number of days a message can remain in the Junk folder before it is automatically purged. The default is 30 days.	Advanced
Users can see the email deletion rules from their Options, Mail tab.		
Allow the user to specify a forwarding address	Users can create a forwarding address for their mail. When this feature is enabled in the COS, in the account configuration, you can specify a default forwarding address that the user can use and enable the function so that a copy of the forwarded message is not saved in the users mailbox. Users can change the information from their account Options tab. In the account configuration, you can also specify forwarding addresses that are hidden from the user. A copy of each message sent to the account is immediately forwarded to the designated forwarding address.	Features tab in COS Forwarding tab in Accounts
Out-of-office reply	Allows users to set up an away-message and turn it on or off from their account Options tab.	Features
New mail notification	Allows users the option to specify an address where to be notified of new mail to their ZWC account. They can turn this feature on or off and designate an address from their account Options tab. An email with information about the email's subject, sender address and recipient address is sent to the address. **Note**: See zmprov (Provisioning) on page 94 in Appendix A CLI commands, for information about how to change the email template.	Features tab in COS Preferences tab in Accounts
Maximum length of mail signature	You can set the maximum number of characters that can be in a signature. The default is unlimited length.	Preferences

Mail Identities	The name and address configured for the account creates the default mail identity. When Mail Identities is enabled, users can create additional account names to manage different roles. Each account name can include a different email address. Users set up these accounts from their Options tab. Note: To let users create email addresses for mail identities, on the Preferences tab, check **Allow sending email from any address**. If this is not enabled, users can only select from email addresses or aliases that you have configured.	Features and Preferences tab for additional option
Advanced Search	Users can build a complex search by date, domain, status, tags, size, attachment, Zimlets, and folders.	Features
Saved searches	Users can save a search that they have previously executed or built.	Features
External POP3 access	Users can set up to retrieve their POP accounts' email messages directly from their ZWC account. They can add the external account address to their account settings. Users can set these up from their Options tab.	Features
Aliases for this account	You can create an aliases for the account. Users cannot change this.	Alias tab in Accounts
Mail filters	Users can define a set of rules and corresponding actions to apply to incoming mail. When an incoming email message matches the conditions of a filter rule, the corresponding actions associated with that rule are applied. Users set up these rules from their account Options tab.	Features
Tagging	Users can create tags and assign them to messages, contacts, and Documents pages.	Feature

Navigation Shortcuts	Users can use keyboard shortcuts within their mailbox, and they can create their own shortcut key combinations for mail folders, searches, and tags from their account Options tab.	Features
GAL access	Users can access the company directory to find names for their email messages.	Features
Autocomplete from GAL	When this is enabled, users enter a few letters in their compose header and names listed in the GAL are displayed. Users can turn this feature on or off from their Options tab.	Features
IMAP access	Users can use third party mail applications, such as Thunderbird or Outlook, to access their mailbox using the IMAP protocol.	Features
POP3 access	Users can use third party mail applications, such as Thunderbird or Outlook, to access their mailbox using the POP protocol. When they retrieve their POP email messages, the messages and attachments are saved on the Zimbra server.	Features

The default behavior for many of these preferences can be set from either the COS or the Accounts Preferences tab. Users can modify the following mail preferences from their account Options Mail tab.

- Number of items to display on a page: 10, 25, 50, 100
- How often, in minutes, that the Web Client checks for new messages
- Whether to show the reading pane when viewing messages
- Which folder should be searched first when running a search
- Whether to save copies of outbound messages to the Sent folder
- Whether to save a local copy of a message that is forwarded or to have it deleted from their mailbox
- Whether to compose messages in a separate window
- Whether to view mail as HTML for messages that include HTML or to view messages as plain text

Important: *To allow users to share their mailbox folders, address books, calendars, and Documents notebooks, enable Sharing in the Features tab.*

Users can modify the following mail preferences from their Options Account tab.

- Whether to automatically append a signature to outgoing messages and what the signature should include.
- Preferences for how messages that are replied to or forwarded are composed.

Address Book

Zimbra Address Book allows users to create multiple contact lists and add contact names automatically when mail is received or sent. By default, a Contacts list and an Emailed Contacts list are created in Address Book. Users can import contacts into their Address Book.

When you create an account you can configure this feature and set a limit to the number of contacts in the address book.

Important: *To allow users to share their address books, calendars, and Documents notebooks, enable Sharing on the Features tab.*

Feature Name	Description	COS/ Account Tabs
Address Book	Users can create their own personal contacts lists. By default, two contact lists folders are in the Address Book.	Features
Address book size limit	Maximum number of contacts a user can have in all address books.	Advanced

Users can modify the following Address Book preferences from their account Options Address Book tab. The default behavior can be set from the COS or Accounts>Preferences tab.

- Enable auto adding of contacts to automatically add contacts to their Emailed Contact list when they send an email to a new address.
- Default view for their contacts, a list or as cards.
- Number of contacts to display per page, 10, 25, 50, 100.

Users can import other contact lists into their Address Book and can export their different address books. The files must be .csv files.

Calender

Zimbra Calendar lets users schedule appointments and meetings, establish recurring activities, create multiple calendars, share calendars with others, and delegate manager access to their calendars. They can subscribe to external calendars and view their calendar information from Zimbra Web Client.

Important: *To allow users to share their calendars, address books, and Documents notebooks, enable Sharing in the Features tab.*

Feature Name	Description	COS/ Account Tabs
Calendar	A calendar and scheduling tool to let users maintain their calendar, schedule meetings, delegate access to their calendar, create multiple personal calendars, and more.	Features
Group Calendar	Must be enabled to have all the Calendar functionality. When this is not checked, the only Calendar feature is the ability to create personal appointments.	Features
Timezone	Set the timezone that is used in the calendar scheduling. A drop down list displays the timezone.	Preferences

Users can modify the following Calendar preferences from their account Options Calendar tab. The default behavior can be set from the COS or Accounts Preferences tab.

- Calendar view they want to see by default, Day, Work Week, 7-Day Week, Month, or Schedule.
- First day of the week to display in the calendar.
- Time-zone list in their appointment dialog, giving them the opportunity to change time zones while making appointments.
- Use the QuickAdd dialog to create appointments from the calendar view. When this option is enabled, the QuickAdd dialog displays when users double-click or drag on the calendar.
- Display the mini-navigation calendar in the Mail view. The mini-calendar automatically displays in the Calendar view.
- Number of minutes before an appointment to be reminded.

Tasks

Zimbra Tasks lets users create to-do lists and manage tasks through to completion. They can add tasks to the default Tasks list and they can create additional task lists to organize to-do lists by more specific activities.

Important: *To allow users to share their Task lists, enable Sharing in the Features tab. Task lists can be shared with individuals, groups, and the public.*

The Tasks feature is enabled from either the COS or the Accounts Preferences tab.

Feature Name	Description	COS/ Account Tabs
Tasks	Users can create and organize tasks from the Zimbra Web Client.	Features

Documents

Zimbra Documents lets users create, organize, and share web documents from the Zimbra Web Client.

Important: *To allow users to share their Documents notebooks, enable Sharing on the Features tab. Notebook can be shared with individuals, groups, and the public.*

When this feature is enabled, users have one Documents Notebook folder by default and can create additional notebooks. Zimbra Documents provides a web-based WYSIWG tool for editing documents and other content. Users have the ability to embed rich content into an editable document from within a Web browser.

You can also create a specific domain Documents account from the administration console. This Documents notebook can be shared with users on the domain, users on all ZCS domains in your environment, as well as individuals and groups. See Managing ZCS Configurations,Documents on page 51.

The Documents feature is enabled from either the COS or the Accounts Preferences tab.

Feature Name	Description	COS/ Account Tabs
Documents	Users can create and organize web documents from the Zimbra Web Client. One Documents Notebook is created for each account. Users can create additional notebooks and pages.	Features

General Configuration Settings for Accounts

The general configuration options include

- Setting the quota for accounts
- Setting the password policy and failed logon policy
- Setting account session length
- View Attachments settings
- ZWC UI theme to display
- Zimlets to enable for accounts

Setting Account Quotas

You can specify mailbox quotas and the number of contacts allowed for each account through the Zimbra administration console.

Account quota is the amount of space in megabytes that an account can use. The quota includes email messages, Calendar meeting information, and Documents pages. When the quota is reached, all email messages are rejected and users cannot add to their Calendars or Documents. You can view mailbox quotas from the administration console, Monitoring, Server Statistics.

Users can be notified that their mailboxes is reaching the quota before they reach their maximum mailbox size. You set the quota percentage threshold quota and when this threshold is reached an quota warning message is sent to the user. The quota percentage threshold can be set and the warning message text can be configured in the Advanced tab settings for COS and accounts. If you set the quota to 0, accounts do not have a quota.

You can view mailbox quotas from the administration console, Monitoring, Server Statistics. See Setting Account Quotas in the Managing End-User Mailbox Features chapter.

The Address Book size limit field sets the maximum number of contacts a user can have across all of their address books. When the number is reached, users cannot add new contacts.

Setting Password Policy

If internal authentication is configured for the domain, you can configure ZCS to require users to create strong passwords.

Important: *If Microsoft Active Directory (AD) is used for user authentication, you must disable the Change Password feature in their COS. The AD password policy is not managed by ZCS.*

The password settings that can be configured are listed below.

Feature Name	Description	COS/ Account Tabs
Minimum/Maximum password length	This specifies the required length of a password. The default minimum length is 6 characters. The default maximum length is 64 characters.	Advanced
Minimum / Maximum password age	Configuring a minimum and maximum password age sets the password expiration date. Users can change their passwords at any time between the minimum and maximum set. They must change it when the maximum password age is reached.	Advanced
Configuring the next settings will require users to create more complex passwords. **Note**: A password cannot included accented characters in the string. Example of accented characters that cannot be used: ã, é, í, ú, ü, ñ.		
Minimum upper case characters	Upper case A - Z	Advanced
Minimum lower case characters	Lower case a - z	Advanced
Minimum punctuation symbols	Non-alphanumeric, for example !, $, #, &, %	Advanced
Minimum numeric characters	Base 10 digits 0 - 9	Advanced
Enforce password history	Number of unique new passwords that a user must create before he can reuse an old password.	Advanced

Password locked	Users cannot change their passwords.This should be set if authentication is external.	Advanced
Must change password	When a user logs in, he is required to change his password.	General Information
Change password	When this is enabled, users can change their password at any time within the password age settings from their account Options tabs.	Features

Setting Failed Login Policy

You can specify a policy that sets the maximum number of failed login attempts before the account is locked out for the specified lockout time. This type of policy is used to prevent password attacks.

Feature Name	Description	COS/ Account Tabs
Enable failed login lockout	When this box is checked, the “failed login lockout” feature is enabled and you can configure the following settings.	Advanced
Number of consecutive failed logins allowed	The number of failed login attempts before the account is locked out. The default is 10 attempts. If this is set to 0, an unlimited number of failed log in attempts is allowed. This means the account is never locked out.	Advanced

Time to lockout the account	The amount of time in seconds, minutes, hours, or days the account is locked out. If this is set to 0, the account is locked out until the correct password is entered, or the administrator manually changes the account status and creates a new password. The default is 1 hour.	Advanced
Time window in which the failed logins must occur within to lock the account	The duration of time in seconds, minutes, hours, or days after which the number of consecutive failed login attempts is cleared from the log. The default is 0, the user can continue attempts to authenticate, no matter how many consecutive failed login attempts have occurred.	Advanced

Setting Session Lifetime

You can set how long a user session should remain open and when to close a session because the session is inactive.

Feature Name	Description	COS/ Account Tabs
Auth token lifetime	Auth token lifetime sets a browser cookie that contains the auth token. User can open ZWC without having to log on again until the auth token expires. The default is 2 days.	Advanced
Session idle lifetime	Session idle lifetime sets how long a user session remains active, if no activity occurs. Activity includes any clickable mouse action, such as viewing contents of a folder or clicking a button. The default is 2 days.	Advanced

Zimbra Web Client UI Themes

The appearance of the Zimbra Web Client user interface can be changed. A number of Zimbra themes are included with ZCS, and you can create others. You can select a theme to be the default and the themes that users can select from to customize their user experience.

Note: *To learn more about themes, go to the Rebrandiing and Themes section of the Zimbra Wiki.*

Change UI themes	When this is enabled, users can select different UI themes to display ZWC. Select the theme types that are available from the Themes tab.	Features

The following theme usage options can be configured either from COS or by individual accounts:

- **Limit users to one theme**. On the Features tab, remove the check mark from **Change UI Themes**. The ZWC theme is the theme listed in **Current UI theme** field on the Themes tab.
- **Let users access any of the installed Zimbra themes**. If the **Change UI Themes** is checked, users can access any of the themes that are listed in the **Available UI themes** list.

Configuring Zimlets for Accounts

Zimlets™ is a mechanism for integrating the Zimbra Collaboration Suite with third party information systems and content. See Chapter 9, Working with Zimlets.

You can add new Zimlets from the administration console and set access privileges from the COS and the Account Zimlets tab. Zimlets that are deployed are listed on the Zimlets tab. To disable access to a Zimlet, you can remove Zimlets from the Zimlets tab's Available Zimlets list.

ZCS includes pre configured Zimlets that enhance the user experience while working in the Zimbra Web Client. These Zimlets are already deployed and made available from the COS.

- **com_zimbra_date**. When users click on a date either in the email or on the mini-calendar, their calendar schedule for that date displays.
- **com_zimbra_email**. Users can see complete contact information if it is available in their address books.
- **com_zimbra_url**. Users can see a thumbnail of the website that is listed in an email message if it is available. They see the screen below if it is not available..
- **com_zimbra_phone**. Users can click on a phone number that displays in any of the application pages to quickly call that number if they have the installed a VOIP software application such as Skype or Cisco VOIP. When they click on the phone number, the VOIP application is launched.

Chapter 9 Working with Zimlets

Zimbra Collaboration Suite created Zimlets™ as a mechanism to integrate ZCS with different third-party applications to enhance the user experience from the Zimbra Web Client. When a Zimlet is added to the ZCS, users can look at information and interact with the third-party application from within their email messages. With Zimlets, arbitrary message content can be made live by linking it with Web content and services on intranets or the Internet.

Mousing over actionable content gives the user a real-time preview (subject to security constraints) that can be factored in decision making. For example, various Zimlets can be enabled to let users preview the following:

- Mouse over a date or time and see what is in their calendar
- Mouse over a name or email address and see details from the address book for this name
- Right-click on a phone number to make a call with your soft-phone
- Right-click on a date to schedule a meeting
- Right-click on a name, address, or phone number to update thier address book

Several pre-defined Zimlets are included with ZCS, and you can create other Zimlets so that users can interact with your company resources or other defined applications from the Zimbra Web Client. For more information about creating Zimlets, see the *Zimlets - A Mechanism for Integrating Disparate Information Systems and Content with the Zimbra Collaboration Suite* specification. A copy is available on the Zimbra website, www.zimbra.com.

This chapter describes how to deploy, configure, and manage Zimlets on the Zimbra server. The Zimlets that are included with Zimbra Collaborating Suite are described at the end of this chapter.

Setting Up Zimlets in ZCS

Zimlets are delivered as a zip file that includes all the files necessary to run the Zimlet. The zip file is copied to the Zimbra servers and the administrator can use the Zimlet Management Tools from either the administration console or from the command line (CLI) to deploy the Zimlet to users. You can configure Zimlets only from the command line.

You can see a list of Zimlets that are installed on the Zimbra server, and which are enabled or disabled on the LDAP server from the administration console Zimlets pane or by entering the following CLI command.

Type **zmzimletctl listZimlets** to view the status of installed Zimlet files.

When you view the information from the command line, you also the which COS make the Zimlets available.

Managing Zimlets from the Administration Console

You can manage the following Zimlet management tasks from the ZCS administration console

- Deploy a Zimlet, which creates the Zimlet entry in the LDAP server, installs the Zimlet files on the server, enables the Zimlet and makes the Zimlet available to the members of the default COS.
- Make a Zimlet available or not available per COS or account.
- Disable a Zimlet, which leaves it on the server, but the Zimlet is not used.
- Undeploy a Zimlet, which removes it from the COS listings and the Zimlets list but does not uninstall the Zimlet from the server.

You cannot uninstall the Zimlet from the administration console.

See the administration console Help for more information about managing Zimlets on the administration console.

Managing Zimlets from the Command Line

The Zimlet zip file should be copied to each Zimbra server where it will be deployed.

To deploy a Zimlet to the default COS

1. Copy the zip file to the **/opt/zimbra/zimlets** directory.
2. Type the following command

   zmzimletctl deploy <zimlet.zip file name>

Deploying the Zimlet creates the Zimlet entry in the LDAP server, installs the Zimlet files on the server, grants access to the members of the default COS, and turns on the Zimlet. The Zimlet is displayed on the administration console Zimlets page.

Running **zmzimletctl deploy** is equivalent to running the following four commands.

- **zmzimletctl install**
- **zmzimletctl ldapDeploy**
- **zmzimletctl acl default grant**

- **zmzimletctl enable**

To deploy a Zimlet to a COS other than default

To deploy a Zimlet to one or more COSs other than default, first install the Zimlet, then adjust the ACL on the COSs.

1. Copy the zip file to the **/opt/zimbra/zimlets** directory.
2. Type the following command

   zmzimletctl deploy <zimlet.zip file name>

   This creates the Zimlet entry in the LDAP server, installs the Zimlet files on the server, grants access to the members of the default COS, and turns on the Zimlet.
3. To add the Zimlet to other COSs and grant access, type

   zmzimletctl acl <zimletname> <cosname1> grant

   You can grant access to more than one COS on the same command line. Enter as **zmzimletctl acl <zimletname> <cosname1> grant <cosname2> grant**

Note: *To turn off access to Zimlets in the default COS, type* **zmzimletctl acl <zimletname> default deny**

Configuring a Zimlet

Some Zimlets may require additional configuration after they are deployed to configure additional information. Your developer will let you know if this is necessary.

The Zimlet Management Tool provides the means for setting up a special Zimlet configuration. You make the configuration changes on the configuration template and then install the new configuration file on the Zimbra server.

How to Change Zimlet Configurations

1. To extract the configuration template type

   zmzimletctl getConfigTemplate <zimlet.zip>

   The config_template.xml is extracted from the Zimlet. zip file.
2. Make the required changes in the template. Be careful to only change the required areas. Save the file.

   Note: *If you have more than one custom Zimlet, you should rename the config_template.xml file before updating the configuration in LDAP so that files are not overwritten.*
3. Type the following command to update the configuration in the LDAP. If you changed the name of the configuration template, replace **config_template.xml** with the new name.

   zmzimletctl configure config_template.xml

Disabling or Removing a Zimlet

You can turn off access to a Zimlet from a COS, disable the Zimlet, or remove the Zimlet from the server.

To turn off access from a COS

Type **zmzimletctl acl <zimletname> <cosname> deny**

To disable a Zimlet on the Zimbra server

Type **zmzimletctl disable <zimletname>**

Note: *To enable a disabled Zimlet, type* **zmzimletctl enable <zimletname>.**

To uninstall and remove a Zimlet from the Zimbra server

When a Zimlet is undeployed, it is removed from all COSs and then removed from LDAP.

Type **zmzimletctl undeploy <zimletname>**

The Zimlet and all associated files are uninstalled.

Remove the Zimlet file from **/opt/zimbra/zimlets**

Important: *Only remove your custom Zimlets. You should not remove Zimlets that are shipped with the Zimbra Collaboration Suite. If you do not want to have the ZCS Zimlets available, disable them.*

Zimlets Included with ZCS

Zimbra Collaboration Suite includes preconfigured Zimlets when ZCS is installed. Some of these Zimlets enhance the user experience while in their email messages, letting them click on the following type of text.

- **Dates**, to see their calendar schedule for that date.
- **Email addresses/names**, to see complete contact information, if available.
- **URLs**, to see a thumbnail of the website.
- **Phone numbers**, to quickly place a call. VOIP software such as Skype or Cisco VOIP phone must be installed on the user's computer. The user can click the phone number in the message to immediately make a call.

When users right-click on these Zimlets within their messages, additional actions are available. The above Zimlets do not require any configuration to work.

You can disable these Zimlets but do not remove them from ZCS.

To see the latest documentation about specific Zimlets, go to the Zimbra Wiki, ZCS Community, Zimlet page.

Chapter 10 Monitoring Zimbra Servers

The Zimbra Collaboration Suite includes the following to help you monitor the Zimbra servers, usage, and mail flow:

- Zimbra Logger package to capture and display server statistics and server status, for message tracing, and to create nightly reports
- Mailbox quota monitoring
- MTA mail queue monitoring
- Log files

Also, selected error messages generate SNMP traps, which can be monitored using an SNMP tool.

Note: *Checking the overall health of the system as a whole is beyond the scope of this document.*

Zimbra Logger

Zimbra-Logger includes tools for syslog aggregation, reporting, and message tracing. Installing the Logger package is optional, but if you do not install Logger, Server Statistics and Server Status information is not captured and message tracing is not available.

In environments with more than one Zimbra server, Logger is enabled on only one mailbox server. This server is designated as the monitor host. The Zimbra monitor host is responsible for checking the status of all the other Zimbra servers and presenting this information on the Zimbra administration console. The information updates every 10 minutes.

Note: *In a multi-server installation, you must set up the syslog configuration files on each server to enable logger to display the server statistics on the administration console, and you must enable the logger host. If you did not configure this when you installed ZCS, do so now.*

To enable Server Statistics:

1. On each server, as root, type **/opt/zimbra/bin/zmsyslogsetup**. This enables the server to display statistics.

2. On the logger monitor host, 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/syslogd stop**.
   c. Start the syslog daemon. Type **/etc/init.d/syslogd start**.

Note: *These steps are not necessary for a single-node installation.*

Reviewing Server Status

The **Server Status** page lists all servers and services, their status, and when the server status was last checked. The servers include the MTA, LDAP, and mailbox server. The services include MTA, LDAP, Mailbox, SNMP, Anti-Spam, Anti-Virus, Spell checker, and Logger.

To start a server if it is not running, use the **zmcontrol** CLI command. You can stop and start services from the administration console, **Servers**>**Services** tab.

Server Performance Statistics

The **Server Statistics** page shows bar graphs of the Message Count, Message Volume, Anti-Spam, and Anti-Virus activity for all servers. You can select a specific server to see that server's statistics. T

This information is displayed for the last 48 hours, and 30, 60, and 365 days.

- **Message Count** displays the number of messages sent and received per hour and per day.
- **Message Volume** displays the aggregate size in bytes of messages sent and receive per hour and per day.
- **Anti-Spam/Anti-Virus Activity** displays the number of messages that were checked for spam or viruses and the number of messages that were tagged as spam or deemed to contain a virus.

The Message Count and the Anti-spam/Anti-virus Activity graphs display a different message count because:

- Outbound messages may not go through the Amavisd filter, as the system architecture might not require outbound messages to be checked.
- Message are received and checked by Amavisd for spam and viruses before being delivered to all recipients in the message. The message count shows the number of recipients who received messages.

Server specific statistics also include the following tabs:

- **Disk** displays the disk usage and the disk space available for individual servers. The information is displayed for the last hour, day, month and year.

- **Session** displays information about the active Web Client, Administrator and IMAP sessions. You can see how many active sessions are opened, who is logged on, when the session was created and the last time the session was accessed.
- **Mailbox Quota** displays account name and quota information. See Monitoring Mailbox Quotas on page 81.

Tracing Messages

You can trace an email message that was sent or received within the last 30 days.

Each email message includes a header that shows the path of an email from its origin to destination. This information is used to trace a message's route when there is a problem with the message. The Zimbra email message header can be viewed from the Zimbra Web Client Message view. Right-click on a message and select **Show Original**.

The following lines in the header can be used to trace a message:

- **Date** - The date and time the message was sent. When you specify time, you can specify range by adding start and stop time to search for messages.
- **From** - The name of the sender and the email address
- **To** - The name of the recipient and the email address
- **Message-ID** - Unique number used for tracing mail routing
- **Received: from** - The name and IP address the message was sent from. The header displays Received: from information from the MTA to the LMTP and from the local host.

The CLI utility, **zmmsgtrace** is run to find email messages by the follow:

• Date and time, setting a start and stop time range is optional	**-t yyyymmdd(hhmmss)**
• Sender address (From)	**-s [sender_addr]**
• Recipient address (To)	**-r [rcpt_addr]**
• Message ID	**-i [msd_id]**
• IP Address sent from	**-F [ip_address]**
• Destination IP/Host	**-D [ip_address/name]**

Note: *If messages are viewed by Conversation view, open the conversation to view the messages. Then select the message and right-click to select Show Original.*

Examples

Message trace is run from the Zimbra monitor host, which is the server where Logger is enabled.

- Message trace, if you know the message ID:

  zmmsgtrace -i 3836172.14011130514432170

- Message trace, if you know the recipient, sender, and date range to search:

  zmmsgtrace -s user@example.com -r user2@example2.com -t 20051105, 20051115

The following message trace example was looking for messages sent from sender, jdoe, to recipient address, aol.com, any time within the last 30 days. The details show that two messages were sent, and it shows to whom the messages were sent.

```
$ zmmsgtrace -s jdoe -r aol.com
Tracing messages
from jdoe
to aol.com


Message ID
17357409.1128717619728.JavaMail.companya@example.com
jdoe@example.com -->
kumsh@aol.com
Recipient kumsh@aol.com
2005-01-07 13:40:19 - example.com (10.10.000.20) -->
2005-01-07 13:40:20 - example --> 000.0.0.1 (100.0.0.0)
status sent
2005-01-07 13:40:20 Passed by amavisd on example (CLEAN)
HITS: -5.773 in 539 ms
2005-01-07 13:40:20 - localhost.localdomain (100.0.0.1) -->
example
2005-01-07 13:40:20 - example --> mta02.example.com
(0.00.000.00) status sent

Message ID
3836172.14011130514432170.JavaMail.root@example.com
jdoe@example.com -->
harma@aol.com
lt@hotmail.com
Recipient harma@aol.com
2005-01-28 08:47:13 - localhost.localdomain (000.0.0.1) -->
example
2005-01-28 08:47:13 - example --> mta02.example.com (
0.70.000.09) status sent

2 messages found
```

Generating Daily Mail Reports

When the Logger package is installed, a daily mail report is automatically scheduled in the crontab. The Zimbra daily mail report includes the following information:

- Errors generated from the Zimbra MTA Postfix logs
- Total number of messages that moved through the Zimbra MTA

- Message size information (totals and average bytes per message)
- Average delay in seconds for message delivery
- Total number of bounced deliveries
- Most active sender accounts and number of messages
- Most active recipient accounts and number of messages

The report runs every morning at 4 a.m. and is sent to the administrator's email address.

You can configure the number of accounts to include in the report. The default is 50 sender and 50 recipient accounts.

To change the number of recipients to add to the report, type:

zmlocalconfig -e zimbra_mtareport_max_recipients=<number>

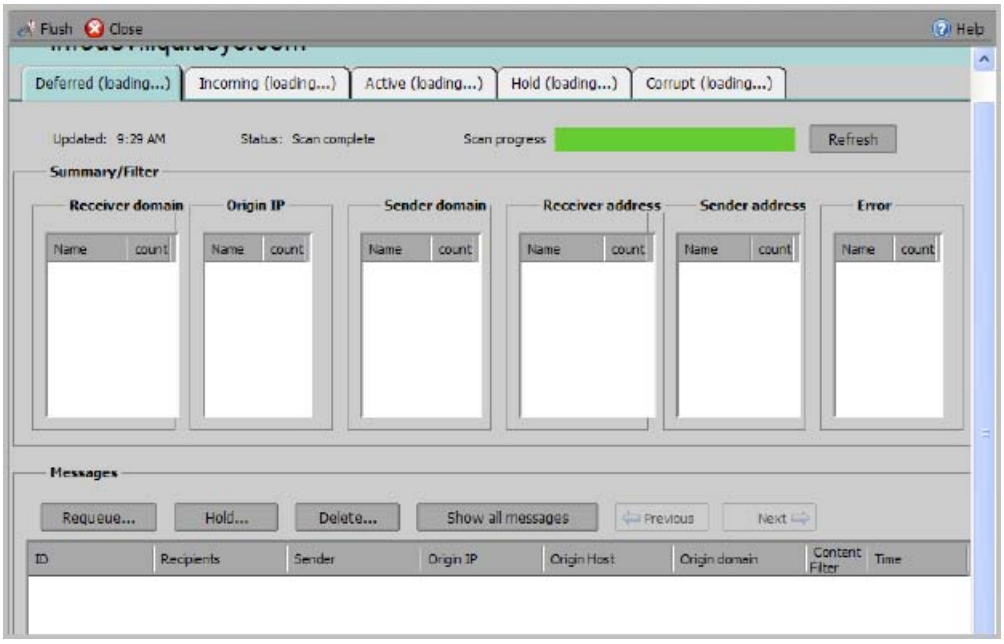
To change the number of senders to add to the report, type:

zmlocalconfig -e zimbra_mtareport_max_senders=<number>

Monitoring Mailbox Queues

If you are having problems with mail delivery, you can view the mail queues from the administration console Monitoring Mail Queues page to see if you can fix the mail delivery problem. When you open mail queues, the content of the Deferred, Incoming, Active, Hold, and Corrupt queues at that point in time can be viewed. You can view the number of messages and where they are coming from and going to. For description of these queues, see Zimbra MTA Message Queues on page 39.

Figure 8: Mailbox Queue Page



For each queue, the Summary pane shows a summary of messages by receiver domain, origin IP, sender domain, receiver address, sender address, and for the Deferred queue, by error type. You can select any of the summaries to see detailed envelope information by message in the Messages pane.

The Messages pane displays individual message envelope information for search filters selected from the Summary pane.

The the following Mailbox Queue functions can be performed for all the messages in a queue:

- **Hold**, to move all messages in the queue being viewed to the Hold queue. Messages stay in this queue until the administrator moves them.
- **Release**, to remove all message from the Hold queue. Messages are moved to the Deferred queue.
- **Requeue** all messages in the queue being viewed. Requeuing messages can be used to send messages that were deferred because of a configuration problem that has been fixed. Messages are re-evaluated and earlier penalties are forgotten.
- **Delete** all messages in the queue being viewed.

The Zimbra MTA, Postfix queue file IDs are reused. If you requeue or delete a message, note the message envelope information, not the queue ID. It is possible that when you refresh the mail queues, the queue ID could be used on a different message.

Flushing the Queues

In addition to moving individual messages in a specific queue, you can flush the server. When you click the Flush button, delivery is immediately attempted for all messages in the Deferred, Incoming and Active queues.

Monitoring Mailbox Quotas

You can view the mailbox quota for all accounts from the administration console in Monitoring>Server Statistics>Mailbox Quota tab. The Mailbox Quota tab gives you an instant view of the following information for each account:

- Mailbox quota allocated
- Disk space used
- Percentage of quota used

When an account quota is reached all mail messages are rejected. Users will need to delete mail off the server to get below their quota limit, or you can increase their quota.

From a COS or Account, you can configure a quota threshold that when reached, triggers sending a warning message alerting users that they are about to reach their mailbox quota.

Log Files

The Zimbra Collaboration Suite logs its activities and errors to a combination of system logs through the syslog daemon as well as Zimbra specific logs on the local file system. The logs described below are the primary logs that are used for analysis and troubleshooting.

Local logs containing ZCS activity are in the **/opt/zimbra/log** directory.

- **audit.log**. This log contains authentication activity of users and administrators, as well as mail delivery, login failure, and mailboxd start/stop activities.
- **clamd.log**. This log contains activity from the antivirus application clamd.
- **freshclam.log**. This log contains log information related to the updating of the clamd virus definitions.
- **logger_myslow.log**. This slow query log consists of all SQL statements that took more then long_query_time seconds to execute. Note: long_query_time is defined in /opt/zimbra/my.logger.cnf.
- **mailbox.log**. This log is a mailboxd log4j server log containing the logs from the mailbox server. This includes the mailbox store, LMTP server, IMAP and POP servers, and Index server. (Note: prior to ZCS 4.5, this log was called **/opt/zimbra/log/zimbra.log**.)

- **myslow.log**. This slow query log consists of all SQL statements from the mailbox server that took more then long_query_time seconds to execute. Note: long_query_time is defined in /opt/zimbra/my.cnf.
- **spamtrain.log**. This log contains output from zmtrainsa during regularly scheduled executions from the cron.
- **sync.log**. This log contains information about Zimbra mobile sync operations.

Other logs include:

- **/opt/zimbra/jetty/logs/**. This is where Jetty-specific activity is logged.
- **/opt/zimbra/db/data**. <hostname>.err. This is the message store database error log.
- **/opt/zimbra/logger/db/data.** <hostname>.err. This is the Logger database error log.

ZCS activity logged to System syslog

- **/var/log/zimbra.log.** The Zimbra syslog details the activities of the ZCS MTA (Postfix, amavisd, antispam, antivirus), Logger, Authentication (cyrus-sasl), and Directory (OpenLDAP). By default LDAP activity is logged to zimbra.log.

Syslog file is written by the operating system, and contains a subset of the messages written to the local logs. SNMP monitoring typically looks at the syslog file and generates traps for critical errors.

Using log4j to Configure Logging

The Zimbra server uses **log4j**, a Java logging package as the log manager. By default, the Zimbra server has **log4j** configured to log to the local file system. You can configure **log4j** to direct output to another location. Go to the Log4j website for information about using log4j.

Logging Levels

The logging level is set by default to include logs that are generated for INFO, WARNING, ERROR and FATAL. When problems start to occur, you can turn on the DEBUG log level.

To change the logging levels, edit the log4j properties, **logger.com.zimbra**.

When enabling DEBUG, you can specify a specific category to debug. . For example, to see debug details for POP activity, you would type **logger.com.zimbra.pop=DEBUG**.

The following categories are pre-defined in log4j:

- zimbra.misc
- zimbra.pop
- zimbra.imap

- zimbra.index
- zimbra.journal
- zimbra.lmtp
- zimbra.mailbox
- zimbra.account
- zimbra.replication
- zimbra.security
- zimbra.soap

Changes to the log level take affect immediately.

Table 1 Zimbra Logging Levels

Level	Local?	Syslog ?	SNMP Trap?	When Used
FATAL	Y	Y	Y	The FATAL level designates very severe error events that will lead the application to abort or impact a large number of users. For example, being unable to contact the MySQL database.
ERROR	Y	Y	N	The ERROR level designates error events that might still allow the application to continue running or impact a single user. For example, a single mailbox having a corrupt index or being unable to delete a message from a mailbox.
WARN	Y	N	N	The WARN level designates potentially harmful situations but are usually recoverable or can be ignored. For example, user log in failed.
INFO*	Y	N	N *	The INFO level designates information messages that highlights the progress of the application, basic transaction-level logging. For example, server start-ups, mailbox creation/deletion, account creation.

* A few non-critical messages such, as service startup messages, will generate traps.

Level	Local?	Syslog ?	SNMP Trap?	When Used
DEBUG	Y	N	N	Events that would generally be useful to help a customer debug problems.

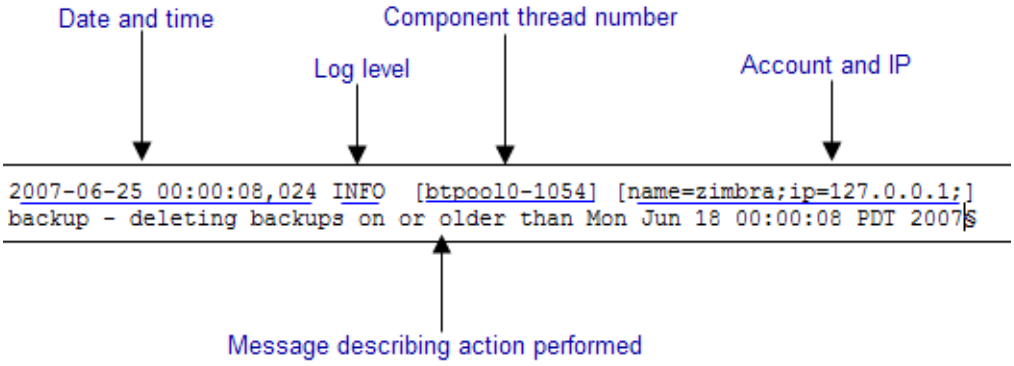
* A few non-critical messages such, as service startup messages, will generate traps.

Reviewing mailbox.log Records

The mailbox.log file logs every action taken on the mailbox server, including authentication sessions, LMTP, POP3, and IMAP servers, and Index server. Review the mailbox.log to find information about the health of your server and to help identify problems.

Mailbox.log records valid and invalid login attempts, account activity such as opening email, deleting items, creating items, indexing of new mail, server activities including start and stop. The progress of an activity on the mail server is logged as INFO and if the expected results of the activity fails and errors occurs, an exception is written to the log.

Reading records in the log The example below is a record showing that on June 25, 2007, the Zimbra server with an IP address of 127.0.0.1 was in the process of deleting backups that were created on Monday, June 18, 2007 at 8 seconds after midnight Pacific Daylight Time (PDT) or older than that date.



Note: ***Component thread number*** *identifies which thread managed by mailboxd is performing the action logged.*

Handler Exceptions and Stack Traces

If an error occurs during the progress of an activity, a handler exception is added to the end of the basic log record to notify you that an event occurred

during the execution of the process that disrupted the normal flow. This signals that some type of error was detected.

```
007-06-25 00:00:10,379 INFO  [btpool0-1064] [name=nringers@zimbra.com;
mid=228;ip=72.255.38.207;ua=Zimbra Desktop/0.38;] SoapEngine - handler
exception
```

Sometimes a stack trace is displayed after the exceptions notification. A stack logs the process in detail. A stack trace is a report of the threads and monitors in the Zimbra's **mailboxd** service. This information aids in debugging, as the trace shows where the error occurred. The last few entries in the stack often indicate the origin of the problem. When the **caused by** descriptor is included in the log line, this is the root of the error. In the example below, the error was caused by 501, bad address syntax.

```
com.example.cs.mailbox.MailServiceException: Invalid address: Jon R
at com.example.cs.mailbox.MailServiceException.internal_SEND_FAILURE
(MailServiceException.java:412)
at com.example.cs.mailbox.MailServiceException.SEND_ABORTED_ADDRESS_
FAILURE MailServiceException.java:416)
.
.
.
at org.mortbay.thread.BoundedThreadPool$PoolThread.run(BoundedThread
Pool.java:442)
Caused by: com.example.cs.mailbox.MailSender$SafeSendFailedException
:501 Bad address syntax
; chained exception is:
com.sun.mail.smtp.SMTPAddressFailedException: 501 Bad address syntax
at com.sun.mail.smtp.SMTPTransport.rcptTo(SMTPTransport.java:1196)
at
com.sun.mail.smtp.SMTPTransport.sendMessage(SMTPTransport.java:584)
at javax.mail.Transport.send0(Transport.java:169)
at javax.mail.Transport.send(Transport.java:98)
at
com.example.cs.mailbox.MailSender.sendMessage(MailSender.java:409)
at
com.example.cs.mailbox.MailSender.sendMimeMessage(MailSender.java:26
2)
... 30 more
```

Mailbox log files

The mailbox.log files rotate daily. The mailbox log files are saved in **/opt/zimbra/log**. Previous mailbox.log file names include the date the file was made. The log without a date is the current log file. You can backup and remove these files.

Note: *For troubleshooting, if the log is too large to search, you can clear the log and rerun the activity that is causing the error. To clear the log, as zimbra type:* **cat/dev/null>/opt/zimbra/log/mailbox.log**

mailbox.log examples

To review the mailbox.log for errors, search for the email address or the service that is experiencing the problem. Also, search for WARN or ERROR log levels, read the text of the message. When you find the error review the records, tracing the events that happened before the problem was recorded.

The following are examples of the three areas that can register exceptions, service, account and email.

Service Error - System Crashing

When your system crashes, look for the startup message and after finding that message, look for errors before the startup message date. This example shows an out-of-memory error on June 17, 2007.

```
2007-06-25 01:56:18,725 INFO  [main] [] soap - Servlet SoapServlet
starting up
```

Look for errors before the startup message.

```
2007-06-17 20:11:34,194 FATAL [btpool0-3335]
[name=samd@example.com;aname=abcadmin@example.com;mid=142;ip=66.92.2
5.194;ua=ZimbraConnectorForBES/5.0.207;] system - handler exception
java.lang.OutOfMemoryError: PermGen space
```

Mail Error - Mail Delivery problem

When you are looking for an error in mail delivery, start by looking for the "LmtpServer" service. This example includes a stack trace report with a **caused by** explanation that the recipient address was rejected as the address must be a fully-qualified address.

```
2007-06-25 10:47:43,008 INFO  [LmtpServer-250]
[name=bigen@example.com;mid=30;msgid=<1291804360.35481182793659172.J
avaMail.root@dogfood.example.com>;] lmtp - rejecting message
bigen@example.com: exception occurred
com.zimbra.cs.mailbox.MailServiceException: redirect to too failed
at com.zimbra.cs.mailbox.MailServiceException.internal_SEND_FAILURE
(MailServiceException.java:412)
at com.zimbra.cs.mailbox.MailServiceException.SEND_FAILURE(MailServi
ceException.java:424)
at com.zimbra.cs.filter.ZimbraMailAdapter.executeActions(ZimbraMailA
dapter.java:286)
at org.apache.jsieve.SieveFactory.evaluate(SieveFactory.java:151)
at com.zimbra.cs.filter.RuleManager.applyRules(RuleManager.java:177)
at com.zimbra.cs.lmtpserver.ZimbraLmtpBackend.deliverMessageToLocal
Mailboxes(ZimbraLmtpBackend.java:325)
at com.zimbra.cs.lmtpserver.ZimbraLmtpBackend.deliver(ZimbraLmtpBack
end.java:140)
at com.zimbra.cs.lmtpserver.LmtpHandler.doDATA(LmtpHandler.java:441)
at com.zimbra.cs.lmtpserver.LmtpHandler.processCommand(LmtpHandler.
java:205)
at com.zimbra.cs.tcpserver.ProtocolHandler.processConnection(Protoc
olHandler.java:231)
at com.zimbra.cs.tcpserver.ProtocolHandler.run(ProtocolHandler.java
:198)
at EDU.oswego.cs.dl.util.concurrent.PooledExecutor$Worker.run(Unkn
own Source)
at java.lang.Thread.run(Thread.java:619)
```

```
Caused by: com.zimbra.cs.mailbox.MailSender$SafeSendFailedException:
504 <too>: Recipient address rejected: need fully-qualified address
; chained exception is:
com.sun.mail.smtp.SMTPAddressFailedException: 504 <too>: Recipient
address rejected: need fully-qualified address
at com.sun.mail.smtp.SMTPTransport.rcptTo(SMTPTransport.java:1196)
at
com.sun.mail.smtp.SMTPTransport.sendMessage(SMTPTransport.java:584)
at javax.mail.Transport.send0(Transport.java:169)
at javax.mail.Transport.send(Transport.java:120)
at
com.zimbra.cs.filter.ZimbraMailAdapter.executeActions(ZimbraMailAdap
ter.java:281)
... 10 more
```

Account Error- Log in error

Mailbox.log logs any successful or unsuccessful login attempts from IMAP, POP3 or ZWC. When you are looking for a login error, start by looking for “Auth.” This example shows that someone from IP address 10.10.131.10 was trying to log in as admin on the Zimbra Web Client, using Firefox 2.0 in a Windows OS. Permission was denied because it was not an admin account

```
2007-06-25 09:16:11,483 INFO  [btpool0-251]
[ip=10.10.131.10;ua=ZimbraWebClient - FF2.0 (Win);] SoapEngine -
handler exception
com.zimbra.common.service.ServiceException: permission denied: not
an admin account
at com.zimbra.common.service.ServiceException.PERM_DENIED(ServiceExc
eption.java:205)
at com.zimbra.cs.service.admin.Auth.handle(Auth.java:103)
```

Account Errors - IMAP or POP related

When you are looking for a log because of an IMAP or POP issue, look for "ImapServer/Pop3Server." This example shows a fatal IMAP server error occurred while trying to connect siress@example.com.

```
mailbox.log.2007-06-19:2007-06-19 15:33:56,832 FATAL [ImapServer-
2444] [name=siress@example.com;ip=127.0.0.1;] system - Fatal error
occurred while handling connection
```

SNMP

SNMP Monitoring Tools

You will probably want to implement server monitoring software in order to monitor system logs, CPU and disk usage, and other runtime information.

Zimbra uses swatch to watch the syslog output to generate SNMP traps.

SNMP Configuration

Zimbra includes an installer package with SNMP monitoring. This package should be run on every server (Zimbra, OpenLDAP, and Postfix) that is part of the Zimbra configuration.

The only SNMP configuration is the destination host to which traps should be sent.

Errors Generating SNMP Traps

The Zimbra error message generates SNMP traps when a service is stopped or is started. You can capture these messages using third-party SNMP monitoring software and direct selected messages to a pager or other alert system.

Checking MySQL

The MySQL database is automatically checked weekly to verify the health of the database. This check takes about an hour. If any errors are found, a report is sent to the administrator's account. The report name that runs the MySQL check is **zmbintegrityreport**, and the crontab is automatically configured to run this report once a week.

Note: *When the MySQL database is checked, running this report can consume a significant amount of I/O. This should not present a problem, but if you find that running this report does affect your operation, you can change the frequency with which zmbintegrityreport is run.*

Appendix A Command-Line Utilities

Command Line Interface (CLI) can be used to create, modify and delete certain features and functions of the Zimbra Collaboration Suite. The administration console is the main tool for maintaining the Zimbra Collaboration Suite, but some functions can only be changed from the CLI utility.

The CLI utility can be used for the following:

- Provisioning accounts*
- Starting and stopping a service
- Installing self-signed certificates
- Local configuration

*In general, provisioning and managing accounts should be performed from the administration console, but bulk provisioning can be done from the CLI

General Tool Information

The Zimbra command-line utilities follow standard UNIX command-line conventions.

Follow these guidelines when using the commands

- CLI commands are run as the zimbra user, that is **su - zimbra**.
- The actual CLI commands are case-sensitive. You must type them in lower case.
- Press **ENTER** after you type a command.
- Typing the CLI command and then **- h** displays the usage options for the command. Example: **zmprov - h** lists all the options available for the zmprov utility.
- Each operation is invoked through command-line options. Many have a long name and a short name. For example, these two commands are equivalent:

  zmprov createAccount joe@domain.com test123

  zmprov ca joe@domain.com test123

Syntax Conventions

When demonstrating the syntax of each tool, the following conventions indicate required, optional, and alternate values:

- {**attribute**} in curly brackets is required information.
- [**attribute**] in square brackets are optional arguments or information.
- {**a**|**b**|**c**} or [**a**|**b**|**c**] options separated by the pipe character | means "a" OR "b" OR "c"
- For attribute names that may contain spaces, surround the name with double quotes.

Location of Command-Line Utilities

The command-line tools available for administrators are all located in the **/opt/zimbra/bin** directory on the Zimbra server.

Zimbra CLI Commands

The table below lists the CLI commands in /opt/zimbra/bin.

Table 2 Zimbra CLI Commands

CLI	Description
ldap	Start, stop, or find the status of Zimbra LDAP
ldapsearch	Perform a search on an LDAP server
logmysql	Start, stop, or find the status of the MySql session. Enters interactive command-line MySQL session with the logger mysql
logmysql.server	Start, stop the SQL instance for the logger package
logmysqladmin	Send myslqadmin commands to the logger mysql
mysql	Enters interactive command-line MySQL session with the mailbox mysql
mysql.server	Start, stop the SQL instance for the mailbox package
mysqladmin	Send admin commands to MySQL
postconf	Postfix command to view or modify the postfix configuration
postfix	Start, stop, reload, flush, check, upgrade-configuration of postfix
qshape	Examine postfix queue in relation to time and sender/recipient domain

Table 2 Zimbra CLI Commands

CLI	Description
tomcat	Start, stop, find the status of the Tomcat server
zmaccts	Lists the accounts and gives the status of accounts on the domain
zmamavisdctl	Start, stop, or find the status of the Amavis-D New
zmantispamctl	Start, stop, reload, status for anti-spam service
zmantivirusctl	Start, stop, reload, status for the anti-virus service
zmapachectl	Start, stop, status of Apache service (for spell check)
zmcertinstall	Installs the self-signed certificate created with zmcreatecert.
zmclamdctl	Start, stop, or find the status of Clam AV
zmcleaniplanetics	Clean iPlanet ICS calendar files
zmcontrol	Start, stop, status of the Zimbra servers. Also can use to find the ZCS version installed.
zmconvertctl	Start, stop, the conversion server or find the status of the converted attachments conversion/ indexing
zmcreateca	Creates a signing certificate. Used with zmcreatecert and zmcertinstall
zmcreatecert	Create a new self-signed certificate
zmdumpenv	General information about the server environment is displayed
zmfixtz	Fixes calendar entries with incorrect TZ offset
zmhostname	Find the hostname of the Zimbra server
zmjava	Execute Java with Zimbra-specific environment settings
zmldappasswd	Changes the LDAP password
zmlmtpinject	Testing tool
zmlocalconfig	Used to set or get the local configuration of a Zimbra server
zmloggerctl	Start, stop, reload, or find the status of the Zimbra logger service
zmlogswatchctl	Start, stop, status of the swatch that is monitoring logging
zmmailbox	Performs mailbox management tasks
zmmailboxctl	Start, stop, reload, or find the status of the mailbox components (Tomcat, MySQL, convert)
zmmsgtrace	Trace messages

Table 2 Zimbra CLI Commands

CLI	Description
zmmtaconfigctl	Start, stop, or find the status of the MTA configuration daemon
zmmtactl	Start, stop, or find the status of the MTA
zmmylogpasswd	Change logger MySQL password
zmmypasswd	Change MySQL passwords
zmmysqlstatus	Status of mailbox SQL instance
zmperditionctl	Start, stop, or find the status of the perdition IMAP proxy
zmprov	Performs all provisioning tasks in Zimbra LDAP, including creating accounts, domains, distribution lists and aliases
zmproxyctl	Start or stop IMAP proxy service
zmsaslauthdctl	Start, stop, or find the status of saslauthd (authentication)
zmshutil	Used for other zm scripts, do not use
zmspamextract	Retrieve spam and relocate it to a specified directory
zmspellctl	Start, stop, or find the status of the spell check server
zmsshkeygen	Generate Zimbra's SSH encryption keys
zmstorectl	Start, stop, or find the status of Zimbra store services
zmswatchctl	Start, stop, or find the status of the Swatch process, which is used in monitoring
zmsyslogsetup	Used to setup system log config file
zmtlsctl	Set the Web server mode to the communication protocol options: HTTP, HTTPS or mixed
zmtrainsa	Used to train the anti-spam filter to recognize what is spam or ham
zmupdateauthkeys	Used to fetch the ssh encryption keys created by zmsshkeygen
zmvolume	Manage storage volumes on your Zimbra Mailbox server
zmzimletctl	Deploy and configure Zimlets

zmprov (Provisioning)

The **zmprov** tool performs all provisioning tasks in Zimbra LDAP, including creating accounts, aliases, domains, distribution lists, and calendar resources.

Each operation is invoked through command-line options, each of which has a long name and a short name.

The syntax for modify can include the prefix “+” or “-” so that you can make changes to the attributes affected and do not need to reenter attributes that are not changing. Use + to add a new instance of the specified attribute name without changing any existing attributes. Use - to remove a particular instance of an attribute. The syntax is **zmprov [cmd] [argument]**.

The following objects use this syntax:

- **ModifyAccount**
- **ModifyDomain**
- **ModifyCos**
- **ModifyServer**
- **ModifyConfig**
- **ModifyDistributionList**
- **ModifyCalendarResource**

The following example would add the attribute **zimbraZimletUserProperties** with the value “testing” to user 1 and would not change the value of any other instances of that attribute.

zmprov ma user1 +zimbraZimletUserProperties testing

Short Name	Long Name	Syntax, Example, and Notes
-h	--help	display usage
-f	--file	use file as input stream
-s	--server	{host}[:{port}] server hostname and optional port
-l	--ldap	provision via LDAP instead of SOAP
-a	--account {name}	account name to auth as
-p	--password {pass}	password for account
-P	--passfile {file}	read password from file
-z	--zadmin	use zimbra admin name/password from localconfig for admin/password

Short Name	Long Name	Syntax, Example, and Notes
-v	--verbose	verbose mode (dumps full exception stack trace)
-d/	--debug	debug mode (dumps SOAP messages)

The commands in the following table are divided into the following tasks types - Account, Calendar Resources, Config, COS, Distribution List, Documents, Domain, Server, and Miscellaneous.

Long Name	Short Name	Syntax, Example, and Notes
Account Provisioning Commands		
CreateAccount	**ca**	Syntax:{name@domain} {password} [attribute1 value1 etc] Type on one line. **zmprov ca joe@domain.com test123 displayName JSmith**
DeleteAccount	**da**	Syntax:{name@domain|id|adminName} **zmprov da joe@domain.com**
GetAccountMembership	**gam**	{name@domain|id}
GetAccount	**ga**	Syntax:{name@domain|id|adminName} **zmprov ga joe@domain.com**
GetAllAccounts	**gaa**	Syntax: [-v] [{domain}] **zmprov gaa** **zmprov gaa -v domain.com**
GetAllAdminAccounts	**gaaa**	Syntax: gaaa **zmprov gaaa**
ModifyAccount	**ma**	{name@domain|id|adminName} [attribute1 value1 etc] **zmprov ma joe@domain.com zimbraAccountStatus maintenance**

Long Name	Short Name	Syntax, Example, and Notes
SetPassword	**sp**	{name@domain|id|adminName} {password} **Note**: Passwords cannot included accented characters in the string. Example of accented characters that cannot be used: ã, é, í, ú, ü, ñ. **zmprov sp joe@domain.com test321**
CheckPasswordStrength	**cps**	Syntax: {name@doman|id} {password} **Note:** This command does not check the password age or history. **zmprov cps joe@domain.com**
AddAccountAlias	**aaa**	{name@domain|id|adminName} {alias@domain} **zmprov aaa joe@domain.com joe.smith@engr.domain.com**
RemoveAccountAlias	**raa**	{name@domain|id|adminName} {alias@domain} **zmprov raa joe@domain.com joe.smith@engr.domain.com**
SetAccountCOS	**sac**	{name@domain|id|adminName} {cos-name|cos-id} **zmprov sac joe@domain.com FieldTechnician**
SearchAccounts	**sa**	[-v] {ldap-query} [limit] [offset] [sortBy {attribute}
RenameAccount	**ra**	{name@domain|id} {newname@domain} **zmprov ra joe@domain.com joe23@domain.com**
Calendar Resource Provisioning Commands		
CreateCalendarResource	**ccr**	{name@domain} [attr1 value1 [attr2 value2...]]
DeleteCalendarResource	**dcr**	{name@domain|id}
GetAllCalendarResources	**gacr**	[-v] [{domain}]
GetCalendarResource	**gcr**	{name@domain|id}
ModifyCalendarResource	**mcr**	{name@domain|id} [attr1 value1 {attr2 value2...]]

Long Name	Short Name	Syntax, Example, and Notes
RenameCalendarResource	**rcr**	{name@domain|id} {newName@domain}
SearchCalendarResources	**scr**	[-v] domain attr op value {attr op value...]
Domain Provisioning Commands		
CreateDomain	**cd**	{domain} [attribute1 value1 etc] **zmprov cd mktng.domain.com zimbraAuthMech zimbra**
DeleteDomain	**dd**	{domain|id} **zmprov dd mktng.domain.com**
GetDomain	**gd**	{domain|id} **zmprov gd mktng.domain.com**
GetAllDomains	**gad**	[-v]
ModifyDomain	**md**	{domain|id} [attribute1 value1 etc] **zmprov md domain.com zimbraGalMaxResults 50**
COS Provisioning Commands		
CreateCos	**cc**	{name} [attribute1 value1 etc] **zmprov cc Executive zimbraAttachmentsBlocked FALSE zimbraAuthTokenLifetime 60m zimbraMailQuota 100M zimbraMailMessageLifetime 0**
DeleteCos	**dc**	{name|id} **zmprov dc Executive**
GetCos	**gc**	{name|id} **zmprov gc Executive**
GetAllCos	**gac**	[-v] **zmprov gac -v**
ModifyCos	**mc**	{name|id} [attribute1 value1 etc] **zmprov mc Executive zimbraAttachmentsBlocked TRUE**
RenameCos	**rc**	{name|id} {newName} **zmprov rc Executive Business**
Server Provisioning Commands		
CreateServer	**cs**	{name} [attribute1 value1 etc]

Long Name	Short Name	Syntax, Example, and Notes
DeleteServer	**ds**	{name|id} **zmprov ds domain.com**
GetServer	**gs**	{name|id} **zmprov gs domain.com**
GetAllServers	**gas**	[-v] **zmprov gas**
ModifyServer	**ms**	{name|id} [attribute1 value1 etc] **zmprov ms domain.com zimbraVirusDefinitionsUpdateFrequency 2h**
Config Provisioning Commands		
GetAllConfig	**gacf**	[-v] All LDAP settings are displayed
GetConfig	**gcf**	{name}
ModifyConfig	**mcf**	attr1 value1 Modifies the LDAP settings.
Distribution List Provisioning Commands		
CreateDistributionList	**cdl**	{list@domain} **zmprov cdl needlepoint-list@domain.com**
AddDistributionListMember	**adlm**	{list@domain|id} {member@domain} **zmprov adlm needlepoint-list@domain.com singer23@mail.free.net**
RemoveDistributionListMember	**rdlm**	{list@domain|id} **zmprov rdlm needlepoint-list@domain.com singer23@mail.free.net**
GetAlldistributionLists	**gadl**	[-v]
Get DistributionListmembership	**gdlm**	{name@domain|id}
GetDistributionList	**gdl**	{list@domain|id} **zmprov gdl list@domain.com**
ModifyDistributionList	**mdl**	{list@domain|id} attr1 value1 {attr2 value2...} **zmprov md list@domain.com**

Long Name	Short Name	Syntax, Example, and Notes
DeleteDistributionList	**ddl**	(list@domain|id}
AddDistributionListAlias	**adla**	{list@domain|id} {alias@domain}
RemoveDistributionListAlias	**rdla**	{list@domain|id} {alias@domain}
RenameDistributionList	**rdl**	{list@domain|id} {newName@domain}
RemoveDistributionListMember	**rdlm**	{list@domain|id) {member@domain}
Zimbra Documents Provisioning Commands		
ImportNotebook	**impn**	{name@domain} {directory} {folder} Before importing files, any file that will become a Documents page (wiki-style page), must be renamed to include the extension ".wiki". If not it is imported as a file, accessed either as an attachment or an image. **impn joe@domain.com /opt/zimbra/wiki/ template template**
InitNotebook	**in**	[{name@domain}] **in joe@domain.com**
initDomainNotebook	**idn**	{domain} [{name@domain}] Creates the domain Documents account **idn domain.com domainwiki@domain.com**
Miscellaneous Provisioning Commands		
SearchGAL	**sg**	{domain} {name} **zmprov sg joe**
AutoCompleteGal	**acg**	{domain} {name}
GenerateDomainPreAuthKey	**gdpak**	{domain|id} Generates a pre-authentication key to enable a trusted third party to authenticate to allow for single-sign on. Used in conjunction with GenerateDomainPreAuth.
GenerateDomainPreAuth	**gdpa**	{domain|id} {name} {name|id|foreignPrincipal} {timestamp|0} {expires|0} Generates preAuth values for comparison.
GetMailboxInfo	**gmi**	{account}

Long Name	Short Name	Syntax, Example, and Notes
GetQuotaUsage	**gqu**	{server}

Examples

- Create one account with a password that is assigned to the default COS.

  zmprov ca name@domain.com password

- Create one account with a password that is assigned to a specified COS. You must know the COS ID number. To find a COS ID, type **gc <COSname>.**

  zmprov ca name@domain.com password zimbraCOS cosIDnumberstring

- Create one account when the password is not authenticated internally.

  zmprov ca name@domain.com ‘’

  The empty single quote is required and indicates that there is no local password.

- Using a batch process to create accounts, see Managing the Zimbra Collaboration Suite chapter for the procedure.

- Add an alias to an account.

  zmprov aaa accountname@domain.com aliasname@domain.com

- Create distribution list. The ID of the distribution list is returned.

  zmprov cdl listname@domain.com

- Add a member to a distribution list. Tip: You can add multiple members to a list from the administration console.

  zmprov adlm listname@domain.com member@domain.com

- Change the administrator’s password. Use this command to change any password. Enter the address of the password to be changed.

  zmprov sp admin@domain.com password

- Create a domain that authenticates against Zimbra OpenLDAP.

  zmprov cd marketing.domain.com zimbraAuthMech zimbra

- Set the default domain.

  zmprov mcf zimbraDefaultDomain domain1.com

- To list all COSs and their attribute values.

  zmprov gac -v

- To list all user accounts in a domain (domain.com)

  zmprov gaa domain.com

- To list all user accounts and their configurations

```
zmprov gaa -v domain.com
```

- To enable logger on a single server

  ```
  zmprov +zimbraServiceEnabled logger
  ```

  Then type **zmloggerctl start**, to start the logger.

- Modify **zimbraNewMailNotification** to customize the notification email template. A default email is sent from Postmaster notifying users that they have received mail in another mailbox. To change the template, you modify the receiving mailbox account. The variables are

  - **${SENDER_ADDRESS}**
  - **${RECIPIENT_ADDRESS}**
  - **${RECIPIENT_DOMAIN}**
  - **${NOTIFICATION_ADDRESSS}**
  - **${SUBJECT}**
  - **${NEWLINE}**

  You can specify which of the above variables appear in the **Subject**, **From**, or **Body** of the email. The following example is changing the appearance of the message in the body of the notification email that is received at **name@domain.com**. You can also change the template in a class of service, use **zmprov mc**. The command is written on one line.

  ```
  zmprov ma name@domain.com zimbraNewMailNotificationBody
  'Important message from
  ${SENDER_ADDRESS}.${NEWLINE}Subject:${SUBJECT}'
  ```

zmaccts

This command runs a report that lists all the accounts, their status, when they were created and the last time anyone logged on. The domain summary shows the total number of accounts and their status.

Syntax

zmaccts

zmcontrol (Start/Stop Service)

This command is run to start or to stop services. You can also find which version of the Zimbra Collaboration Suite is installed.

Syntax

zmcontrol [-v -h] command [args]

Description

Long Name	Short Name	Description
	-v	Displays Zimbra software version.
	-h	Displays the usage options for this command.
	-H	Host name (localhost).
Command in...		
maintenance		Toggle maintenance mode.
shutdown		Shutdown all services and manager on this host. When the manager is shutdown, you cannot query that status.
start		Startup manager and all services on this host.
startup		Startup manger and all services on this host.
status		Returns services information for the named host.
stop		Stop all services but leave the manager running.

zmcreatecert and zmcertinstall (For a Certificate)

The CLI command **zmcreateca** creates the signing certificate and **zmcreatecert** creates a new self-signed certificate. After a certificate is created, **zmcertinstall** is the CLI command to install it.

Tomcat must be stopped and then restarted after the certificate is installed.

Example of steps to use to stop tomcat, delete a certificate that is not working and then create a new certificate and install it.

1. As root, type:

   rm -rf /opt/zimbra/ssl
   mkdir /opt/zimbra/ssl
   chown zimbra:zimbra /opt/zimbra/ssl

2. Type **su - zimbra,** then type the following all on one line

keytool -delete -alias my_ca -keystore /opt/zimbra/java/jre/lib/security/cacerts -storepass changeit

3. Next, type the following on one line

   keytool -delete -alias tomcat -keystore /opt/zimbra/tomcat/conf/keystore -storepass zimbra

4. Type **zmcreateca**, press **Enter**
5. Type **zmcreatecert**, press **Enter**
6. Type **zmcertinstall mailbox**, press **Enter**
7. Type **tomcat stop**, press **Enter**
8. Type **tomcat start**, press **Enter**

zmlocalconfig

This command is used to set or get the local configuration for a Zimbra server.

Syntax

zmlocalconfig [options]

To see the local config type

zmlocalconfig

Description

zmmailbox

Long Name	Short Name	Description
--config	**-c**	<**arg**> File in which the configuration is stored
--default	**-d**	Show default values for keys listed in [args]
--edit	**-e**	Edit the configuration file, change keys and values specified. The [args] is in the key=value form.
--force	**-f**	Edit the keys whose change is known to be potentially dangerous
--help	**-h**	Shows the help for the usage options for this tool
--info	**-i**	Shows the documentation for the keys listed in [args]
--format	**-m**	<**arg**> Shows the values in one of these formats: plain (default), xml, shell, nokey.
--changed	**-n**	Shows the values for only those keys listed in the [args] that have been changed from their defaults
--path	**-p**	Shows which configuration file will be used
--quiet	**-q**	Suppress logging
--random	**-r**	This option is used with the edit option. Specified key is set to a random password string.
--show	**-s**	Forces the display of the password strings
--unset	**-u**	Removes the local setting for a variable, which causes it to fallback to the default
--expand	**-x**	Expand values

The **zmmailbox** tool is used for mailbox management. The command can help administrators provision new mailboxes along with accounts, debug issues with a mailbox, and help with migrations.

You can invoke the zmmailbox command from within the zmprov command. You enter **selectMailbox** within zmprov to access the zmmailbox command connected to that specified mailbox. You can then enter zmmailbox

commands until you type **exit**. Exit returns you to zmprov. This is useful when you want to create accounts and also pre-create some folders, tags, or saved searches at the same time.

Syntax

zmmailbox [args] [cmd] [cmd-args ...]

Description

Short Name	Long Name	Syntax, Example, and Notes
-h	--help	display usage
-f	--file	use file as input stream
-u	--url	http[s]://{host}[:{port}] server hostname and optional port. Must use admin port with -z/-a
-a	--account {name}	account name to auth as
-z	--zadmin	use zimbra admin name/password from localconfig for admin/password
-m	--mailbox	mailbox to open
-p	--password {pass}	password for admin account and or mailbox
-P	--passfile {file}	read password from file
-v	--verbose	verbose mode (dumps full exception stack trace)
-d	--debug	debug mode (dumps SOAP messages)

Specific CLI tools are available for the different components of a mailbox. Usage is described in the CLI help for the following

zmmailbox help admin	help on admin-related commands
zmmailbox help commands	help on all commands

zmmailbox help contact	help on contact-related commands (address book)
zmmailbox help conversation	help on conversation-related commands
zmmailbox help folder	help on folder-related commands
zmmailbox help item	help on item-related commands
zmmailbox help message	help on message-related commands
zmmailbox help misc	help on miscellaneous commands
zmmailbox help search	help on search-related commands
zmmailbox help tag	help on tag-related commands

Examples

- When you create an account, you may want to pre-create some tags and folders. You can invoke zmmailbox inside of zmprov by using “selectMailbox(sm)”

```
domain.example.com$ /opt/zimbra/bin/zmprov
prov> ca user10@domain.example.com test123
9a993516-aa49-4fa5-bc0d-f740a474f7a8
prov> sm user10@domain.example.com
mailbox: user10@domain.example.com, size: 0 B, messages: 0,
unread: 0
mbox user10@domain.example.com> createFolder /Archive
257
mbox user10@domain.example.com> createTag TODO
64
mbox user10@domain.example.com> createSearchFolder /unread
"is:unread"
258
mbox user10@domain.example.com> exit
prov>
```

- To find the mailbox size for a user

```
zmmailbox -z-m user@example.com gms
```

zmtlsctl

This command is used to set the Web server mode to the communication protocol options: HTTP, HTTPS, or mixed. Mixed mode uses HTTPS for logging in and HTTP for normal session traffic. All modes use SSL encryption for back-end administrative traffic.

Tomcat has to be stopped and restarted for the change to take effect.

Note: *If you switch to HTTPS, you use the self-signed certificate generated during Zimbra installation, in /opt/zimbra/ssl/ssl/server/server.crt.*

Syntax

zmtlsctl [mode]

mode = http, https, or mixed

Steps to run

1. Type **zmtlsctl [mode]**, press **Enter.**
2. Type **tomcat stop**, press **Enter.**
3. When Tomcat is stopped, type **tomcat start**, press **Enter.**

zmmsgtrace

This command is used to trace an email message that was sent or received with the last 30 days.

Syntax

zmmsgtrace {-i|-s|-r|-F} <message_id>

Description

Long Name	Short Name	Description
--help	**-h**	Shows the help for the usage options for this tool.
	-i	Message ID.
	-s	Sender address.
	-r	Recipient address.
	-F	From Times in YYYYMMDD (hhmmss) format.
	-D	dest_ip/host
	-t	start, end times in YYYYMMDD (hhmmss) format

zmmylogpasswd

This command is used to change the zimbra_logger_myql_password. If the --root option is specified, the MySql_logger_root_passwd is changed. In both cases, MySQL is updated with the new passwords. Refer to the MySQL documentation to see how you can start the MySQL server temporarily to skip grant tables, to override the root password.

Syntax

zmmylogpasswd <new_password>

zmmypasswd

This command is used to change zimbra_myql_password. If the --root option is specified, the mysql_root_passwd is changed. In both cases, MySQL is updated with the new passwords. Refer to the MySQL documentation to see how you can start the MySQL server temporarily to skip grant tables, to override the root password.

Syntax

zmmypasswd [--root] <new_password>.

zmtrainsa

This command is used to train the anti-spam filter. This command is run automatically every night to train the SpamAssasin filter from messages users mark as “junk” “not junk” from their mailbox. See Anti-Spam Training Filters on page 37.

You can use this command to manually send one account’s mail through the spam filter. You will need to know the account password.

Syntax

zmtrainsa <server> <user> <pass> <spam|ham> [folder]

Description

zmtrainsa fetches the mail from <user> with password <pass> from <server> and trains the filter as either spam or ham <spam|ham>. The folder is optional. If a folder is not defined, the contents of the Inbox is fetched.

zmvolume

This command can be used to manage storage volumes from the CLI. Volumes can be easily managed from the administration console, Server, Volume tab.

Syntax

zmvolume {-a|-d|-l|-e|-dc|-sc} [options]

Description

Long Name	Short Name	Description
--add	**-a**	Adds a volume
--compress	**-c**	<**arg**> Compress BLOBs; "true" or "false"
--compressionThreshold	**-ct**	Compression threshold; default 4KB
--delete	**-d**	Deletes a volume
--displayCurrent	**-dc**	Displays the current volume
--edit	**-e**	Edits a volume
--help	**-h**	Shows the help for the usage options for this tool.
--id	**-id**	<**arg**> Volume ID
--list	**-l**	Lists volumes
--name	**-n**	<**arg**> Volume name
--path	**-p**	<**arg**> Root path
--server	**-s**	<**arg**> Mail server hostname. Default is localhost.
--setCurrent	**-sc**	Sets the current volume
--type	**-t**	<**arg**> Volume type (primaryMessage, secondaryMessage, or index)
--turnOffSecondary	**-ts**	Turns off the current secondary message volume

zmzimletctl

This command is used to deploy Zimlets to users. See Chapter 9, Working with Zimlets.

Syntax

zmzimletctl {-l} {command} <zimlet.zip|config.xml|zimlet>

Description

Long Name	Short Name	Description
deploy		<**zimlet.zip**> Creates the Zimlet entry in the LDAP server, installs the zimlet files on the Server, grants, access to the members of the default COS, and turns on the Zimlet
undeploy		<**zimlet**> Uninstall a zimlet from the Zimbra server
install		<**zimlet.zip**> Installs the Zimlet files on the host
ldapDeploy		<**zimlet**> Adds the Zimlet entry to the LDAP
enable		<**zimlet**> Enables the Zimlet
disable		<**zimlet**> Disables the Zimlet.
acl		<**zimlet**> <**cos1**> **{grant|deny} [**<**cos2**> **{grant|deny}...]** Sets the access control, grant|deny, to a COS
listAcls		<**zimlet**> Lists the ACLs for the Zimlets
listZimlets		Shows the status of all the Zimlets on the server
getConfigTemplate		<**zimlet.zip**> Extracts the configuration template from the Zimlet.zip file
configure		<**config.xml**>Installs the configuration
listPriority		Shows the current Zimlet priorities (0 is high, 9 is low)
setPriority		<**zimlet**> Sets the Zimlet priority

Appendix B Glossary

The Glossary lists terms and acronyms used in this document, and includes both industry terms and application-specific terms. If a general industry concept or practice has been implemented in a specific way within the product, that is noted as well.

A record

A (Address) records map the hostname to the numeric IP address. For ZCS, the A record is the IP address for the Zimbra server.

Account Policy

Class of Service as exposed in Zimbra administration console.

AD

Microsoft Active Directory Server. Used in Zimbra as an optional choice for authentication and GAL, along with OpenLDAP for all other Zimbra functions.

Alias

An “also known as” email address, which should be routed to a user at a different email address.

Attribute

Contains object-related data for directory server entries. Attributes store information such as a server host name or email forwarding address.

Authentication

Process by which user-supplied login information is used to validate that user’s authority to enter a system.

Blacklist

Anti-spam term, indicates a known bad IP address. This could be one that has been hijacked by spammers, or also one from a poorly maintained but legitimate site that allows mail relaying from unauthorized parties.

BLOB

Binary Large Object.

Class of Service (COS)

Describes an object in the Zimbra LDAP data schema, which contains settings for things like user mail quotas. Each Zimbra account includes a COS, and the account inherits all the settings from the selected COS.

CLI

Command-Line Interface. Used to refer to the collective set of Zimbra command-line tools, such as **zmprov**.

Cluster

A type of network configuration for high availability, using clusters of servers (nodes). If one server fails or drops off the network, a spare takes over.

Contacts

Within Zimbra, Contacts are a user-interface feature listing that user's personal collection of address and contact information.

Conversation

Within Zimbra, Conversations are a user-interface feature that presents email threads (emails sharing the same subject line) as a single Conversation listing. Users can expand the Conversation to view all emails within it.

DHTML

Dynamic HTML. A technology employed in the Zimbra Web Client.

DNS

Domain Name System is an Internet directory service. DNS is how domain names are translated into IP addresses and DNS also controls email delivery. Correctly configured DNS is required for Postfix to route messages to remote destinations

Edge MTA

Generic term used to refer to any mail transfer agent that is the first line of defense in handling incoming email traffic. Functions that may occur on the Edge MTA include spam filtering.

Entry

An item in the directory server, such as an account or mail host.

Failover

Takeover process where a spare server machine detects that a main server is unavailable, and the spare takes over processing for that server.

FQDN

Fully qualified domain name. The hostname and the path to the host. For example, www.zimbra.com is a fully qualified domain name. www is the host, zimbra is the second-level domain, and .com is the top level domain.

GAL

Global Address List, the Outlook version of a company directory. Lists contact information, including email addresses, for all employees within an organization.

Global Configuration

A Zimbra object containing default settings for servers and Class of Service.

High Availability

Abbreviated as HA, high availability refers to the availability of resources in a computer system in the wake of component failures in the system.

HTTP

HyperText Transfer Protocol, used along with SOAP for UI integration.

IMAP

Internet Message Access Protocol is a method of accessing mail from a remote message store as if the users were local.

Index Store

Within Zimbra, a directory area that stores all the indexing information for mail messages on a particular mailbox server.

Indexing

The process of parsing incoming email messages for search words.

Java

Java is an industry standard object-oriented programming language. Used for the core Zimbra application server.

JavaScript

Scripting largely developed by Netscape that can interact with HTML source code. Technology used in the Zimbra Web Client.

LDAP

Lightweight Directory Access Protocol, an industry standard protocol used for authentication.

Zimbra administration console

The Zimbra administrator interface.

Zimbra Web Client

The Zimbra end-user interface.

LMTP

Local Mail Transfer Protocol, used for transferring messages from Postfix MTA to the Zimbra server for final delivery.

Mailbox Server

Alternative term for Zimbra server.

MAPI

Messaging Application Programming Interface. A system built into Microsoft Windows to enable different email applications to work together.

Message Store

Within Zimbra, a directory area that stores the mail messages on a particular mailbox server.

MDA

Mail Delivery Agent, sometimes known as a mail host. The Zimbra server functions as an MDA.

Metadata

Data that describes other data, rather than actual content. Within Zimbra, metadata consists of user folders, threads, message titles and tags, and pointers.

MIME

Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII Internet message content such as image files. Format used to store messages in Message Store.

MTA

Message Transfer Agent. MTA is a program that delivers mail and transports it between machines. A Zimbra deployment assumes both the Postfix MTA and an edge MTA.

MX Record

Mail eXchange. An MX record is an entry in a domain name database that identifies the mail server that is responsible for handling emails for that domain name. The email system relies on DNS MX records to transmit emails between domains. When mail is processed, the MX record is checked before the A record for the destination address.

OOTO

Common shorthand for "out of the office", used when sending vacation messages.

Open Source

Refers to software created by groups of users for non-commercial distribution, where source code is published rather than proprietary.

OS

Operating system, such as Linux, UNIX, or Microsoft Windows.

POP

Post Office Protocol is used to retrieve email from a remote server over TCP/IP and save it to the local computer.

Provisioning

The process of creating accounts or other data, usually in batch or automated fashion.

RBH

Real-time black hole. Usually refers to web sites that, as a public service, provide lists of known bad IP addresses from which mail should be blocked, because the

servers are either known to be spammers, or are unsecured and exploited by spammers.

Redo Logs

Detailed transaction log for the Zimbra server, used for replay and replication.

SAN

Storage Array Network. A high-availability data storage area.

Schema

Describes the data structures in use for by directory services at a particular organizational site.

SMTP

Simple Mail Transfer Protocol. Used in Zimbra deployments between the Edge MTA and the Postfix MTA.

SNMP

Simple Network Monitoring Protocol. Used by monitoring software to pick up critical errors from system logs.

SOAP

Simple Object Access Protocol, an XML-based messaging protocol used for sending requests for Web services. The Zimbra servers use SOAP for receiving and processing requests, which can come from Zimbra command-line tools or Zimbra user interfaces.

Spam

Unsolicited commercial email. Spammers refer to their output as “bulk business email”.

SQL

Structured Query Language, used to look up messages in the Message Store.

SSL

Secure Sockets Layer.

Tags

A Zimbra Web Client feature. Users can define tags and apply them to mail messages for searching.

TCO

Total Cost of Ownership. Zimbra reduces total cost of ownership (TCO) by reducing requirements for server hardware, OS licensing fees, supporting application license fees, disk storage requirements, and personnel (IT, help desk, consulting).

TLS

Transport Layer Security.

UCE

Unsolicited commercial email, also known as spam.

Virtual Alias

A type of mail alias recognized in the Postfix MTA.

Whitelist

Anti-spam term for a known good mail or IP address. Mail coming from such an address may be "automatically trusted".

XML

eXtended Markup Language.

Index

Q

R

S

T

U

V

W

Z