



Zimbra Collaboration Suite™ Administrator's Guide

**ZCS 3.1
Open Source Edition
April 2006**

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

No part of this document may be reproduced, in whole or in part, without the express written permission of Zimbra Inc.

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

MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Postfix is copyright © 1999 International Business Machines Corporation and others and it was created by Wietse Venema <wietse@porcupine.org>.

SpamAssassin is a trademark of Deersoft, Inc.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

All other marks are the property of their respective owners.

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

April 2006 ..

Table of Content

Chapter 1 Introduction	7
Intended Audience	7
Available Documentation	7
Support for Recommended Third-Party Components	8
Support and Contact Information	8
Chapter 2 Product Overview	9
Core Functionality	9
Zimbra Components	10
System Architecture	11
Zimbra Core	11
Zimbra LDAP	11
Zimbra MTA (mail routing server)	11
Zimbra Store (Zimbra server)	11
Zimbra-SNMP	12
Zimbra Logger	12
Zimbra Spell	12
Zimbra System Directory Tree	13
Example of a Typical Multi-Server Configuration	15
Chapter 3 Zimbra Server	17
Incoming Mail Routing	17
Disk Layout	17
Message Store	18
Data Store	18
Index Store	19
Backup	20
Redo Log	20
Log	20
Chapter 4 Zimbra Directory Service	21
Directory Services Overview	21
LDAP Hierarchy	22
Zimbra Schema	23
Account Authentication	23
The Internal Authentication Mechanism	24
External LDAP and External Active Directory Authentication Mechanism	24
Zimbra Objects	25
Company Directory/GAL	27
Chapter 5 Zimbra MTA	31
Zimbra MTA Deployment	31
Postfix Configuration Files	32

MTA Functionality	32
SMTP Authentication	33
SMTP Restrictions	33
Relay Host Settings	33
MTA-LDAP Integration	33
Account Quota and the MTA	34
MTA and Amavisd-New Integration	34
Anti-Virus Protection	34
Anti-Spam Protection	34
Receiving and Sending Mail through Zimbra MTA	36
Zimbra MTA Message Queues	37
Chapter 6 Using the Administration Console	39
Administrator Accounts	39
Global Administrator	39
Domain Administrator	39
Logging on	40
Changing Administrator Passwords	40
About the Administration Console	40
Management Tasks from the Administration Console	41
Management Tasks Not Available from Administration UI	42
Chapter 7 Managing Zimbra Collaboration Suite	43
Managing Global Configurations	43
General Tab	44
Attachments Tab	44
MTA Tab	44
POP Tab	45
IMAP Tab	45
Anti-Spam Tab	45
Anti-Virus Tab	45
HSM	46
Managing Domains	46
Global Address List (GAL) Mode	46
Authentication Modes	47
Managing Servers	47
General Tab	48
Services Tab	48
MTA Tab	48
IMAP and POP Tabs	48
Volume Tab	48
Managing User Accounts	49
Using Search	49
Adding user accounts	49
Manage Aliases	50
Distribution Lists	50
Class of Service	50
Changing Password	51
View an Account's Mailbox	52
Changing an Account's Status	52
Enforcing Mailbox and Contact Quotas	52
Moving a Mailbox	52

Managing Resources for	53
Chapter 8 Managing End-User Mailbox Features	55
User Mailbox Features	55
Advanced Options	57
Preferences	58
Additional Account Options	59
Email Aliases	59
Email Forwarding	59
Displaying HTML in an Email	59
Users Preferences	59
General	60
Mail	60
Mail Filter Rules	60
Contacts	60
Calendar	61
Chapter 9 Working with Zimlets	63
Setting Up Zimlets in ZCS	63
Deploying Zimlets	63
Configuring a Zimlet	64
Viewing a List of Zimlets	65
Disabling or Removing a Zimlet	65
Zimlets Included with ZCS	65
Chapter 10 Zimbra Collaboration Suite	
Import Wizard for Outlook	67
Downloading Import Wizard for Outlook Install Program	67
Administrator's Responsibilities	67
The ZCS Import Wizard for Outlook Process	67
Outlook Features Not Imported	68
Chapter 11 Monitoring Zimbra Servers	69
Zimbra Logger	69
Reviewing Server Status	69
Server Performance Statistics	70
Tracing Messages	70
Generating Daily Mail Reports	71
Monitoring Mailbox Quotas	72
Log Files	72
Using log4j to Configure Logging	73
Logging Levels	73
SNMP	73
SNMP Monitoring Tools	73
SNMP Configuration	74
Errors Generating SNMP Traps	74
Appendix A Command-Line Utilities	75
General Tool Information	75

Zimbra CLI Commands	76
zmprov (Provisioning)	78
zmcontrol (Start/Stop Service)	83
zmcreatecert and zmcertinstall (For a Certificate)	84
zmlocalconfig (Local Configuration)	85
zmtlsctl	86
zmmsgtrace	86
zmmylogpasswd	87
zmmypasswd	87
zmtrainsa	87
zmvolume	87
zmzimletctl	89
 Appendix B Glossary	 91
 Index	 97

Chapter 1 Introduction

Zimbra™ Collaboration Suite is a full-featured email system offering reliable high-performance service and advanced mail features including advanced search capability, mail sorted by conversations, group calendaring, and tags, as well as standard mail features, such as contacts, user-defined folders, and user-defined filters.

Intended Audience

This guide is intended for systems 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 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, includes 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 Guide*. This guide provides instructions for running the Migration Wizard to migrate accounts from a Microsoft Exchange server.
- *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 Community Forum](#), to participate and learn more about the Zimbra Collaboration Suite.
- Send an email to feedback@zimbra.com to let us know what you like about the product and what you would like to see in the product. Or, if you prefer, post your ideas to the Zimbra Forum.

If you encounter problems with this software, 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 Tomcat, 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 offers a robust set of features. 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
- Mail delivery and routing
- 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
- 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
- Use Search Builder to perform advanced searches
- Save searches
- Use the Calendar to schedule appointments
- Share calendars with others
- Create a personal contacts list
- Set mailbox usage preferences, including defining mail filtering options

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.

- Apache Tomcat, the web application server that Zimbra software runs in.
- 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 a 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 Apache Tomcat, which is the servlet container the Zimbra software runs within. 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.

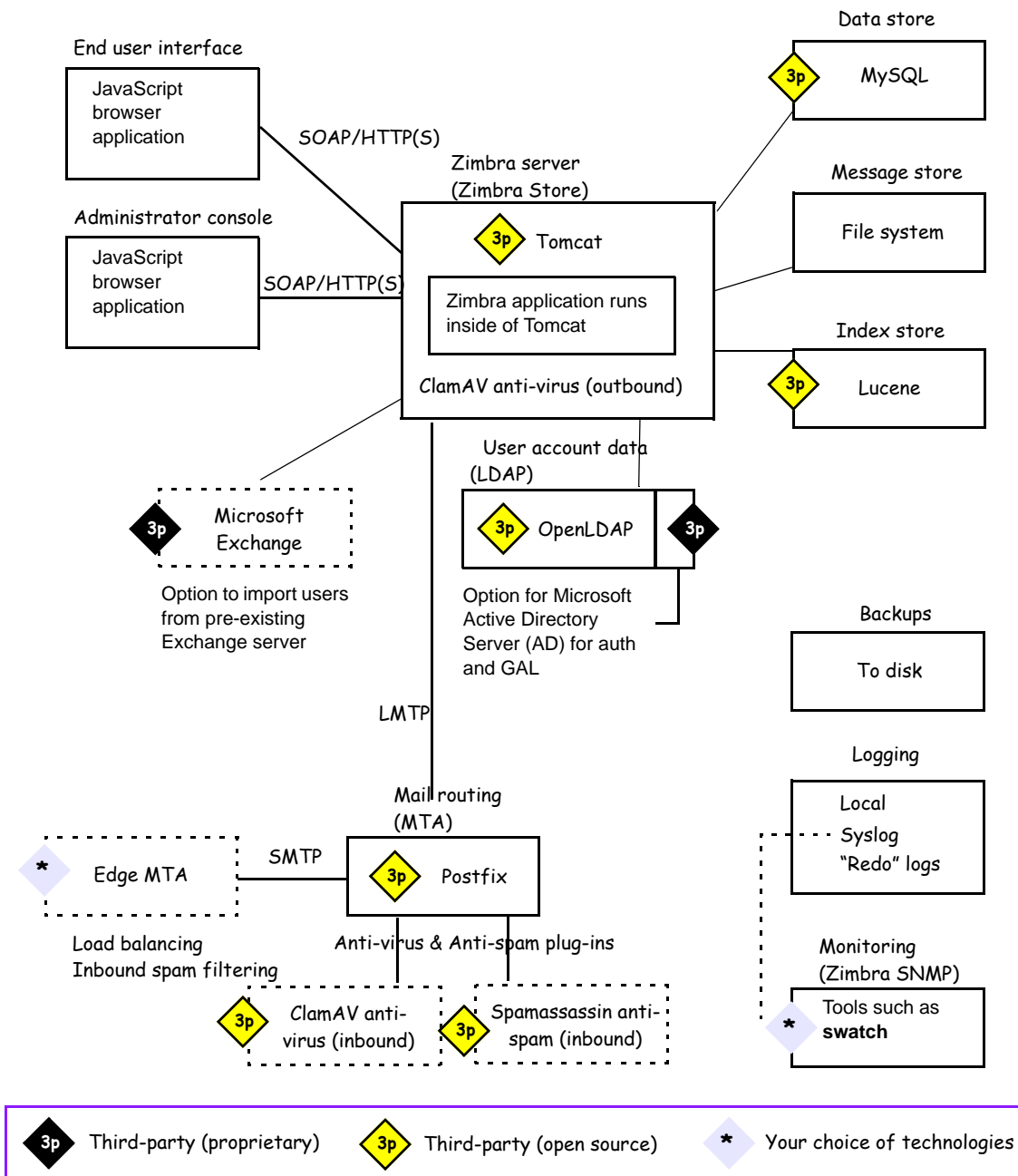
Zimbra Logger

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

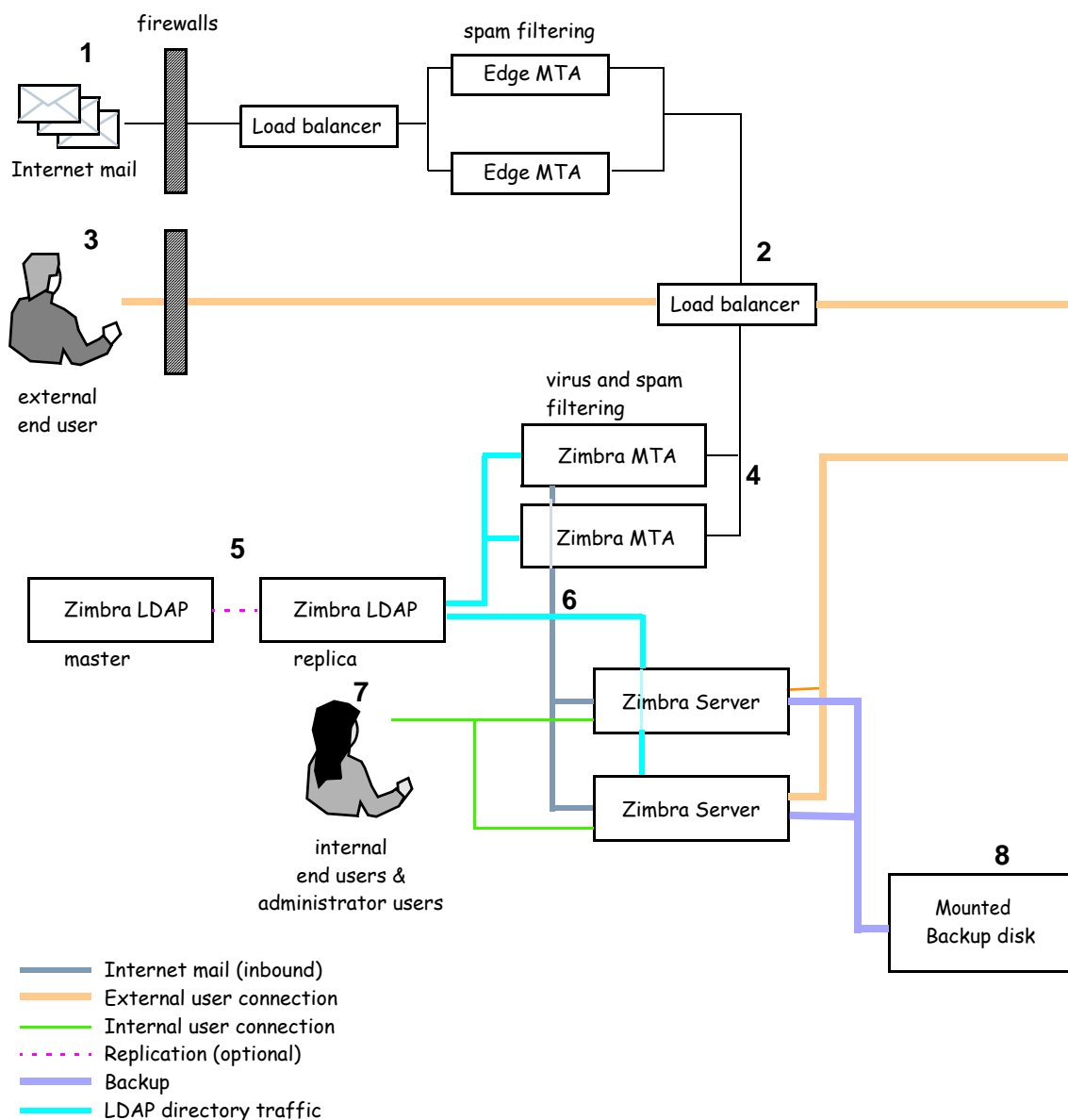
Parent	Directory	Description
/opt/ zimbra/		Created by all Zimbra installation packages
	bin/	Zimbra application files, including the command-line utilities described in Appendix A, Command - Line Utilities.
	conf/	Configuration information
	db/	Data Store
	doc/	Zimbra documentation and readme files
	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
	redolog/	Contains current transaction logs for the Zimbra server
	openldap/	OpenLDAP server installation, pre-configured to work with Zimbra
	postfix/	Postfix server installation, pre-configured to work with Zimbra
	sleepycat/	Berkeley DB
	snmp/	SNMP monitoring files
	ssl/	Certificates
	store/	Message Store
	tomcat/	Tomcat application server instance
	zimbramon/	Contains the control scripts and Perl modules

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, 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. In multi-server configurations, where recipients may be in different Message Stores, one copy exists per server.

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.

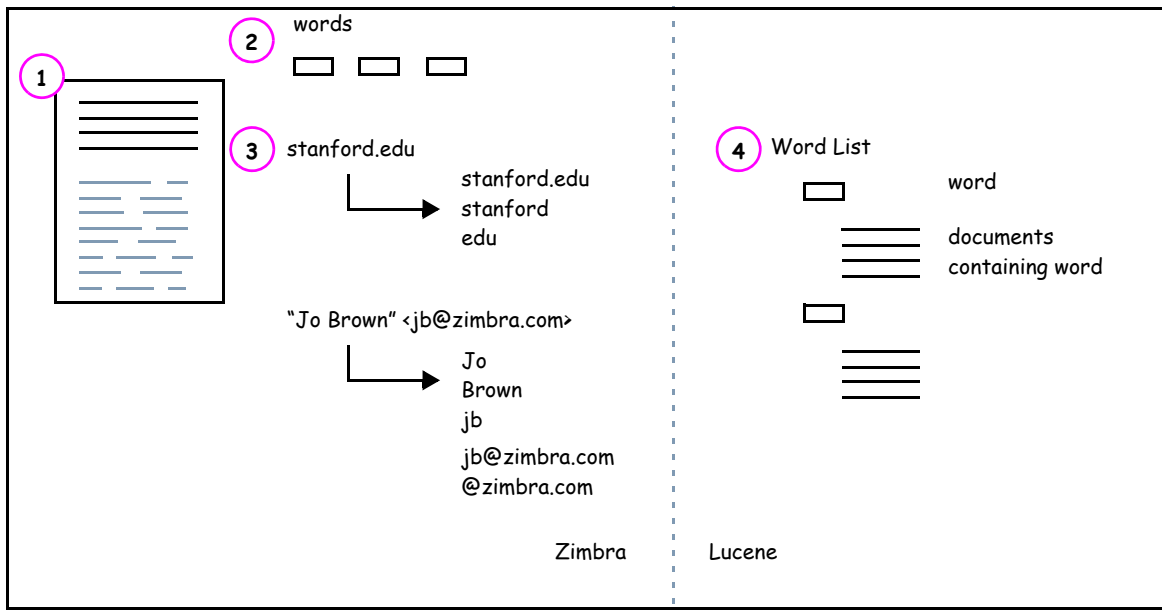
The process is as follows:

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 1: 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 12, 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 describes 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.

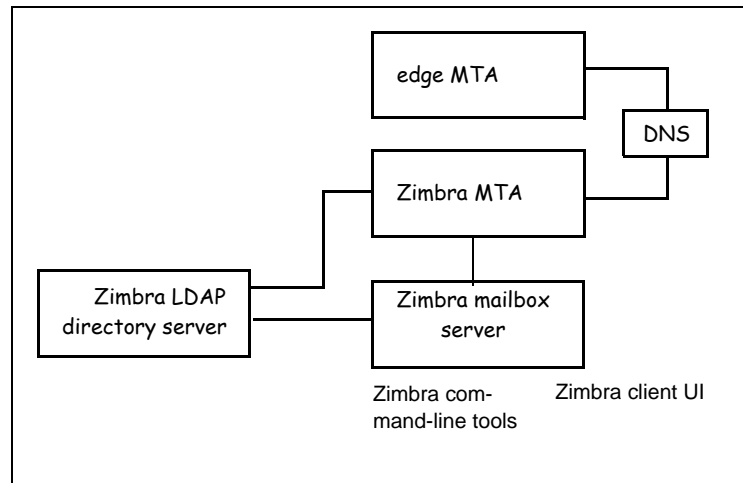
Directory Services Overview

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 1: 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.

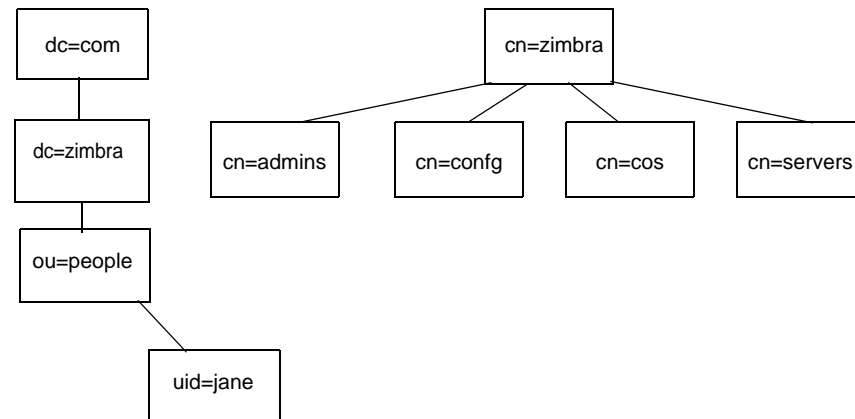
The object classes determine what type of object the entry refers to and what type of data can be stored for that entry. An entry's object classes that determines what kind of entry it is, is called a structural object class and cannot be changed. Other object classes are called auxiliary and may be 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 2: 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://ldapservice:port/`

where *ldapservice* 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

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 [Managing User Accounts section, Chapter 7](#).

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.

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 2 maps generic GAL search attributes to their Zimbra contact fields.

Table 2 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
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.

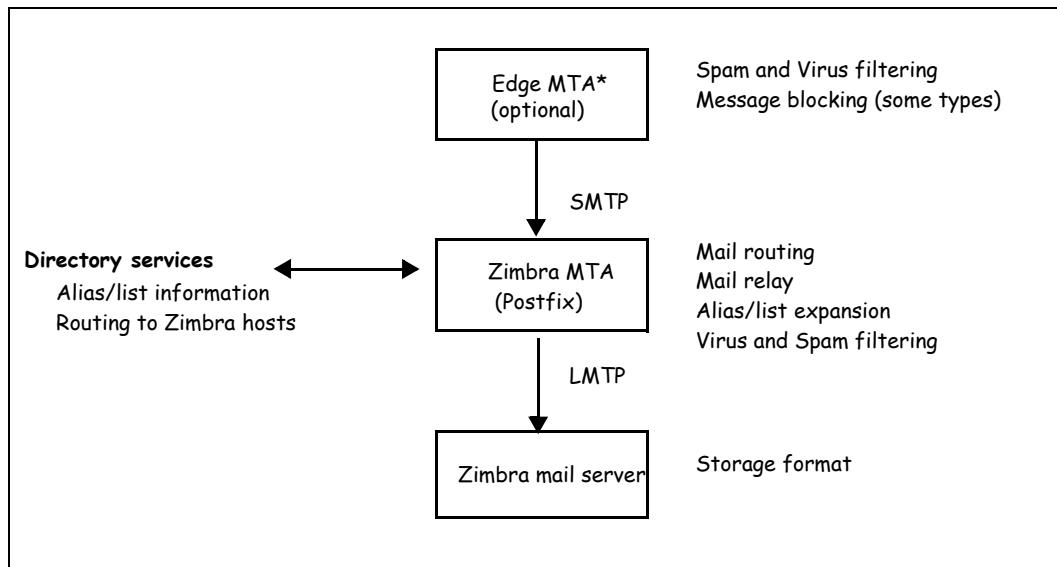
Zimbra MTA Deployment

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 1: 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. 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 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 accounts, 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. To send a folder to the spam training mailbox, type the command as:

```
zmtrainsa <server> <user> <password> spam [foldername]
```

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

```
zmtrainsa <server> <user> <password> 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 opm.blitzed.org
- reject_rbl_client relays.ordb.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 opm.blitzed.org" zimbraMtaRestriction "reject_rbl_client  
relays.ordb.org" zimbraMtaRestriction "reject_rbl_client cbl.abuseat.org"  
zimbraMtaRestriction "reject_rbl_client bl.spamcop.net" zimbraMtaRestriction  
"reject_rbl_client dnsbl.sorbs.net"
```

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

Receiving and Sending Mail through Zimbra MTA

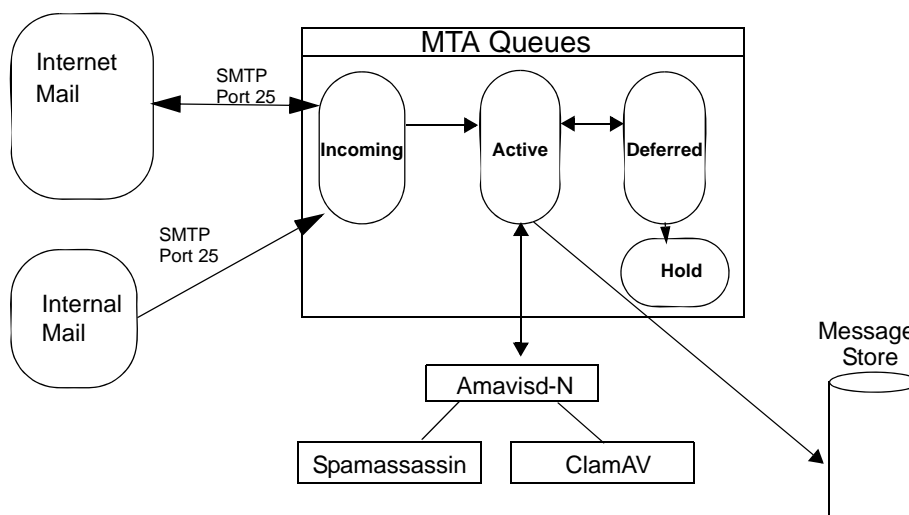
The Zimbra MTA delivers both the incoming and the outgoing mail messages. For outgoing mail, the Zimbra MTA determines the destination of the recipient address. If the destination host is local, the message is passed to the Zimbra server for delivery. If the destination host is a remote mail server, 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 84.

Chapter 6 Using the Administration Console

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

When you install the Zimbra Collaboration Suite, the administrator's user name and password are configured during installation and an admin account is configured. You can 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. Click **Log On**.

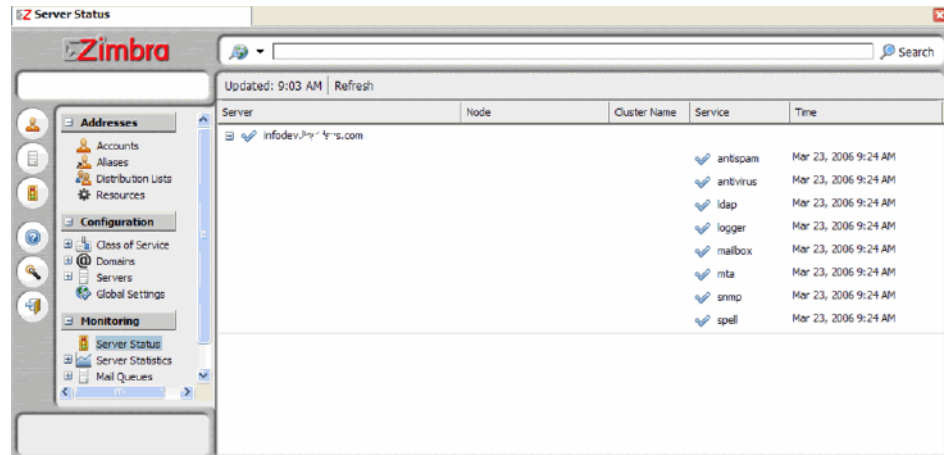
Changing Administrator Passwords

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 administrator account and click Change Password.

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

About the Administration Console

When you open the admin console, the right pane is the Server Status page, and the navigation pane, on the left, displays the functions exposed through the console.



The left navigation pane includes the following folders:

- **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.
- **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 use for that domain.
- **Servers.** Lists the servers, the host name and description. You can configure services, MTA, SMTP, IMAP, and POP features for servers.

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

The **Search** field allows you to quickly find accounts, aliases, distribution lists and resources for editing.

See the [Chapter 7, Managing Zimbra Collaboration Suite](#), for information about how to configure these functions.

Management Tasks from the Administration Console

From the administration console, you 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 distribution lists
- Enable or disable optional user-interface features such as conversations and contacts in the email client
- Configure various global settings for security, address book, and MTAs
- Use the Migration Wizard to migrate Microsoft Exchange server email accounts to the Zimbra server and to import the email and contact information

Management 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 Zimbra Collaboration Suite

This chapter describes the following functions used to manage the Zimbra Collaboration Suite. Features can be managed from either the administration console or from the CLI utility.

- Global configuration
- Domains
- Servers
- User Accounts
- Resource Accounts

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 default global rules that apply to accounts in the Zimbra servers. These are set during installation. The settings can be modified from the administration console.

Global settings include the following tabs:

- General
- Attachments
- MTA
- Pop
- IMAP
- Anti-Spam
- Anti-Virus

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 COS or Account set up, they override the global settings.*

General Tab

In the General tab configure the **Most results returned by GAL search** field, which sets a global ceiling for the number of GAL results returned from a user search. The default is 100 results per search.

Attachments Tab

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.

If **Disable attachment viewing from web mail UI** is enabled, users cannot view any attachments in their mailbox. You can set this global setting to prevent a virus outbreak if you think that mail has already been sent.

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: *Zimbra also supports the following types of attachment blocking:*

- **Class of Service**, to disable attachment viewing for members of that COS
- **Accounts**, to disable attachment viewing for individual accounts

MTA Tab

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.
- The **Relay MTA for external delivery** is the relay host name. This is the Zimbra MTA to which Postfix relays non-local email.
- 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.

POP Tab

POP3 (Post Office Protocol) can be enabled to allow users with a POP client to retrieve their mail stored on the Zimbra server and download new mail to their computer after messages are downloaded. The POP configuration determines if messages are deleted from the Zimbra server.

IMAP Tab

The Internet Message Access Protocol (IMAP) can be enabled to allow users with an IMAP client to access their mail stored on the Zimbra mailbox server from more than one computer. Messages are stored on the mailbox server.

Anti-Spam Tab

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 38.

RBL (Real time black-hole lists) can be turned on or off in SpamAssassin from the Zimbra CLI. See "To turn RBL on" on page 40.

Anti-Virus Tab

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 and the authentication mode.

The administration console can also be used to edit domain information or to remove a 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 whether 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.

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.

Server settings include the following tabs:

- General
- Services
- MTA
- IMAP
- POP
- 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 Tab

The General tab includes the server display name, the server hostname, and LMTP information including name and IP address if configured.

Services Tab

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

MTA Tab

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 and disable DNS lookup for the server.

IMAP and POP Tabs

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

Volume Tab

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 its 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 User Accounts

Managing accounts in the Zimbra system allows you to create accounts and change features easily from the administration console or by using the **zmprov** command-line tool described in Appendix A.

From the administration console you can manage user accounts as follows:

- Quickly create new accounts with the **New Account Wizard**
- Find a specific account using the **Search** feature
- Change account information

- Create and change alias addresses
- Change password for a selected account
- View an account's mailbox
- Change an account's status
- Delete an account

See the [Chapter 8, Managing End-User Mailbox Features](#), for descriptions of the mailbox features that can be configured.

Using Search

Search is used to quickly locate individual accounts, aliases, distribution lists, and resources on the LDAP server. Search by display name, first name, last name, the first part of the email address, alias, or delivery address. If you do not know the complete name, you can enter a partial name. Partial names can result in a list that has the partial name string anywhere in the information.

You can also use the Zimbra mailbox ID number to search for an account. To return a search from a mailbox ID, the complete ID string must be entered in the search.

Adding user accounts

If you are using the administration console, the New Account Wizard steps you through the account information to be completed. Before you add an user account, you should determine what features and access privileges should be assigned. You configure the following type of information:

- General information, including account name, class of service to be assigned, password
- Contact information, including phone number, company name and address
- Aliases to be used
- Forwarding directions
- Features and preferences available for this specific account. Changes made at the account level override the rules in the COS assigned to the account.

Creating an account sets up the appropriate entries on the Zimbra LDAP directory server. When the end-user logs in for the first time or when an email is delivered to the user's account, the mailbox is created on the mailbox server.

Batch Provisioning from the CLI Utility

For provisioning many accounts at once, you create a formatted text file with the user names. This file runs through a script, using the CLI command, `zmprov`. The `zmprov` utility provisions one account at a time.

Create a text file with the list of the accounts you want to add. Each account should be typed in the format of `ca (Create Account), email address, empty password`. For example, `ca name@company.com ''`

Note: *In this example, the empty single quote indicates that there is no local password.*

When the text file includes all the names to provision, log on to the Zimbra server and type the CLI command

```
zmprov <accounts.txt
```

Each of the names listed in the text file will be provisioned.

See Appendix A, for additional syntax definitions.

Manage Aliases

Manage and view all created aliases from the Aliases content pane. You can see to which account an alias is configured. From the Alias toolbar, you can move an alias from one account to another.

Distribution Lists

A distribution list is a group of email addresses contained in a list with a common email address. Distribution lists can be added, changed and deleted from the administration console.

Class of Service

Class of Service (COS) is a Zimbra-specific object that determines what default attributes a Zimbra Web Client email account has and what features are added or denied. The COS controls mailbox quotas, message lifetime, password restrictions, attachment blocking, and server pools for creation of new accounts.

A default COS is automatically created during the installation of Zimbra software. You can modify the default COS to set the attributes to your email restrictions, and you can create new COSs to assign to accounts.

Each account is assigned one class of service. When an account is created, if the COS is not explicitly set, the default COS is assigned. Also, if the COS assigned to the user no longer exists, the account is automatically assigned the default COS.

Note: *COS settings assigned to an account are not enforced for IMAP clients.*

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

Assigning a COS to an account quickly configures account features and restrictions. Some of the COS settings can be overridden either by global settings or by user settings. For example:

- Whether outgoing messages are saved to **Sent** can be changed in the user **Options**.
- Attachment blocking set as a global setting can override the COS setting.

See the Administration Console Help for a complete description of the fields in a class of service object.

Distributing Accounts Across Servers

In an environment with multiple mailbox servers, the class of service is used to assign a new account to a mailbox server. The COS server pool tab lists the mailbox servers in your Zimbra environment. When you configure the COS, you select which servers to add to the server pool. Within each pool of servers, a random algorithm assigns new mailboxes to any available server.

Note: You can assign an account to a particular server when you create an account in the New Account Wizard, Mail Server field.

Changing Password

Password restrictions can be set either at the COS level or at the account level. You can configure the following password rules:

- Password length. The default is minimum 6, maximum 64. The password is case sensitive.
- When passwords expire. The Zimbra default is to never expire the password.
- How frequently a password can be reused. The default password history allows the password to be reused.
- Password locked. Password cannot be changed.

View an Account's Mailbox

View Mail in Accounts lets you view the selected account's mailbox content, including all folders, calendar entries, and tags. This feature can be used to assist users who are having trouble with their mail account as you and the account user can be logged on to the account.

Any View Mail action to access an account is logged to the *audit.log* file.

Changing an Account's Status

Account status determines whether a user can log in and receive mail. The account status is displayed when account names are listed on the Accounts content pane.

The following account statuses can be set:

- **Active.** Active is the normal status for a mailbox account. Mail is delivered and users can log into the client interface.

- **Maintenance.** When a mailbox status is set to maintenance, login is disabled, and mail addressed to the account is queued at the MTA. An account can be set to maintenance mode for backing up, importing or restoring the mailbox.
- **Locked.** When a mailbox status is locked, the user cannot log in, but mail is still delivered to the account. The locked status can be set, if you suspect that a mail account has been hacked or is being used in an unauthorized manner.
- **Closed.** When a mailbox status is closed, the login is disabled, and messages are bounced. This status is used to soft-delete an account before deleting it from the server.

Enforcing Mailbox and Contact Quotas

You can specify mailbox quotas and the number of contacts allowed for each account through the Zimbra administration console. These limits can be set in the Class of Service or on a per-account basis on the Advanced page.

Account quota is the amount of space in megabytes that an account can use. The quota includes email messages and calendar meetings. When the quota is reached, all email messages are rejected. You can view mailbox quotas from the administration console, Monitoring, Server Statistics.

The address book size limit field sets the maximum number of contacts a user can have in their personal contacts list.

Managing Resources

A resource is a location or piece of equipment that can be scheduled for a meeting. The resource has its own mailbox address and accepts or rejects invitations automatically. Accounts with the Calendar feature can select resources for their meetings.

You create resources and manage their use from the administration console. A Resource Wizard guides you through the resource configuration, including designating the type of resource, the scheduling policy, the location, and a description.

To schedule a resource or location, users invite the equipment and/or location to a meeting. When they select the resource, they can view the notes about the resource and view free/busy status for the resource, if set up. When the meeting invite is sent, an email is sent to the resource account, and if the resource is free, the meeting is automatically entered in the resource's calendar.

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 Managing End-User Mailbox Features

When an account is provisioned, you create the email mailbox, assign the email address and configure how users access and use their mailboxes. This chapter describes the features, advanced controls, and user preferences that can be configured for an account either by assigning a COS or by specifying the feature when you create the account.

When accounts are created from the administration console, the New Account Wizard enables most of the features available to that account. The account creation utility creates the appropriate entries on the zimbra LDAP directory server. The mailbox is created on the Zimbra server upon the user's first log in to the system.

User Mailbox Features

The COS assigned to an account sets the default features for the account. These defaults can be changed for individual accounts. The following table lists the features that can be configured either by COS or by account. If the feature is not enabled, it does not display in the Zimbra Web Client.

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.

Table 3 Configurable Mailbox Features

Feature Name	COS	Account	Description
Contacts	X	X	Lets users create their own personal address book. The maximum number of contacts an account can have can be set in the advanced options.
Calendar	X	X	A calendar and scheduling tool to let users maintain their calendar, schedule meetings, delegate access to their calendar, create multiple personal calendars, and more.

Table 3 Configurable Mailbox Features

Feature Name	COS	Account	Description
Tagging	X	X	Tags allows users to create labels and assign them to messages.
Advanced search	X	X	Advanced search allows users to build a complex search using email by date, domain, flag, object, size, attachment, and folder.
Saved searches	X	X	Saved searches allows users to save a search that they have previously executed or built.
Conversations	X	X	Messages can be displayed grouped into conversations or as a message list. Conversations group messages by subject. If this feature is turned on, it is the default.
Change password	X	X	Change password allows users to change their password at any time.
Initial search preference	X	X	Users can specify a search to execute when they log in.
User-defined mail filters	X	X	Allows users to create rules for managing their email. Rules can include routing mail to different folders.
GAL access	X	X	GAL access allows users to access the company directory.
HTML compose	X	X	Allows the user to use HTML markup to compose messages that can contain different fonts, colors, and style.
IMAP access	X	X	Enables users to use third party mail applications, such as Thunderbird or Outlook, to access their mailbox using the IMAP protocol.
POP3 access	X	X	Enables users to use third party mail applications, such as Thunderbird or Outlook, to access their mailbox using the POP protocol.

Advanced Options

Advanced options that can be set at both the COS and account level are described in the table that follows.

Table 4 Configurable Advanced Options

Advanced Options	COS	Account	Description
Disable attachment viewing from web mail UI	X	X	Users cannot view attachments to their messages. If this feature is enabled in Global Settings, it overrides the COS and individual account settings.
Account quota	X	X	Mailbox size limit in MB. The default is not to set a mailbox quota, which makes the quote unlimited.
Address book size limit	X	X	Maximum number of contacts a user can have in their personal Contacts list.
Minimum/Maximum password length	X	X	Specifies the required length of a password.
Minimum / Maximum password age	X	X	Number of days that a password must remain unchanged before a user can change the password, or the number of days that can elapse before a user is forced to change his password.
Enforce password history	X	X	Number of times a user can change his password before he can reuse an old password.
Password locked	X	X	Users cannot change their passwords.
Email message lifetime	X	X	Number of days a message can remain in any folder before it is automatically purged.
Trashed message lifetime	X	X	Number of days a message remains in the Trash folder before it is automatically purged.
Spam message lifetime	X	X	Number of days a message can remain in the Junk folders, before it is automatically purged.

Table 4 Configurable Advanced Options

Advanced Options	COS	Account	Description
Session token lifetime	X	X	Session token 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.
Must change password		X	When a user logs in for the first time, he is required to change his password.
Administrator		X	In the General Information section, is the option to enable the account to be an administrator account and allows the user to log in to the administration console.

Preferences

How user mailboxes display and behave when a message is composed or received is controlled by preferences that can be configured in the COS and in account configuration. If the preference is set for the account, the user can change it from the Options application on the Web client.

The preferences are listed in the following table.

Table 5 Configurable Preferences

Preferences	COS	Account
Save to Sent	X	X
View mail as HTML	X	X
Always compose in new window	X	X
Reply/Forward using format of the original messages	X	X
Always compose mail using either text or HTML Default is text.	X	X
Signature style, use a separator between message or not. Default is to not separate the signature.	X	X
Enable automatic adding of contacts	X	X
Contacts per page	X	X
Number of items to display per page	X	X
Initial mail search	X	X
Show search string	X	X
Group mail by conversations	X	X

Table 5 Configurable Preferences

Preferences	COS	Account
Enable address for new mail notification and add address		X
Enable mail signature		X
Show time-zone list in appointment view	X	X
Show IMAP search folders	X	X

Additional Account Options

Email Aliases

An alias is an email address that redirects all email it receives to another email account. It is not an email account. An unlimited number of email aliases can be created for an account. Email sent to an alias address is automatically forwarded to the user's account.

Email Forwarding

When setting up an account, you can enable the account to allow users to specify a forwarding address, specify a forwarding address for the user's account and specify a forwarding address that is hidden from the user. A copy of each message sent to the account is immediately forwarded to the designated forwarding address.

Users Preferences

End-users can further customize their mailboxes when they log in to the Zimbra Web Client. The options they modify overrule the account and COS preference settings. The preferences include a General tab, Mail tab, Mail Filters tab, Contacts tab, and a Calendar tab. Only those features that are enabled are shown in the user's Options.

General

Users can:

- Change their passwords
- Select whether to include Junk and Trash folders in their search folders
- Select to always show the search string in the search field
- Set the default font settings

Note: If Microsoft Active Directory is used for user authentication instead of the Zimbra LDAP, you must disable the user's **Change Password** feature in their Class of Service. In that case, the **Change password** option is not displayed.

Mail

Users can define the following features for their mailbox's behavior:

- Default view to use (conversations or mail messages)
- The number of items to display on a page
- How often, in minutes, that the Web Client checks for new messages
- Whether to save copies of outbound messages to the **Sent** folder
- Reply-to address
- Reply and forwarding preferences; whether to include original text, and if so, as inline text or as a separate attachment
- Set an address to forward mail and enable to have the copy of the forwarded mail deleted from their mailbox.
- Whether to automatically append a signature to outgoing messages and what the text should be
- Enable a vacation/out of office message and what the text should be
- Whether to generate new mail notifications and if so, to which email address notifications should be sent
- Whether to view mail as HTML for messages that include HTML, default is to display messages as plain text
- Whether to ignore messages they send that they then receive
- Whether to compose mail as HTML or plain text
- Whether to compose messages in a separate window

Mail Filter Rules

Users can define a set of rules and corresponding actions to apply to incoming mail. When an incoming mail message matches the conditions of a filter rule, the corresponding actions associated with that rules are applied.

Contacts

Users can configure the following contact behavior:

- Whether to automatically add a contact from a recipient of a message the user has sent
- Which view to view their contacts in, list or as cards
- How many contacts to show on a single page
- Import a contact list or export their contact list to a csv text file.

Calendar

Users can set the following:

- Which calendar view they want to see when they open their calendar; Day, Work Week, 7-Day Week, Month, or Schedule.
- Which day of the week is the first day to display in the calendars.
- Select to display the time-zone list in their appointment dialog, giving them the opportunity to change time zones while making appointments.
- Whether to use the QuickAdd dialog to create appointments from the calendar pane.
- Whether the mini-navigation calendar always displays in the Mail view. The mini-calendar automatically displays in the Calendar view.
- Select when to be reminded of an appointment. The default is 5 minutes before the appointment.

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. Zimlets can be made available from the Zimbra Web Client Overview Pane to users by modifying the Class of Service (COS).

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 use the Zimlet Management Tools to deploy the Zimlet to users.

Deployment and management of Zimlets is only from the command line (CLI).

Deploying Zimlets

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/zimlet` 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.

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/zimlet** 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
```

Viewing a List of Zimlets

You can see a list of which Zimlets are installed on the Zimbra server, which are enabled or disabled on the LDAP server, and in which COSs the Zimlets are available.

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

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 Zimlets, type `zmzimletctl enable <zimletname>`.

To uninstall and remove a Zimlet from the Zimbra server

Type `zmzimletctl undeploy <zimletname>`

The Zimlet and all associated files are uninstalled.

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

Important: Only remove 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. These Zimlets do not require any configuration to work.

The following Zimlets are available by default from Zimlets on the Overview Pane on the Zimbra Web Client.

- The **Amazon** Zimlet, to search Amazon. com
- The **Maps** Zimlet, to quickly look up an address in Yahoo Maps for general reference.
- **Wikipedia** Zimlet lets users quickly search for an entry in Wikipedia.
- The **Search** Zimlet lets users right-click and select from several popular websites to search without having to leave the Zimbra Web Client.

No additional configuration is required to make these Zimlets work. These Zimlets can be disabled, if you do not want users to access them. See [Disabling or Removing a Zimlet](#) in this chapter.

Chapter 10 Zimbra Collaboration Suite

Import Wizard for Outlook

The Zimbra Collaboration Suite Import Wizard for Outlook lets users import the contents of a .pst file from a Microsoft® Outlook® 2003 mailbox to accounts on the Zimbra server.

The Import Wizard imports email messages, attachments, and contacts. When the files are imported, the Outlook folder hierarchy is maintained. If categories have been assigned to messages and contacts, these are converted to tags in the user's Zimbra mailbox.

Downloading Import Wizard for Outlook Install Program

The ZCS Import Wizard for Outlook and user import instructions can be downloaded from the Administration Console>Downloads area. You should download these files to an internal directory that users can access. Users then can download the Import Wizard for Outlook file to their computers and run the executable.

Administrator's Responsibilities

You will need to do the following for users that want to import their .pst files to the Zimbra Server:

- Create the user account on the Zimbra server before they download their .pst.
- Let your users know how to get the Import Wizard file and how to complete the Zimbra server information as listed below.
- Assist users with locating their .pst files.

The ZCS Import Wizard for Outlook Process

The ZCS Import Wizard asks for server information, user information, and import options. The following is a general overview of the steps.

1. Users enter information about the Zimbra server that will receive their .pst files. This is information you must provide to users, including:
 - Zimbra server domain name (DNS).

- Which server port to use. For non secured connections, the default is 80. For secured connection, the default is 443. Your configuration can be different.
 - Whether to check **Use Secure Connection** (SSL). This box is checked to establish a secure connection to that port.
2. Users enter their Zimbra email address and password
 3. Users browse to locate their .pst file
 4. Users set import options for their Outlook junk and deleted items folder and can set a date filter to only import messages received after a specified date.

Users can import more than one .pst file. They run the import program once for each .pst file. When additional .pst files are imported, that data is merged with the previously imported data. The Zimbra Inbox folder contains all the items from all .pst folders that were imported.

By default, messages larger than 10 MB will not be imported. The message size includes the message and attachments. If the message is larger than 10 MB, a warning is logged to Import Wizard log file.

Any errors or warnings in the import process are displayed on the Import Complete dialog. Users should review items that are listed on this page. If issues need to be investigated, users can click the **Log File** button on this dialog and search the log for details. Once the Wizard is closed, the log file is not longer available.

If a .pst file is run through the Import Wizard more than once, users should check **Ignore previously imported items** on the Import Options dialog so that messages and contacts that have been imported are not imported again.

Outlook Features Not Imported

The following commonly used Outlook features are not imported:

- Meeting requests
- Calendar entries
- Notes
- Tasks
- Rules and alerts
- Other files the user created such as journal entries
- Personal Distribution Lists

Chapter 11 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 a 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 of the mailbox servers. 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.

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. The 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.

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

- Message ID, `-i [msd_id]`
- Sender address (From), `-s [sender_addr]`
- Recipient address (To), `-r [rcpt_addr]`
- IP Address sent from, `-f [ip_address]`
- Date and time, `-t yyyyymmdd{hhmmss}`

The Zimbra email message header can be viewed from the Zimbra Web Client Message view. Right-click on a message and select **Show Original**.

Note: *If messages are viewed by Conversation view, first open the conversation to view the messages. Then select the message.*

Examples

Note: *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

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

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 section to see if you can fix the mail delivery problem. When you open Mail Queues, you see a snapshot of the Deferred, Incoming, Active, Hold, and Corrupt queues content at that point in time. 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 37.

The **Summary** pane shows a summary of messages by receiver domain, origin IP, sender address, receiver address, sender domain, and for the Deferred queue, by error type. Click on any of the summaries to see detailed envelope information by message in the Messages pane. You can also refresh, requeue, hold, or delete all messages listed in the summary pane

The **Messages** pane displays individual message envelope information for search filters selected from the Summary pane. When you right-click on a message, you can select from several options:

- **Hold** to move the message to the Hold queue. Messages stay in this queue until the administrator moves them.
- **Release** to remove a message from the Hold queue. The message is moved to the Deferred queue.

- **Requeue** a message that is in the queue. 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** a message.

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.

Log Files

Zimbra and Zimbra-related processes generate the following types of log files:

- **Local logs** created by each of the following processes
 - Tomcat server logs. By default logs to **/var/log/zimbra.log** and to **/opt/zimbra/log/zimbra.log**. Some Tomcat information is logged to **/opt/zimbra/tomcat/logs/catalina.out**.
 - MySQL binary logs. By default logs to **/var/log/zimbra.log**.
 - Postfix logs. The MTA logs via syslog to the mail facility. By default this is **/var/log/maillog**.
 - OpenLDAP logs. By default logs to **/var/log/zimbra.log**.
- **Syslog** file. This 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. 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.

Logging Levels

The levels for Zimbra logging messages are shown below, along with which ones generate SNMP traps and where, by default, each message type is logged.

Table 1 Zimbra Logging Levels

Level	Local?	Syslog ?	SNMP Trap?	When Used
Critical	Y	Y	Y	A component is down, such as disk full
Error	Y	Y	N	Single user error, unexpected; for example, can't open index
Warning	Y	N	N	Non-fatal error for operation, such as user login failed
Info *	Y	N	N *	Transaction-level logging, such as "user X logged in"
Debug	Y	N	N	Parameters to transactions

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

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.

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*
- Start and stop a service
- Install 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 1 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 mysqlqadmin commands to the logger mysql
mysqladmin	Send admin commands to MySQL
mysql	Enters interactive command-line MySQL session with the mailbox mysql
mysql.server	Start, stop the SQL instance for the mailbox package
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
tomcat	Star, stop, find the status of the Tomcat server
zmamavisdctl	Start, stop, or find the status of the Amavis-D New

Table 1 Zimbra CLI Commands

CLI	Description
zmantispsamctl	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
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
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
zmmailboxctl	Start, stop, reload, or find the status of the mailbox components (Tomcat, MySQL, convert)
zmmsgtrace	Trace messages
zmmtaconfigctl	Start, stop, or find the status of the
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

Table 1 Zimbra CLI Commands

CLI	Description
zmprov	Performs all provisioning tasks in Zimbra LDAP, including creating accounts, domains, distribution lists and aliases
zmsaslauthdctl	Start, stop, status of saslauthd (authentication)
zmshutil	Used for other zm scripts, do not use
zmspellctl	Start, stop, or find the status of the spell check server
zmsshkeygen	Generate Zimbra's SSH encryption keys
zmwatchctl	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, and distribution lists. 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**

In this example, **zmprov ma user1 +zimbraZimletUserProperties testing** 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.

The following commands can be used as subcommands to **zmprov**.

Long Name	Short Name	Syntax, Example, and Notes
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
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
SetPassword	sp	{name@domain id adminName} {password} zmprov sp joe@domain.com test321
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

Long Name	Short Name	Syntax, Example, and Notes
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}]
SearchGAL	sg	{domain} {name} zmprov sg joe
RenameAccount	ra	{name@domain id} {newname@domain} zmprov ra joe@domain.com joe23@domain.com
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
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.
CreateCos	cc	{name} [attribute1 value1 etc] zmprov cc Executive zimbraAttachmentsBlocked FALSE zimbraAuthTokenLifetime 60m zimbraMailQuota 100M zimbraMailMessageLifetime 0

Long Name	Short Name	Syntax, Example, and Notes
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
CreateServer	cs	{name} [attribute1 value1 etc]
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
GetAllConfig	gacf	[-v] All LDAP settings are displayed
GetConfig	gcf	{name}
ModifyConfig	mcf	attr1 value1 Modifies the LDAP settings.
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

Long Name	Short Name	Syntax, Example, and Notes
GetAlldistributionLists	gdl	<code>[-v]</code>
GetDistributionList	gdl	<code>{list@domain id}</code> <code>zmprov gdl list@domain.com</code>
ModifyDistributionList	md	<code>{list@domain id} attr1 value1 {attr2 value2...}</code> <code>zmprov md list@domain.com</code>
DeleteDistributionList	ddl	<code>{list@domain id}</code>
AddDistributionListAlias	adla	<code>{list@domain id} {alias@domain}</code>
RemoveDistributionListAlias	rdla	<code>{list@domain id} {alias@domain}</code>
RenameDistributionList	rdl	<code>{list@domain id} {newName@domain}</code>

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 cd1 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
```

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.

Long Name	Short Name	Description
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 create, **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/tomcat/conf/keystore -keypass zimbra
Next type the following all on one line
keytool -delete -alias tomcat -keystore /opt/zimbra/tomcat/conf/keystore -keypass zimbra
3. Type **zmcreateca**, press **Enter**
4. Type **zmcreatecert**, press **Enter**
5. Type **zmcertinstall mailbox**, press **Enter**
6. Type **tomcat stop**, press **Enter**
7. Type **tomcat start**, press **Enter**

zmlocalconfig (Local Configuration)

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

Syntax

zmlocalconfig [options] [args]

To see the local config type

zmlocalconfig

Description

Long Name	Short Name	Description
--config <arg>	-c	File in which the configuration is stored.
--default	-d	The default values for the keys listed in [args] is listed.
--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 <arg>	-m	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.
--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.
--expand	-x	Expand values.

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.

Syntax

zmtlsetl [mode]

mode = http, https, or mixed

Steps to run

1. Type **zmtlsetl** [mode], press **Enter**.
2. Type **tomcat stop**, press **Enter**.
3. When Tomcat has 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.

zmmylogpasswd

This command is used to change the zimbra_logger_mysql_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_mysql_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 <new_password>.

zmtrainsa

This command is used to train the anti-spam filter. This command is run automatically every night to train the SpamAssassin filter from messages users mark as “junk” “not junk” from their mailbox. See “Anti-Spam Training Filters” on page 35.

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 --add --name <message volume> --type <primaryMessage> --path /<data/msgvol>

Description

Long Name	Long Name Second Attribute	Short Name	Description
--add		-a	Adds a volume

	--name <arg>	-n	Volume name
	--type <arg>	-t	Type of volume, primaryMessage, secondaryMessage, or index. SecondaryMessage is used only when the Network Edition, HSM feature is enabled.
	--path <arg>	-p	File system root path of the volume
	--compress <arg>	-c	Compress blobs, "true" or "false". The default is "false." True means that message blobs whose size are above the compression threshold are compressed.
	--compressionThreshold <arg>	-ct	Compression threshold size is specified in bytes. The default is 4KB
--edit		-e	Edits a volume. Any of the options listed under --add can also be specified to have its volume modified.
	--id <arg>	-id	Volume ID
--delete		-d	Deletes a volume
	--id <arg>	-id	Volume ID
--list		-l	Lists volumes
	--id <arg>	-id	ID is optional. If it is specified, just that volume is listed. If not, all volumes are displayed.
--displayCurrent		-dc	Displays the current volumes
--setCurrent		-sc	Sets the volume specified by --id to be the current volume of its volume type.
	--id <arg>	-id	Volume ID
--turnOffSecondary		-ts	Turns off the current secondary message volume. After this command completes, no current secondary volume is enabled.

zmzimletctl

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

Syntax

zmzimletctl {command} <zimletname> <arg>

Description

Long Name	Short Name	Description
deploy <zimletname>		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		Uninstall a zimlet from the Zimbra server
install		Installs the Zimlet files on the host
ldapDeploy		Adds the Zimlet entry to the LDAP
acl		Sets the access control, grant deny, to a COS
enable		Enables the Zimlet
disable		Disables the Zimlet.
listAcls		Lists the ACLs for the Zimlets
listZimlets		Shows the status of all the Zimlets on the server
getConfigTemplate		Extracts the configuration template from the Zimlet.zip file
configure		Installs the configuration
listPriority		Shows the current Zimlet priorities (0 is high, 9 is low)
setPriority		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 mail-box 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, meta-data 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.

OOO

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

A

- account authentication 23
- account distribution by COS 51
- account quota and MTA 34
- account status 52
- account, provision with zmprov 82
- accounts object 25
- accounts, list all 83
- accounts, user 41
- adding user accounts 49
- admin console, tasks 41
- admin password, change 83
- administration console 39
- administration functions 10
- administrator password, change 40
- advanced feature options 57
- alias, add with zmprov CLI 82
- anti-spam component 10
- anti-spam configuration 45
- anti-spam protection 34
- anti-spam statistics 70
- anti-spam training filter 35
- anti-virus component 10
- anti-virus configuration 45
- anti-virus protection 34
- anti-virus statistics 70
- anti-virus updates 34, 46
- application packages, Zimbra 11
- attachment blocking 44
- attachments, mail 44
- authentication 23
- authentication modes 47

B

- backup files 20
- batch provisioning new accounts 50
- blocking attachments 44
- blocking by extension 44
- bounced delivery report 72

C

- change administrator password 40
- change zimlet configuration 63
- changing account status 52
- changing password 51
- Clam AntiVirus software 34
- class of service 50
 - about 26, 50
- class of service object 26
- class of service, COS 41
- CLI commands, provisioning 78
- CLI commands, start/stop service 83
- CLI utilities 75
- company director 27
- components, Zimbra 10
- configuration, typical example 15
- Connector for Outlook 67
- contact 8
- contact quota 52
- core functionality 9
- COS, denying access from a zimlet 65
- COS, list all 83
- creating accounts 50

D

- daily mail report 71
- data store 12, 18
 - about 18
 - file location 14
- deploying zimlets 63
- directory structure 13
- disable attachment 44
- distribution list, create with zmprov CLI 82
- disk layout 17
- distribution lists object 26
- documentation 7
- domain, create with zmprov CLI 83
- domain, set default with zmprov CLI 83
- domains object 26
- DSPAM 34

E

- edge MTA 32
- email aliases 59
- email forwarding 59
- equipment resources 53
- error report, daily 72
- external AD account authentication 24
- external LDAP account authentication 24

F

- features, administrative 10
- features, advanced options 57
- features, core 9
- features, mailbox 55
- features, web client 10

G

- GAL 27
 - LDAP search filter used 27
 - search options 27
 - search parameter settings 28
 - Zimbra attributes 28
- GAL attributes 28
- GAL mode 46
- global configuration object 27
- global settings 41

H

- ham mailbox 35
- horizontal scalability 9
- HTML 59

I

- IMAP 45
- incoming mail routing 17
- index store 12, 19
 - file location 14
- index/search
 - back-end technologies used 19
- indexing 19
- install certificate, CLI 84
- installing ZCS Connector for Outlook 67
- installing zimlets 63
- internal account authentication 24
- internal authentication mechanism 24

K

- kill percent for spam 34

L

- LDAP

- directory traffic 22
- hierarchy 22
- implementation 22
- overview 21
- schema include files for Zimbra 23
- Zimbra schema, overview 26

- LDAP schema 23
- local configuration, CLI 85
- location resources 53
- log files 20
- logger 69
- logging levels 73
- logging on to admin console 40
- Lucene 19

M

- mail report 71
- mail report, change 72
- mailbox features 55
- Mailbox move 52
- mailbox quotas
 - specifying 52
- mailbox quotas, monitoring 72
- mailbox server, overview 17
- mailbox, move 52
- main.cf file 32
- management tasks 41
- management tasks from CLI 42
- master.cf file 32
- message count 70
- message store 11, 12, 18
 - about 18
 - file location 14
- message store, single-copy 18
- message trace 70
- message trace, CLI 86
- message volume 70
- messages received and sent report 72
- MIME format 12
- modes, set with `zmctl` CLI 86
- monitoring quotas 72
- monitoring tool 69
- moving mailbox 52
- MTA 11
- MTA functionality 32
- MTA package, Zimbra 11
- MTA queues 37
- MySQL 12

N

- navigation pane 41

O

open source components 10

P

password, admin change 83
password, changing admin 40
POP 45
Postfix 31
Postfix configuration files 32
postfix error report 72
preferences 58
product overview 9
protocol, set with CLI 86
provisioning, CLI commands 78

Q

queues 37
quotas, mailbox, contact 52
quotas, monitoring 72

R

recipient object 26
recipients, most active report 72
redo log 20
reject message 44
relay host settings 33
removing zimlets 65
report, daily mail 71
resources, managing 53

S

schema LDAP 23
search for accounts 49
self-signed certificate, CLI 84
senders, most active report 72
server statistics, statistics 70
server status 69
service, start/stop 83
setting up zimlets 63
single-copy message storage 18
single-copy store 18
skype 66
smart host 33
SMTP authentication 33
SMTP restrictions 33
SNMP monitoring 73, 74
SNMP package, Zimbra 12
SNMP traps, error 74
spam configuration settings 34
spam mailbox 35
spam training filter 35

spam training, CLI 87
spam, turning on/off training attributes 35
SpamAssassin 34
start service 83
statistics 41
status 41
stop service 83
store package 11
support 8
system architecture 11
system architecture graphic 13

T

tasks from admin console 41
third-party software bundled with 10
tracing messages 70
transaction log 20

U

updating anti-virus software 34, 46
user accounts, managing 49
user preference list 59

V

view mailbox from admin console 52
volumes, managing with CLI 87

W

Web client features 10

Z

Zimbra logger 69
Zimbra monitor host 69
Zimbra MTA 31
Zimbra objects, ldap 25
Zimbra Schema 23
zimlets 63
zimlets included with ZCS 65
zimlets, disabling 65
zimlets, viewing a list 65
zmpov CLI 78
zmtrainsa spam training tool 35

