



Zimbra™ Collaboration Suite Administrator's Guide

**Release 4.5
Network Edition
January 2007**

Legal Notices

Copyright Zimbra, Inc. 2005 - 2007. 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.

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.

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 software.

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

Zimbra Administration Guide Table of Contents

Chapter 1 Introduction	9
Intended Audience	9
Zimbra Collaboration Suite License	9
Available Documentation	10
Support for Recommended Third-Party Components	10
Support and Contact Information	10
Chapter 2 Product Overview	13
Core Functionality	13
Zimbra Components	15
System Architecture	15
Zimbra Core	15
Zimbra LDAP	15
Zimbra MTA (mail routing server)	16
Zimbra Store (Zimbra server)	16
Zimbra-SNMP	17
Zimbra Logger	17
Zimbra Spell	17
Backup Process Overview	17
Zimbra System Directory Tree	18
Example of a Typical Multi-Server Configuration	20
Chapter 3 Zimbra Server	23
Zimbra Licenses	23
Incoming Mail Routing	24
Disk Layout	24
Message Store	24
Data Store	25
Index Store	25
Backup	26
Redo Log	26
Log	27
Chapter 4 Zimbra Directory Service	29
Directory Services Overview	29
LDAP Hierarchy	30
Zimbra Schema	31
Account Authentication	31
The Internal Authentication Mechanism	32
External LDAP and External Active Directory Authentication Mechanism	32
Zimbra Objects	33
Company Directory/GAL	35

Chapter 5	Zimbra MTA	39
	Zimbra MTA Deployment	39
	Postfix Configuration Files	40
	MTA Functionality	40
	SMTP Authentication	41
	SMTP Restrictions	41
	Relay Host Settings	41
	MTA-LDAP Integration	41
	Account Quota and the MTA	42
	MTA and Amavisd-New Integration	42
	Anti-Virus Protection	42
	Anti-Spam Protection	42
	Receiving and Sending Mail through Zimbra MTA	45
	Zimbra MTA Message Queues	45
Chapter 6	Using the Administration Console	47
	Administrator Accounts	47
	Global Administrator	47
	Domain Administrator	47
	Logging on	48
	Changing Administrator Passwords	48
	About the Administration Console	48
	Management Tasks from the Administration Console	50
	Management Tasks Not Available from Administration UI	51
Chapter 7	Managing ZCS Configurations	53
	Managing Global Configurations	53
	General Global Settings	54
	Global Attachment Settings	54
	Global MTA Settings	55
	Global IMAP and POP Settings	55
	Anti-Spam Settings	56
	Anti-Virus Settings	57
	License Information	57
	Global HSM Session Setting	58
	Managing Domains	58
	Global Address List (GAL) Mode	58
	Authentication Modes	58
	Virtual Hosts	59
	Documents	59
	Managing Servers	60
	General Server Settings	60
	Services Settings	60
	MTA Server Settings	60
	IMAP and POP Server Settings	61
	Volume Settings	61
	Managing Other Functions	62
	Zimlets	62
	Admin Extensions	62

Chapter 8 Managing User Accounts	63
Setting up and Configuring Accounts	64
Manage Aliases	65
Class of Service	65
Changing Password	66
View an Account's Mailbox	66
Re indexing a Mailbox	66
Changing an Account's Status	66
Deleting an account	67
Enforcing Mailbox and Contact Quotas	67
Moving a Mailbox	67
Managing Distribution Lists	68
Using Distribution Lists for Group Sharing	68
Managing Resources	69
Searching for Addresses	69
 Chapter 9 Customizing Accounts and Setting General Preferences and Password Rules	 71
Zimbra Messaging and Collaboration Applications	71
Email messaging	71
Address Book	75
Calender	76
Documents	77
General Configuration Settings for Accounts	78
Setting Account Quotas	78
Setting Password Policy	78
Setting Failed Login Policy	80
Setting Session Lifetime	80
Setting Attachment Viewing Options	81
Zimbra Web Client UI Themes	82
Zimbra Mobile	82
Configuring Zimlets for Accounts	83
 Chapter 10 Working with Zimlets	 85
Setting Up Zimlets in ZCS	85
Managing Zimlets from the Administration Console	85
Managing Zimlets from the Command Line	86
Configuring a Zimlet	87
Disabling or Removing a Zimlet	87
Zimlets Included with ZCS	88
 Chapter 11 Monitoring Zimbra Servers	 89
Zimbra Logger	89
These steps are not necessary for a single-node installation.	90
Reviewing Server Status	90
Server Performance Statistics	90
Tracing Messages	90
Generating Daily Mail Reports	92
Monitoring Mailbox Queues	93
Flushing the Queues	94
Monitoring Mailbox Quotas	94

Log Files	94
Using log4j to Configure Logging	95
Logging Levels	95
SNMP	96
SNMP Monitoring Tools	96
SNMP Configuration	96
Errors Generating SNMP Traps	96
Chapter 12 Backup and Restore	97
Zimbra Backup and Restore	98
Directory Structure for Backup Files	99
Backup and Restore from the Administration Console	101
Backup and Restore Using the Command Line Interface	101
Scheduling Backups	102
Backing up the Mailbox Server	102
Full Backup Process	103
Incremental Backup Process	103
Finding Specific Backup Files	104
Aborting Full Backup In Progress	105
Restoring the Files	105
Restore Process	105
Stopping a Restore Process	108
Restoring the LDAP Server	109
Disaster Recovery for Specific Situations	109
General Steps for Disaster Recovery	109
Crash Recovery Server Startup	110
Restore the Zimbra Collaboration Suite Servers	110
Restoring Individual Accounts on a Live System	110
Restoring from Different Failure Scenarios	111
Changing Local Configuration Files after Restoring Zimbra	112
Appendix A Command-Line Utilities	113
Zimbra CLI Commands	114
zmprov (Provisioning)	117
zmmailbox	124
zmaccts	126
zmbbackup	126
zmschedulebackup	128
zmbbackupabort (Aborting a Full Backup)	129
zmbbackupquery	130
zmrestore	131
zmrestoreoffline (Offline Restore)	133
zmrestoreldap	134
zmcontrol (Start/Stop Service)	135
zmmailboxmove (Move Mailbox)	135
zmmailboxsearch (Cross mailbox search)	136
zmcreatecert and zmcertinstall (For a Certificate)	137
zmlocalconfig (Local Configuration)	138
zmtlsctl	139
zmhsm	139
zmlicense	140
zmmsgtrace	140

zmmylogpasswd	141
zmmypasswd	141
zmtrainsa	142
zmvolume	142
zmzimletctl	143
 Appendix B Glossary	 145
 Index	 151

Chapter 1 Introduction

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

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, SUSE operating systems, and open source concepts
- Industry practices for mail system management

Zimbra Collaboration Suite License

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

A trial and a regular license are available:

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

Also see the ["Zimbra Server" chapter, Zimbra Licenses](#).

Go to Zimbra's website to obtain a trial license from the Network Downloads link. Contact Zimbra Sales to purchase a regular license, email sales@zimbra.com or telephone 1 650-212-7767, extension 100.

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 Guides*. The guides provides instructions for running the Migration Wizard to migrate accounts from either Microsoft Exchange servers or Lotus Domino servers.
- *Zimbra administration console Help*. The Help topics describes how to perform tasks required to centrally manage Zimbra servers and mailbox accounts from the administration console.
- *Zimbra Web Client Help*. The Help topics describes how to use the features of the Zimbra Web Client.
- *Release Notes*. Late-breaking news for product releases and upgrade instructions are contained in the release notes. The latest notes can be found on the Zimbra website, www.zimbra.com.

Support for Recommended Third-Party Components

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

Support and Contact Information

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

- Contact sales@zimbra.com to purchase Zimbra Collaboration Suite
- Network Edition customers can contact support at support@zimbra.com
- Explore the Zimbra Forums for answers to installation or configurations problems
- Join the [Zimbra Community Forum](#), to participate and learn more about the Zimbra Collaboration Suite.

- Send an email to feedback@zimbra.com to let us know what you like about the product and what you would like to see in the product. Or, if you prefer, post your ideas to the Zimbra Forum.

If you encounter problems with this software, 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.
- **High availability support.** Red Hat Cluster Suite is integrated with ZCS, for cluster management.
- Browser based client interface.
- Administration console to manage accounts and servers.

Core Functionality

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

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

The core functionality within the Suite is as follows:

- Mail delivery and storage
- Indexing of mail messages upon delivery
- Backup services
- Mailbox server logging
- IMAP and POP support
- Directory services
- Anti-spam protection
- Anti-virus protection

Administrators can easily manage domains, servers, and accounts from the browser based administration console and can manage backup, bulk provision accounts, and perform cross-mailbox searches from the Command Line Utility.

- Delegate a Domain Administrator
- Move mailboxes from one server to another
- Import Microsoft Exchange user accounts
- Add accounts and domains
- Set account restrictions either for an individual account or by COS
- Manage distribution lists
- Set up virtual hosts on a domain
- Manage servers
- Define policies for moving older messages to secondary storage
- Backup and restore accounts
- Monitor usage

The Zimbra Web Client mail features include the ability to:

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

Zimbra Components

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

- 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.
- Verity®, a third-party source that converts certain attachment file types to HTML.
- 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
- HTML attachment conversion utility

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). Any attachments to the mail message are scheduled to be converted to HTML, and then the HTML version is scheduled to be indexed.

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.

HTML conversion. As each email message arrives, the Zimbra server schedules a thread to have the message indexed. Any attachments to the mail message are scheduled to be converted to HTML, and then the HTML version is scheduled to be indexed.

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

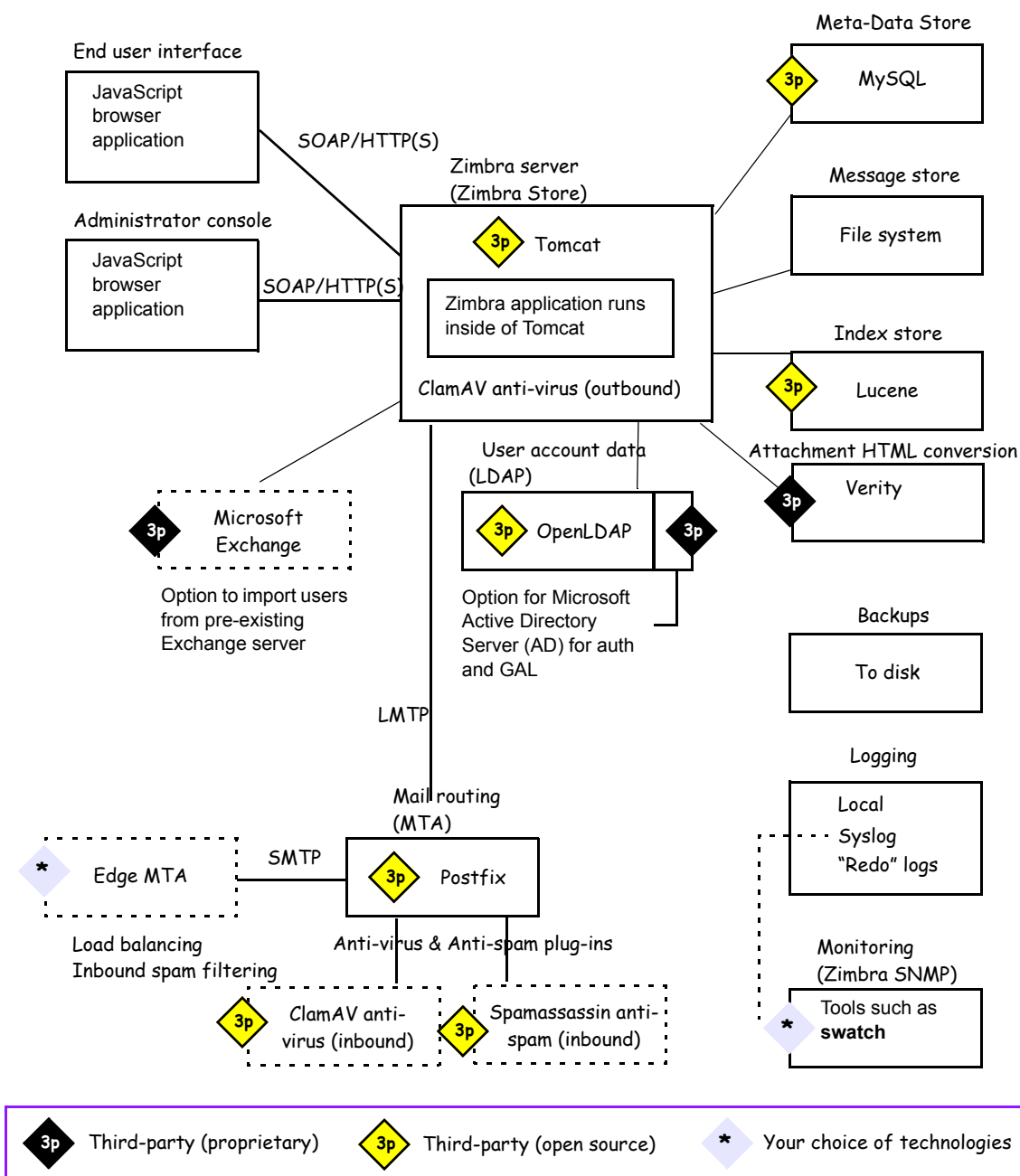
Installing the Zimbra Logger package is optional and is installed on one mailbox server. The Zimbra logger installs tools for syslog aggregation, reporting, and message tracing. If you do not install Logger, you cannot use the message trace feature. In addition, the server statistics are not captured,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

Backup Process Overview

Zimbra includes a configurable backup manager that resides on every Network Edition Zimbra server and performs both backup and restore functions. You do not have to stop the server in order to run the backup process. You can use the backup manager to restore a single user in the event that one user's mailbox becomes corrupted. See [Chapter 12, Backup and Restore](#).

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

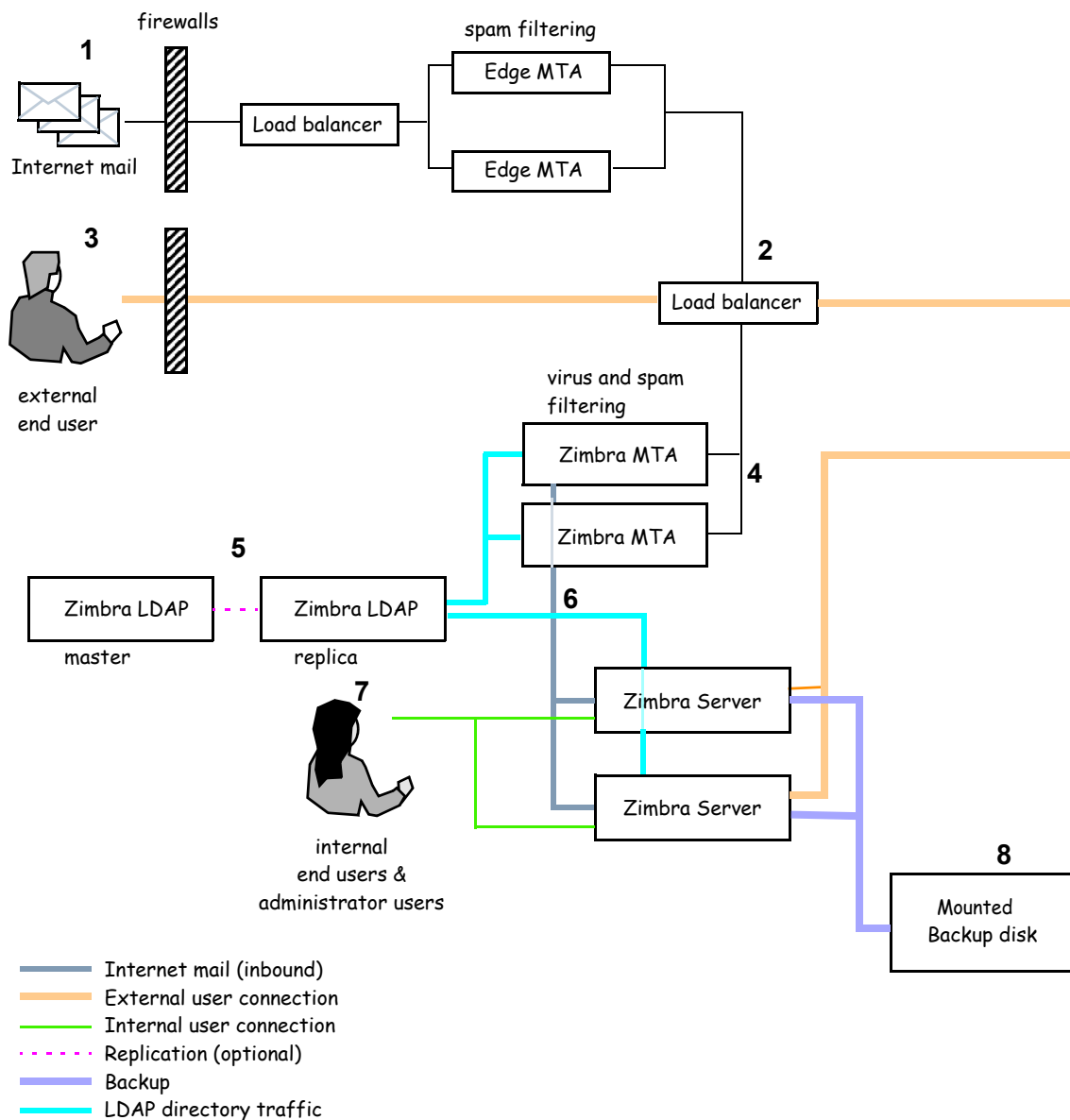
Parent	Directory	Description
/opt/ zimbra/		Created by all Zimbra installation packages
	backup/	Backup target contains full and incremental backup data
	bin/	Zimbra application files, including the command-line utilities described in Appendix A, Command - Line Utilities.
	clamav	Clam AV application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

Parent	Directory	Description
	postfix/	Postfix server installation, pre-configured to work with Zimbra
	redolog/	Contains current transaction logs for the Zimbra server
	sleepycat/	Berkeley DB
	snmp/	SNMP monitoring files
	ssl/	Certificates
	store/	Message Store
	tomcat/	Tomcat application server instance. The webapps/zimbra/skins directory includes the Zimbra UI themes files
	verity	Files that are being converted by Verity
	wiki	Contains the Zimbra Documents global template file
	zimbramon/	Contains the control scripts and Perl modules
	zimlets	Contains zimlet zip files that are installed with Zimbra
	zimlets-extra	Contains zimlet zip files that can be installed
	zimlets-network	Contains zimlet zip files for features that are installed with the network edition.

Example of a Typical Multi-Server Configuration

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

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

Figure 2: Typical Configuration with Incoming Traffic and User Connections

Explanation of Figure 2 follows.

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

-
- 5 The designated Zimbra MTA server looks up the addressee's directory information from the Zimbra LDAP replica server.
 - 6 After obtaining the user's information from the Zimbra LDAP server, the MTA server sends the mail to the appropriate Zimbra server.
 - 7 Internal end-user connections are made directly to any Zimbra server which then obtains the user's directory information from Zimbra LDAP and redirects the user as needed.
 - 8 Zimbra servers' backups can be processed to a mounted disk.

Chapter 3 Zimbra Server

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

In addition to content management, the Zimbra mailbox server has dedicated volumes for backup and log files.

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.

Zimbra Licenses

A Zimbra license is required in order to create accounts. See “Zimbra Collaboration Suite License” on page 9 for a description of the license types.

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

When you purchase, renew, or change the Zimbra license, you must update the Zimbra server with the new license information. Use the **Update License Wizard** from the administration console’s Global Settings to upload and install a new license and to update an existing license, or you can install or update the license using the **zmlicense** CLI command. See Appendix A, CLI Commands, “zmlicense” on page 140 to use the CLI command.

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`
- **Backup Area.** Full and incremental backups are in `opt/zimbra/backup`
- **Log files.** Each component in the Zimbra Collaboration Suite has log files. Local logs are in `/opt/zimbra/log`

Note: *The system logs, the redo logs, and the backup disk should be on separate disks to minimize the possibility of unrecoverable data loss in the event that one of those disks fails.*

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.

Hierarchical Storage Management

Hierarchical Storage Management (HSM) allows you to configure storage volumes for older messages. To manage your email storage resources, you can implement a different HSM policy for each message server. Messages and attachments are moved from a primary volume to the current secondary volume based on the age of the message. The messages are still accessible.

Data Store

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

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

The Data Store contains:

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

Index Store

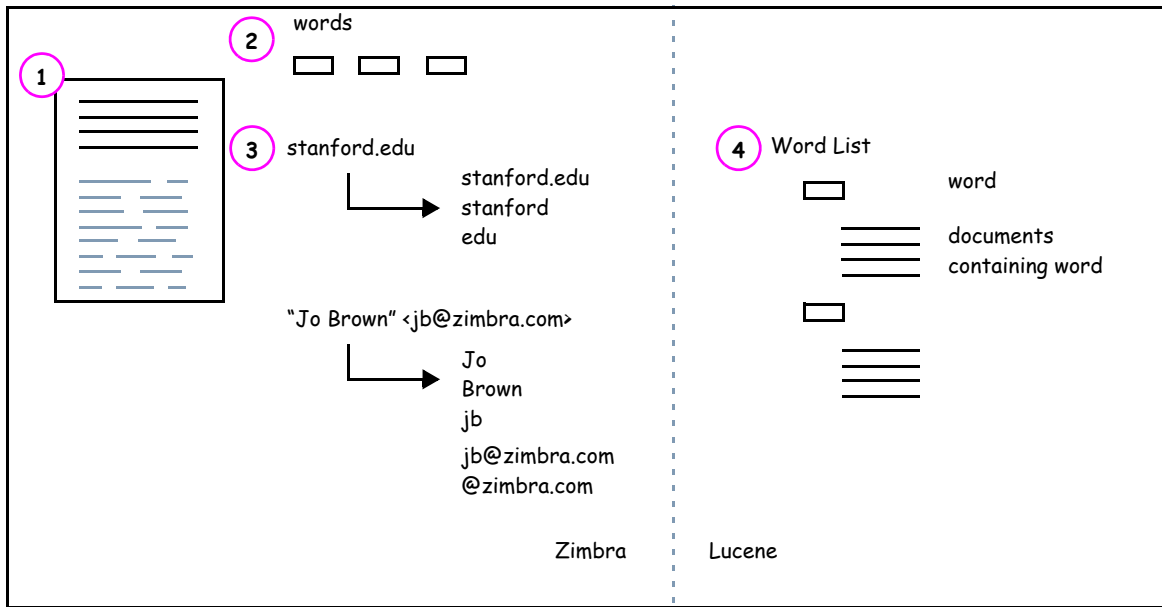
The index and search technology is provided through Apache Lucene. Each message is automatically indexed as it enters the system. Each mailbox has an index file associated with it.

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

The process is as follows:

1. The Zimbra MTA routes the incoming email to the Zimbra mailbox server that contains the account's mailbox.
2. The mailbox server parses the message, including the header, the body, and all readable file attachments such as PDF files or Microsoft Word documents, in order to tokenize the words.
3. The mailbox server passes the tokenized information to Lucene to create the index files.

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

Figure 3: Message tokenization

Backup

Zimbra includes a configurable backup manager that resides on every Zimbra server and performs both backup and restore functions. You do not have to stop the Zimbra server in order to run the backup process. The backup manager can be used to restore a single user, rather than having to restore the entire system in the event that one user's mailbox becomes corrupted. See [Chapter 12, Backup and Restore](#).

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.

When an incremental backup is run, the redo logs are moved from the archive to the backup directory.

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 11, 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.

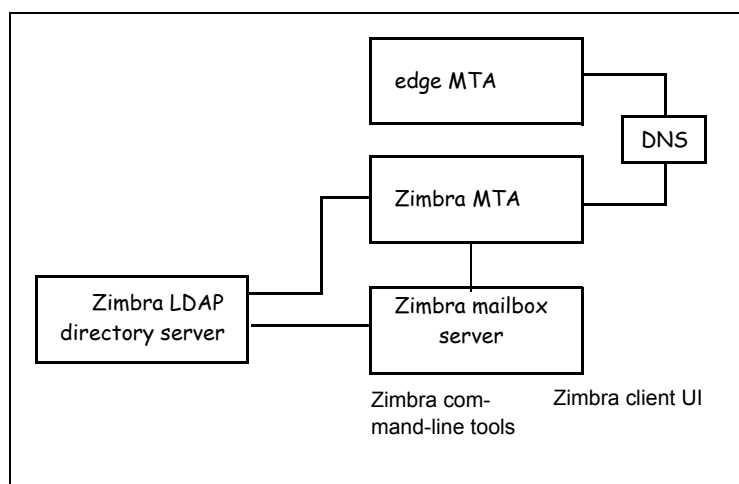
Directory Services Overview

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 4: LDAP Directory Traffic



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

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

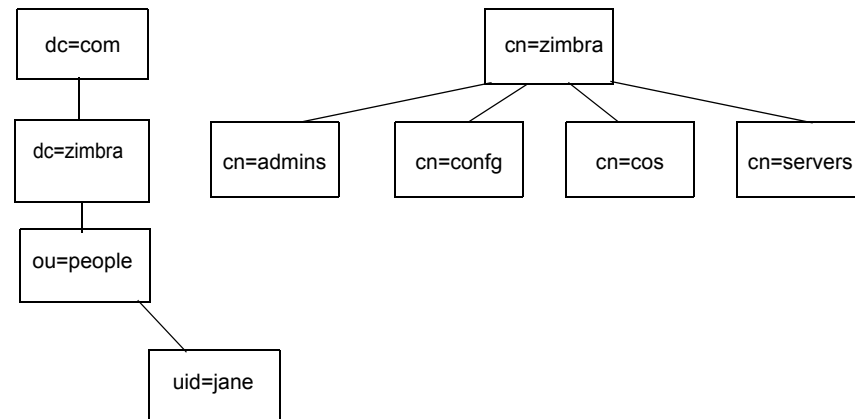
The object classes determine what type of object the entry refers to and what type of data can be stored for that entry. An entry's object classes that determines what kind of entry it is, is called a structural object class and cannot be changed. Other object classes are called auxiliary and may be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

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

LDAP Hierarchy

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

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

Figure 5: Zimbra LDAP Hierarchy

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

Zimbra Schema

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

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

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

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

Note: You cannot modify the Zimbra schema.

Account Authentication

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

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

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

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

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

The Internal Authentication Mechanism

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

External LDAP and External Active Directory Authentication Mechanism

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

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

zimbraAuthLdapURL Attribute and SSL

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

`ldap://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
- TimeZone
- Zimlet
- CalendarResource

Accounts Object

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

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

All accounts have the following properties:

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

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

For more about account provisioning, see the [Chapter 8, Managing User Accounts](#).

Class of Service (COS) Object

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

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

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

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

Domains Object

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

Distribution Lists Object

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

Recipient Object

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

Servers Object

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

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

Global Configuration Object

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

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

Alias Object

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

TimeZone Object

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

Zimlet Object

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

CalendarResource Object

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

Company Directory/GAL

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

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

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

GAL Searches in Zimbra Client

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

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

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

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

GAL Attributes in Zimbra

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

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

Table 1 Attributes Mapped to Zimbra contact

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

Table 1 Attributes Mapped to Zimbra contact

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

Zimbra GAL Search Parameters

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

Modifying Attributes

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

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

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

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

Chapter 5 Zimbra MTA

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

The Zimbra MTA server includes the following programs:

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

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

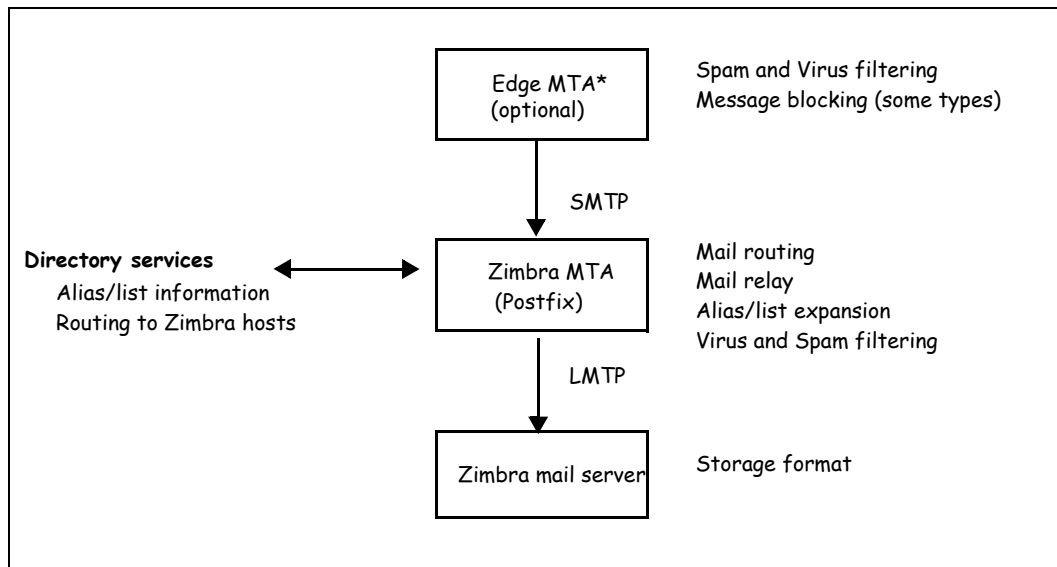
MTA configuration is stored in LDAP and a configuration script automatically polls the LDAP directory every two minutes for modifications, and updates the Postfix configuration files with the changes.

Zimbra MTA Deployment

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

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

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

Figure 6: Postfix in a Zimbra Environment

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

Postfix Configuration Files

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

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

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

MTA Functionality

Zimbra MTA Postfix functionality includes:

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

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

SMTP Authentication

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

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

SMTP Restrictions

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

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

Relay Host Settings

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

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

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

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

MTA-LDAP Integration

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

Account Quota and the MTA

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

MTA and Amavisd-New Integration

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

Anti-Virus Protection

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

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

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

Anti-Spam Protection

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

The SpamAssassin default configuration for ZCS is as follows:

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

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

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

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

Anti-Spam Training Filters

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

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

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

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

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

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

```
zmprov mcf <attribute> ''
```

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

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

The **zmtrainsa** command can be run manually to forward any folder from any mailbox to the spam training mailboxes.

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

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

To send a folder 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 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 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

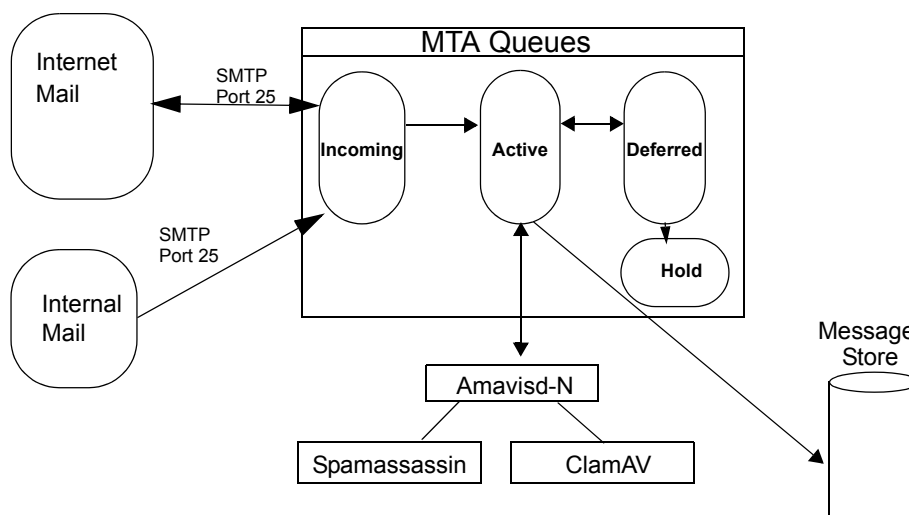
The Zimbra MTA delivers both the incoming and the outgoing mail messages. For outgoing mail, the Zimbra MTA determines the destination of the recipient address. If the destination host is local, the message is passed to the Zimbra server for delivery. If the destination host is a remote mail server, 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 93.

Chapter 6 Using the Administration Console

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

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

Administrator Accounts

Only accounts designated as administrator can log on to the administration console to manage accounts and server configurations. Two kinds of administrator accounts can be created:

- Global Administrators, who have full privileges to manage servers, global settings, domains, and accounts. One global administrator account is initially created when the software is installed. Additional administrator accounts can be created.
- Domain Administrators, who can create, modify, and delete accounts for a specific domain.

The administrator type is designated when an account is created.

Global Administrator

A global administrator manages servers, global configuration, all domains and accounts. Administration tasks can be performed either from the administration console or using the Zimbra command-line interface tools. The global administrator can delegate a user as a domain administrator. More than one global administrator can be configured.

Domain Administrator

Domain administrators can create and maintain accounts, aliases, distribution lists, and calendar resources for accounts in their domain. The Zimbra global administrator configures the domain's global settings and COS features and preferences. All accounts on the domain are assigned the same COS. The domain administrator cannot view or modify this information.

The global administrator can give the domain administrator privileges to set mail quotas for accounts. The global administrator sets the maximum quota that can be configured for an account.

All tasks are performed from the administration console. Domain administrator see only the functions they can maintain, Accounts, Aliases, Distribution Lists, and Resources. Help topics explain delegated administrator tasks.

The domain administrator can access the following utilities on the Downloads page to be used for accounts on domains they administer:

- Migration wizards to migrate email accounts from Microsoft® Exchange or Lotus® Dominoes® servers to their ZCS accounts.
- Import wizard to let users import the contents of their .pst files from Microsoft Outlook 2003 mailboxes to ZCS accounts.
- Connector for Outlook to let users access their account and synchronize data to and from Microsoft® Outlook
- Connector for Apple® iSync so that Mac users can access their address books and calendar information and synchronize data to and from the Mac

Logging on

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

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

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

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

Changing Administrator Passwords

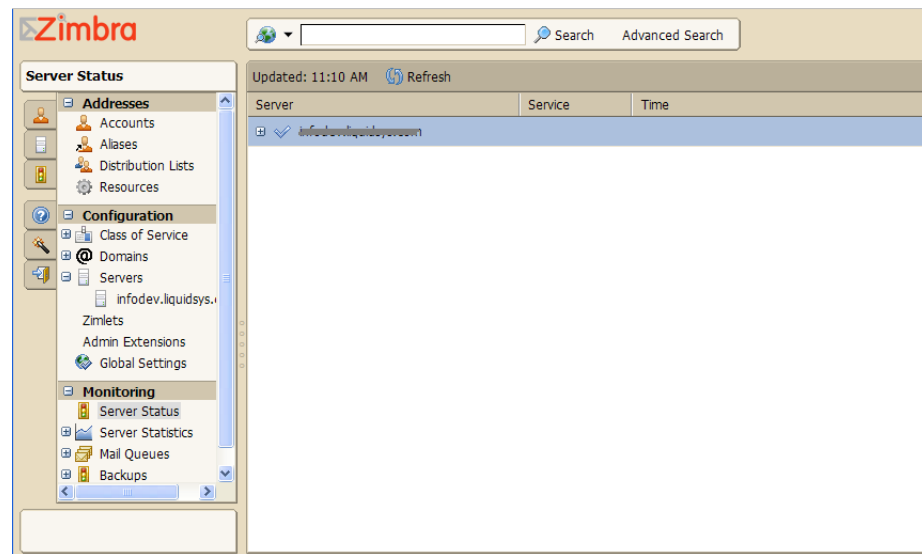
The administrator password is created when the Zimbra software is configured during installation. The password can be changed at any time from the **Accounts** toolbar. Select the account and change the password.

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

About the Administration Console

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

Note: Domain administrators can only access the Addresses and Downloads sections on the administration console.

Figure 7: Administration Console - First Page Displayed

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 be used for that domain.
- **Servers.** Lists the servers, the host name and description. You can configure services, MTA, SMTP, IMAP, and POP features for servers.
- **Zimlets.** You can add new Zimlets, set access privileges by COS and by individual accounts and disable and uninstall Zimlets from ZCS.
- **Admin Extensions.** You can create custom modules to add to the Zimbra administration console user interface. You can use the administration console to easily upload and install your modules

- **Global Settings.** From the Global Settings folder, you set the global defaults rules for GAL search results, acceptance of incoming attachments, for MTA, POP, IMAP, anti-spam and anti-virus configuration. These default settings are used when personal options and COS settings are not set.
- **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.
- **Backups.** You can immediately start a full or incremental backup, restore mailboxes, and abort a backup that is in progress.

Search and **Advanced Search** allow you to quickly find accounts, aliases, distribution lists and resources for editing.

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

Management Tasks from the Administration Console

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

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

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**
- Move a mailbox, CLI **zmprov**
- Cross mailbox searches, CLI **zmmboxsearch**
- Message tracing, CLI **zmmsgtrace**

Chapter 7 Managing ZCS Configurations

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

- Global configuration
- Domains
- Servers
- Zimlets
- Admin Extensions

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

Managing Global Configurations

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

Global settings that can be configured include:

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

- License information, including the account limit and the number of accounts used.
- Set the global HSM schedule for when messages should be moved to a secondary storage space.

You can view the current Zimbra license information, update the license if necessary and view the number of accounts created in Global Settings.

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

General Global Settings

In the General tab configure the **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.

Global Attachment Settings

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

The attachment settings are as follows:

- **Attachments cannot be viewed regardless of COS.** Users cannot view any attachments. This global setting can be set to prevent a virus outbreak from attachments, as no mail attachments can be opened.
- **Attachments are viewed in HTML regardless of COS.** Email attachments can only be viewed in HTML. The COS may have another setting but this global setting overrides the COS setting.
- Attachments are viewed according to COS. This global settings states the COS sets the rules for how email attachments are viewed.

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

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

Global MTA Settings

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

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

Global IMAP and POP Settings

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

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

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

Configuring IMAP and POP Proxy Server

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

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

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

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

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

Table 1 Zimbra IMAP/POP Proxy Server Port Mapping

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

Anti-Spam Settings

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

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

When a message is tagged as spam, the message is delivered to the recipient's Junk folder. Users can view the number of unread messages that

are in their Junk folder and can open the Junk folder to review the messages marked as spam. If you have the anti-spam training filters enabled, when they add or remove messages in the Junk folder, their action helps train the spam filter. See “Anti-Spam Protection” on page 42.

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 44.

Anti-Virus Settings

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

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

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

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

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

License Information

A Zimbra license is required in order to create accounts. When you purchase, renew, or change the Zimbra license, you must update the Zimbra server with the new license information. The **Update License Wizard** from the administration console’s Global Settings is used to upload and install a new license and to update an existing license, or you can install or update the license using the **zmlicense** CLI command. See Appendix A, CLI Commands, “zmlicense” on page 140 to use the CLI command.

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

When the number of accounts created is equal to the number of accounts purchased you will not be able to create new accounts. You can purchase additional accounts or you can delete existing accounts. Contact Zimbra sales to purchase additional accounts.

You must renew your license within 30 days of the expiration date. Starting 30 days before the license expires, when you log on to the administration console, a reminder notice is displayed.

Global HSM Session Setting

Global Settings HSM (Hierarchical Storage Management) sets the default message age thresholds to 30 days. The HSM global setting is the default unless you change the schedule in the Server configuration. See “Scheduling HSM Sessions” on page 61.

Managing Domains

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

For domains, you configure the Global Address List mode, the authentication mode, virtual domains and create a Domain Documents account. You can assign a COS to the domain and have the COS automatically assigned to accounts created on the domain.

Global Address List (GAL) Mode

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

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

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

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

Authentication Modes

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

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

Virtual Hosts

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

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

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

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

Documents

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

The Documents application consists of a Global Documents account which holds the templates, one optional domain Documents account per domain, and Documents Notebooks.

The Global Documents account is automatically created when ZCS is installed. Documents is enabled from the COS or for individual accounts.

One domain Documents account can be created per domain. The domain Documents Notebook folder can be used to collect, organize, and share information with your users. You can set access for the following for each Documents notebook: all users in your domain, all users in the ZCS environment, public view-only, individual user, and distribution lists for groups. You can change the access permissions at any time from the administration console.

One domain Documents account can be created per domain. The domain Documents Notebook folder can be used to collect, organize, and share information with your users. You can set access for the following for each Documents notebook: all users in your domain, all users in the ZCS environment, public view-only, individual user, and distribution lists for groups.

You can view and change the access permissions at any time from the administration console.

Managing Servers

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

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

The server settings include:

- General information about the service host name, and LMTP advertised name and bind address.
- A list of enabled services
- Determining how authentication should work for the server, setting a web mail MTA hostname different from global, setting relay MTA for external delivery, and enabling DNS lookup if required.
- Enabling Pop and IMAP and setting the port numbers for a server. If IMAP/POP proxy is set up, making sure that the port numbers are configured correctly.
- Adding and configuring new index and message volumes.

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

General Server Settings

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

Services Settings

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

MTA Server Settings

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

IMAP and POP Server Settings

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

Volume Settings

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

Index Volume

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

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

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

Message Volume

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

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

Scheduling HSM Sessions

HSM can be configured for secondary storage volumes for older messages. Messages and attachments are moved from a primary volume to the current secondary volume based on the age of the message. Users are not aware of any change and do not see any noticeable difference when opening an older message that has been moved.

To manage your email storage resources, you can implement a different HSM policy for each mailbox server. The message age threshold for HSM is set globally on the HSM tab or for individual servers from the Server, Volume tab.

The default is 30 days. The thresholds configured on individual servers override the threshold configured as the global setting.

Sessions to move messages to the secondary volume are scheduled in your cron table. From the administration console, when you select a server, you can manually start a session, monitor sessions, and abort sessions that are in progress from the Volumes tab.

Managing Other Functions

Zimlets

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

Admin Extensions

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

Note: Go to the Zimbra wiki, [Extending Admin UI](#) for documentation about how to create an extended admin UI module.

Chapter 8 Managing User Accounts

You create accounts and configure features and access privileges from either the administration console or using CLI commands. The following are some of the account tasks you perform from the administration console:

- Quickly create new accounts with the **New Account Wizard**
- Find a specific account using the **Search** feature
- Change account information
- Add or delete an account to multiple distribution lists at one time, and view which lists the account is on
- Create, change, and move alias addresses
- Change password for a selected account
- View an account's mailbox
- Change an account's status
- Reindex a mailbox
- Delete an account

See the ZCS administration console Help for information about how to perform these tasks from the administration console.

The following CLI commands are also available to help facilitate account management.

- The CLI **zmprov** can be used to manage accounts, aliases, distribution lists, and calendar resources.
- The CLI **zmmailboxmove** command is used to move a mailbox.
- The CLI **zmmboxsearch** is used to search across mailboxes to find messages and attachments that match specific criteria and then save copies of these messages to a directory.
- The CLI **zmmailbox** command can be used for mailbox management. This command can help you provision new mailboxes, debug issues with a mailbox, and help with migrations. You can invoke **zmmailbox** from within **zmprov**.

See ["" chapter, Appendix A Command-Line Utilities](#) for information about how to use these commands.

Setting up and Configuring 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.

For a description of the features see [Chapter 9, Customizing Accounts and Setting General Preferences and Password Rules](#).

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.

Manage Aliases

An email alias is an email address that redirects all mail to a specified mail account. An alias is not an email account. Each account can have unlimited numbers of aliases.

When you select Aliases from the Manage Addresses Overview pane, all aliases that are configured are displayed in the content pane. From Aliases you can quickly view the account information for a specific alias, move the alias from one account to another, and delete the alias.

Class of Service

Class of Service (COS) determines what default attributes a Zimbra Web Client email account has and which features are enabled 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 Collaboration Suite. You can modify the default COS to set the attributes to your email restrictions, and you can create new COS's. A COS is global and is not restricted to a particular domain or set of domains. You can assign a COS to a domain.

Each account is assigned one COS. By default, when an account is created, the account is assigned the domain COS, if the domain has a COS assigned. If the domain does not have a COS, the default COS is automatically assigned. You can assign any COS to the account. If the COS assigned to the account no longer exists, the account is automatically assigned the default COS.

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.

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

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 mailbox server when you create an account in the New Account Wizard, Mail Server field. Uncheck **auto** and enter the mailbox server in the Mail Server field.

Changing Password

If you use internal authentication, you can quickly change an account's password from the Account's toolbar. The user must be told the new password to log on.

If you want to make sure users change a password that you create, you can enable **Must Change Password** for the account. The user must change the password the next time he logs on.

Password restrictions can be set either at the COS level or at the account level. You can configure settings to require users to create strong passwords and change their passwords regularly, and you can set the parameters to lock out accounts when incorrect passwords are entered. See [Setting Password Policy](#) and [Setting Failed Login Policy](#) in the Managing End-User Mailbox Features chapter.

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.

Re indexing a Mailbox

Mail messages and attachments are automatically indexed before messages are deposited in a mailbox. Each mailbox has an index file associated with it. This index file is required to retrieve search results from the mailbox.

If a mailbox's index file becomes corrupt or is accidentally deleted, you can re-index the messages in the mailbox from the administration console. Messages and attachments in all the user's folders are re-indexed. Re-indexing a mailbox's contents can take a some time, depending on the number of messages in the mailbox. Users can still access their mailbox while re-indexing is running, but because searches cannot return results for messages that are not indexed, searches may not find all results.

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.
- **LockOut.** Users who try to log in and do not enter their correct password are locked out of their account after a specified number of consecutive failed login attempts. An account's status is automatically changed to Lockout. How long the account is locked out is set by COS or Account configuration, but you can change the lockout status at any time.

Deleting an account

You can delete accounts from the administration console. This removes the account from the server, deletes the message store, and changes the number of accounts used against your license.

Note: Before you delete an account you can run a full backup of that account to save the account information. See the *Backup and Restore* chapter.

Enforcing Mailbox and Contact Quotas

You can specify mailbox quotas and the number of contacts allowed for each account through the Zimbra administration console. You can view mailbox quotas from the administration console, Monitoring, Server Statistics. See [Setting Account Quotas](#) in the Managing End-User Mailbox Features chapter.

Moving a Mailbox

Mailboxes can be moved between Zimbra servers that share the same LDAP server. The CLI command, `zmmailboxmove` is used to move a mailbox from one server to another without taking down the servers.

The mailbox move process goes through the following steps:

- Puts the mailbox into maintenance mode. In this mode, incoming and outgoing messages are queued but not delivered or sent, and the user will be temporarily unable to access the mailbox
- Packs up the mailbox's Message Store directory and Index directory on the source server

- Marks all rows associated with the mailbox in the Data Store on the source server
- Creates the new entries and directories on the target server
- Updates the routing information for mail delivery
- Puts the mailbox back into the active mode

After the mailbox is moved to a new server, a copy still remains on the older server, but the status of old mailbox is closed. Users cannot log on and mail is not delivered. You should check to see that all the mailbox contents were moved successfully before purging the old mailbox.

To move a mailbox to a new server, type

```
zmmailboxmove -a <email@address> -ow -s <servername> -t <movetoservername>
```

To purge the mailbox from the old server, type

```
zmmailboxmove -a <email@address> -po.
```

The mailbox and its contents and references are deleted from the server.

Managing Distribution Lists

A distribution list is a group of email addresses contained in a list with a common email address. When users send to a distribution list, they are sending to everyone whose address is included in the list. The address line displays the distribution list address; the individual recipient addresses cannot be viewed. Only administrators can create, change, or delete distribution lists.

When a Zimbra user's email address is added to a distribution list, the user's account **Member Of** tab is updated with the list name. When a distribution list is deleted or the removed, the distribution list is automatically removed from the **Member Of** tab.

The **Hide in GAL** check box can be enabled to create distribution lists that do not display in the Global Address List (GAL). You can use this feature to limit the exposure of the distribution list to only those that know the address.

Using Distribution Lists for Group Sharing

Distribution lists can be created as group lists so that users can quickly share their contact lists, calendars, and Zimbra documents with everyone on the list. Everyone has the same share privileges that the user defines. When new members are added to the group distribution list, they are automatically granted the same shared privileges as other members of the group. When members are removed from the group distribution list, their share privileges are revoked.

If you create a distribution list for sharing and do not want the distribution list to receive mail, you can disable the **Can receive mail** checkbox.

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. User 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.

Searching for Addresses

You can use Search and Advanced search to locate individual accounts, aliases, distribution lists, and resources on the LDAP server. From the search bar you quickly 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.

The Advanced search feature lets you create a complex query to search for addresses by domain or server. Individual mini-search panes let you select the criteria for the search.

The results of a search display in the content pane and the total number of items found are displayed on the right side of the toolbar.

Chapter 9 Customizing Accounts and Setting General Preferences and Password Rules

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

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

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

Zimbra Messaging and Collaboration Applications

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

- Email messaging
- Calendaring
- Address Books
- Documents for Web document authoring (Beta)

The default settings for accounts can be configured either by [Class of Service](#) (COS) or by individual accounts. Configuring the COS and assigning a COS to accounts lets you configure account features and restrictions for groups of accounts. Individual accounts can be configured differently and any changes you make override the COS setting. When you update the COS, the changes are not reflected in accounts that have COS overrides.

Email messaging

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

Messaging features that can be enabled are listed below; the third column is the tab where the feature can be enabled. Many of these features can than be managed from the users' account Options tabs.

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

Allow the user to specify a forwarding address	Users can create a forwarding address for their mail. You can specify the default forwarding address that the user can use. Users can change the address from their account Options tabs. You can also specify forwarding addresses that are hidden from the user. A copy of each message sent to the account is immediately forwarded to the designated forwarding address.	Features tab in COS Forwarding tab in Accounts
Out-of-office reply	Allows users to set up an away-message and turn it on or off from their account Option tabs.	Features
New mail notification	Allows users the option to specify an address where to be notified of new mail to their ZWC account. They can turn this feature on or off and designate an address from their account Options tabs. An email with information about the email's subject, sender address and recipient address is sent to the address. Note: See “zmprov (Provisioning)” on page 117 in Appendix A CLI commands for information about how to change the email template.	Features tab in COS Preferences tab in Accounts
Mail Identities	The name and address configured for the account creates the default mail identity. When Mail Identities is enabled, users can create additional mail identities to manage different roles. Each identity includes a name and email address. Users can set up mail identities from their account Option tabs Note: To let users create email addresses for mail identities, on the Preferences tab, check Allow sending email from any address. If this is not enabled, users can only select from email addresses or aliases that you have configured.	Features and Preferences tab for additional option

Advanced search	Users can build a complex search by date, domain, status, tags, size, attachment, Zimlets, and folders.	Features
Saved searches	Users can save a search that they have previously executed or built.	Features
POP Accounts	Users can set up to retrieve their POP accounts' email messages directly from their ZWC account. They can also create a mail identity for the POP account. Users can set these up from their account Options tabs.	Features
Aliases for this account	You can create an aliases for the account. Users cannot change this.	Alias tab in Accounts
Mail filters	Users can define a set of rules and corresponding actions to apply to incoming mail. When an incoming email message matches the conditions of a filter rule, the corresponding actions associated with that rule are applied. Users set up these rules from their account Options tabs	Features
Tagging	Users can create labels and assign them to messages, contacts, and Documents pages.	Feature
Navigation Shortcuts	Users can use keyboard shortcuts within their mailbox, and they can create their own shortcut key combinations for mail folders, searches, and tags from their account Options tab.	Features
GAL access	Users can access the company directory to find names for their email messages.	Features
Auto-complete from GAL	When this is enabled, users enter a few letters in their compose header and names listed in the GAL are displayed. Users can turn this feature on or off from their account Options tabs.	Features
IMAP access	Users can use third party mail applications, such as Thunderbird or Outlook, to access their mailbox using the IMAP protocol.	Features

POP3 access	Users can use third party mail applications, such as Thunderbird or Outlook, to access their mailbox using the POP protocol. When they retrieve their POP email messages, the messages and attachments are saved on the Zimbra server	Features
-------------	---	----------

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

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

Users can modify the following mail preferences from their account Options Mail Identities tab.

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

Address Book

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

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

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

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

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

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

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

Calendar

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

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

Feature Name	Description	COS/ Account Tabs
Calendar	A calendar and scheduling tool to let users maintain their calendar, schedule meetings, delegate access to their calendar, create multiple personal calendars, and more.	Features

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

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

Documents

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

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

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

You can also create a specific domain Documents account from the administration console. This Documents notebook can be shared with users on the domain, users on all ZCS domains in your environment, as well as individuals and groups. See Managing ZCS Configurations, “Documents” on [page 59](#).

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

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

General Configuration Settings for Accounts

The general configuration options include

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

In addition, you can enable Zimbra Mobile for users to access their accounts from their mobile devices.

Setting Account 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 from the COS or the Account Preferences tab.

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

The default quota is 0, which means that accounts have unlimited storage space. Users are not notified when they reach their maximum mailbox size, but they can see their usage against their quota from the Zimbra Web Client.

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

Setting Password Policy

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

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

The password settings that can be configured are listed below.

Feature Name	Description	COS/ Account Tabs
Minimum/Maximum password length	This specifies the required length of a password. The default minimum length is 6 characters. The default maximum length is 64 characters.	Advanced
Minimum / Maximum password age	Configuring a minimum and maximum password age sets the password expiration date. Users can change their passwords at any time between the minimum and maximum set. They must change it when the maximum password age is reached.	Advanced
Configuring the next settings will require users to create more complex passwords.		
Minimum upper case characters	Upper case A - Z	Advanced
Minimum lower case characters	Lower case a - z	Advanced
Minimum punctuation symbols	Non-alphanumeric, for example !, \$, #, &, %	Advanced
Minimum numeric characters	Base 10 digits 0 - 9	Advanced
Enforce password history	Number of unique new passwords that a user must create before he can reuse an old password.	Advanced
Password locked	Users cannot change their passwords. This should be set if authentication is external.	Advanced
Must change password	When a user logs in, he is required to change his password.	General Information
Change password	When this is enabled, users can change their password at any time within the password age settings from their account Options tabs.	Features

Setting Failed Login Policy

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

Feature Name	Description	COS/ Account Tabs
Enable failed login lockout	When this box is checked, the "failed login lockout" feature is enabled and you can configure the following settings.	Advanced
Number of consecutive failed logins allowed	The number of failed login attempts before the account is locked out. The default is 10 attempts. If this is set to 0, an unlimited number of failed log in attempts is allowed. This means the account is never locked out.	Advanced
Time to lockout the account	The amount of time in seconds, minutes, hours, or days the account is locked out. If this is set to 0, the account is locked out until the correct password is entered, or the administrator manually changes the account status and creates a new password. The default is 1 hour.	Advanced
Time window in which the failed logins must occur within to lock the account	The duration of time in seconds, minutes, hours, or days after which the number of consecutive failed login attempts is cleared from the log. The default is 0, the user can continue attempts to authenticate, no matter how many consecutive failed login attempts have occurred.	Advanced

Setting Session Lifetime

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

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

Setting Attachment Viewing Options

Attachment viewing rules can be set from Global Settings, by COS, and Accounts. The global setting rule takes precedence over COS and account settings. You can select from four options.

Feature Name	Description	COS/ Account Tabs
Disable attachment viewing from web mail UI.	If checked, attachments cannot be viewed. This can also be set as a global setting.	Advanced
Attachments may be viewed in HTML only.	Attachments received in another format are opened in HTML view	Advanced
Attachments may be viewed in their original format only	Note: Users may not be able to open attachments that require a specific application that is not on their computer.	Advanced
Attachments may be viewed in HTML and their original format.	Users can select to open either in the original format or as HTML.	Advanced

Zimbra Web Client UI Themes

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

Note: To learn more about themes, go to the [Rebranding and Themes section](#) of the Zimbra Wiki.

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

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

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

Zimbra Mobile

Zimbra Mobile is an optional component that enables two-way, over-the-air synchronization of email, calendar, and contacts data between mobile devices and the Zimbra server.

Zimbra Mobile	Enables the Zimbra Mobile feature that allows Zimbra to provide mobile data access to email, calendar, and contacts for users of selected mobile phones. See Zimbra Mobile in this chapter for more details.	Features
---------------	--	----------

You enable this feature in the ZCS COS or for individual accounts. In most case, no additional plug-ins are required, users configure the device's software for Zimbra Mobile similarly to how they configure the device to sync against Microsoft® Exchange. The following may need to be configured:

- **Server address.** Type the fully qualified hostname of the user's Zimbra Collaboration Suite mailbox server.
- **User name.** Type the user's primary Zimbra account name. The domain is configured separately.

- **Domain Type** the user's Zimbra mailbox domain name.

Users can now sync their Zimbra mailbox to their mobile device. They can send email, create appointments, and add contacts.

For details about specific device setup go to the Mobile Device Setup page on the Zimbra Wiki.

Important: *Some users may experience configuration difficulty if using SSL. WM5 includes a limited number of root certificates and it may be necessary to install your server's signing CA's certificate on the device in order to use SSL.*

Configuring Zimlets for Accounts

Zimlets™ is a mechanism for integrating the Zimbra Collaboration Suite with third party information systems and content. See [Chapter 10, Working with Zimlets](#).

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

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

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

Chapter 10 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 can use the Zimlet Management Tools from either the administration console or from the command line (CLI) to deploy the Zimlet to users. You can configure Zimlets only from the command line.

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

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

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

Managing Zimlets from the Administration Console

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

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

You cannot uninstall the Zimlet from the administration console.

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

Managing Zimlets from the Command Line

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

To deploy a Zimlet to the default COS

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

```
zmzimletctl deploy <zimlet.zip file name>
```

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

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

- `zmzimletctl install`
- `zmzimletctl ldapDeploy`
- `zmzimletctl acl default grant`
- `zmzimletctl enable`

To deploy a Zimlet to a COS other than default

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

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

```
zmzimletctl deploy <zimlet.zip file name>
```

This creates the Zimlet entry in the LDAP server, installs the Zimlet files on the server, grants access to the members of the default COS, and turns on the Zimlet.

3. To add the Zimlet to other COSs and grant access, type

```
zmzimletctl acl <zimletname> <cosname1> grant
```

You can grant access to more than one COS on the same command line.

Enter as `zmzimletctl acl <zimletname> <cosname1> grant <cosname2> grant`

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

Configuring a Zimlet

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

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

How to Change Zimlet Configurations

1. To extract the configuration template type

```
zmzimletctl getConfigTemplate <zimlet.zip>
```

The `config_template.xml` is extracted from the Zimlet. zip file.

2. Make the required changes in the template. Be careful to only change the required areas. Save the file.

Note: If you have more than one custom Zimlet, you should rename the `config_template.xml` file before updating the configuration in LDAP so that files are not overwritten.

3. Type the following command to update the configuration in the LDAP. If you changed the name of the configuration template, replace `config_template.xml` with the new name.

```
zmzimletctl configure config_template.xml
```

Disabling or Removing a Zimlet

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

To turn off access from a COS

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

To disable a Zimlet on the Zimbra server

Type `zmzimletctl disable <zimletname>`

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

To uninstall and remove a Zimlet from the Zimbra server

Type `zmzimletctl undeploy <zimletname>`

The Zimlet and all associated files are uninstalled.

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

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

Zimlets Included with ZCS

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

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

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

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

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

Chapter 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 mailbox server. This server is designated as the “monitor host.” The Zimbra monitor host is responsible for checking the status of all the other Zimbra servers and presenting this information on the Zimbra administration console. The information updates every 10 minutes.

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

To enable Server Statistics.

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

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

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

Reviewing Server Status

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

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

Server Performance Statistics

The **Server Statistics** page shows bar graphs of the Message Count, Message Volume, Anti-Spam, and Anti-Virus activity. 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.
- **Disk** displays the disk usage and the disk space available for individual servers. The information is displayed for the last hour, day, month and year.

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.

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

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

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

2 messages found
```

Generating Daily Mail Reports

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

- Errors generated from the Zimbra MTA Postfix logs.
- Total number of messages that moved through the Zimbra MTA
- Message size information (totals and average bytes per message)
- Average delay in seconds for message delivery
- Total number of bounced deliveries
- Most active sender accounts and number of messages
- Most active recipient accounts and number of messages

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

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

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

```
zmlocalconfig -e zimbra_mtareport_max_recipients=<number>
```

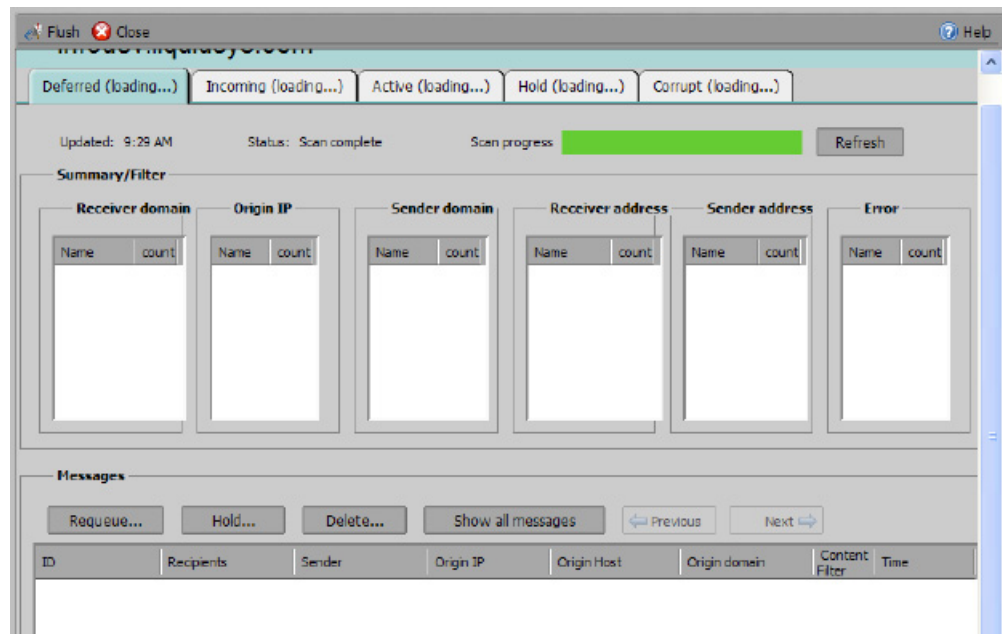
To change the number of senders to add to the report, type:

```
zmlocalconfig -e zimbra_mtareport_max_senders=<number>
```

Monitoring Mailbox Queues

If you are having problems with mail delivery, you can view the mail queues from the administration console, Monitoring Mail Queues page to see if you can fix the mail delivery problem. When you open Mail Queues, the content of the Deferred, Incoming, Active, Hold, and Corrupt queues at that point in time can be viewed. You can view the number of messages and where they are coming from and going to. For description of these queues, see “Zimbra MTA Message Queues” on page 45.

Figure 8: Mailbox Queue Page



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

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

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

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

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

Flushing the Queues

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

Monitoring Mailbox Quotas

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

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

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

Log Files

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

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

- **audit.log**. This log contains authentication activity of users and administrators, as well as mail delivery, login failure, and Tomcat start/stop activities.

- **clamd.log.** This log contains activity from the antivirus application clamd.
- **freshclam.log.** This log contains log information related to the updating of the clamd virus definitions.
- **logger_myslow.log.** This slow query log consists of all SQL statements that took more than `long_query_time` seconds to execute. Note: `long_query_time` is defined in `/opt/zimbra/my.logger.cnf`.
- **mailbox.log.** This log is a Tomcat log4j server log containing the logs from the mailbox server. This includes the mailbox store, LMTP server, IMAP and POP servers, and Index server. (Note: prior to ZCS 4.5, this log was called `/opt/zimbra/log/zimbra.log`.)
- **myslow.log.** This slow query log consists of all SQL statements from the mailbox server that took more than `long_query_time` seconds to execute. Note: `long_query_time` is defined in `/opt/zimbra/my.cnf`.
- **spamtrain.log.** This log contains output from `zmtrainsa` during regularly scheduled executions from the cron.
- **sync.log.** This log contains information about Zimbra mobile sync operations.

Other logs include:

- `/opt/zimbra/tomcat/logs/catalina.out.` This is where Tomcat-specific activity is logged.
- `/opt/zimbra/db/data.<hostname>.err.` This is the message store database error log.
- `/opt/zimbra/logger/db/data.<hostname>.err.` This is the Logger database error log.

ZCS activity logged to System syslog system

- `/var/log/zimbra.log.` The Zimbra syslog details the activities of the ZCS MTA (Postfix, amavisd, antispam, antivirus), Logger, Authentication (cyrus-sasl), and Directory (OpenLDAP),

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

Using log4j to Configure Logging

The Zimbra server uses `log4j`, a Java logging package. 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.

Chapter 12 Backup and Restore

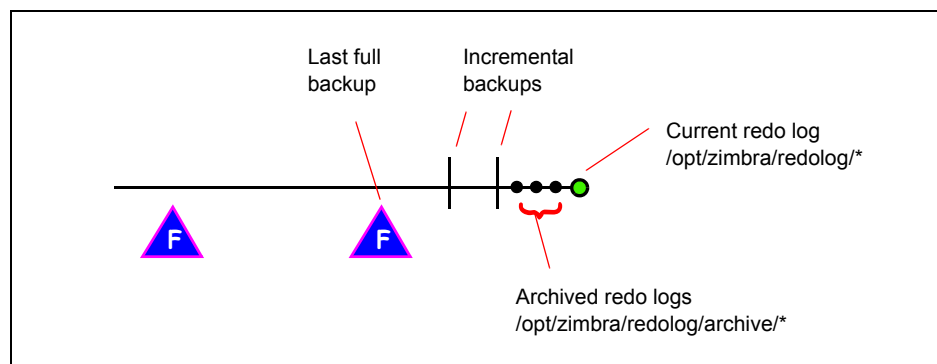
Backing up the Zimbra server on a regular basis can help you quickly restore your mail service, if an unexpected crash occurs. The backup process writes a consistent snapshot of mailboxes to a designated backup directory.

Zimbra mailboxes can be restored from the following:

- Full backup files that contains all the information needed to restore mailboxes
- Incremental backup files that contains the LDAP directory server files and all the redo log transactions written since the last backup
- Redo logs that contains current and archived transactions processed by the Zimbra server since the last incremental backup

Figure 9 shows the sequence of a full point-in-time recovery. When a system is restored, the last full backup is restored, each incremental backup since the last backup is restored, and the archived and current redo logs are restored.

Figure 9: Sample backup timeline



Backup is performed using CLI commands. This chapter describes how Zimbra data is backed up and restored, and how to use the CLI tools to backup or restore your Zimbra server. In addition, this chapter also provides information and general guidelines for disaster recovery.

Zimbra Backup and Restore

A full backup process backs up all the information needed to restore mailboxes, including the LDAP directory server, database, index directory, and message directory for each mailbox.

When backing up shared messages, the backup process looks to see whether a Binary Large Object file (BLOB) representing a message already exists in the backup. If it does, it simply flags this object as such and does not copy its content again.

An incremental backup process backs up the LDAP directory server and gathers all the redo log transactions written since the last incremental backup or the last full backup, if this is the first incremental since the last full backup. If the incremental backup process finds no previous full backup for a mailbox, a full backup is performed on that mailbox.

Incremental backups move the redo logs to the backup directory. The redo logs are a journal of every activity that has been logged. They contain a full copy of all BLOBs delivered, as well as metadata such as tags, contacts, and conversations.

These backup files can be used to restore the complete Zimbra system or individual mailboxes so that account and message data is completely restored.

The LDAP directory is backed up as part of either the full or incremental backup process. All accounts, domains, servers, COS, and other data are backed up. You can restore the LDAP directory without restoring the message server, and restore specific accounts to the LDAP server.

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.
- To recover data written since the last full backup in the event of a server failure.

If the server is restored, after the backed up files are fully restored, any redo logs in the archive and the current redo log in use are replayed to bring the system to the point before the failure.

Note:

- The Zimbra MTA is not backed up, as the data is only on the server for a very short time.
- Custom configurations, such as Tomcat's server.xml, are not backed up.

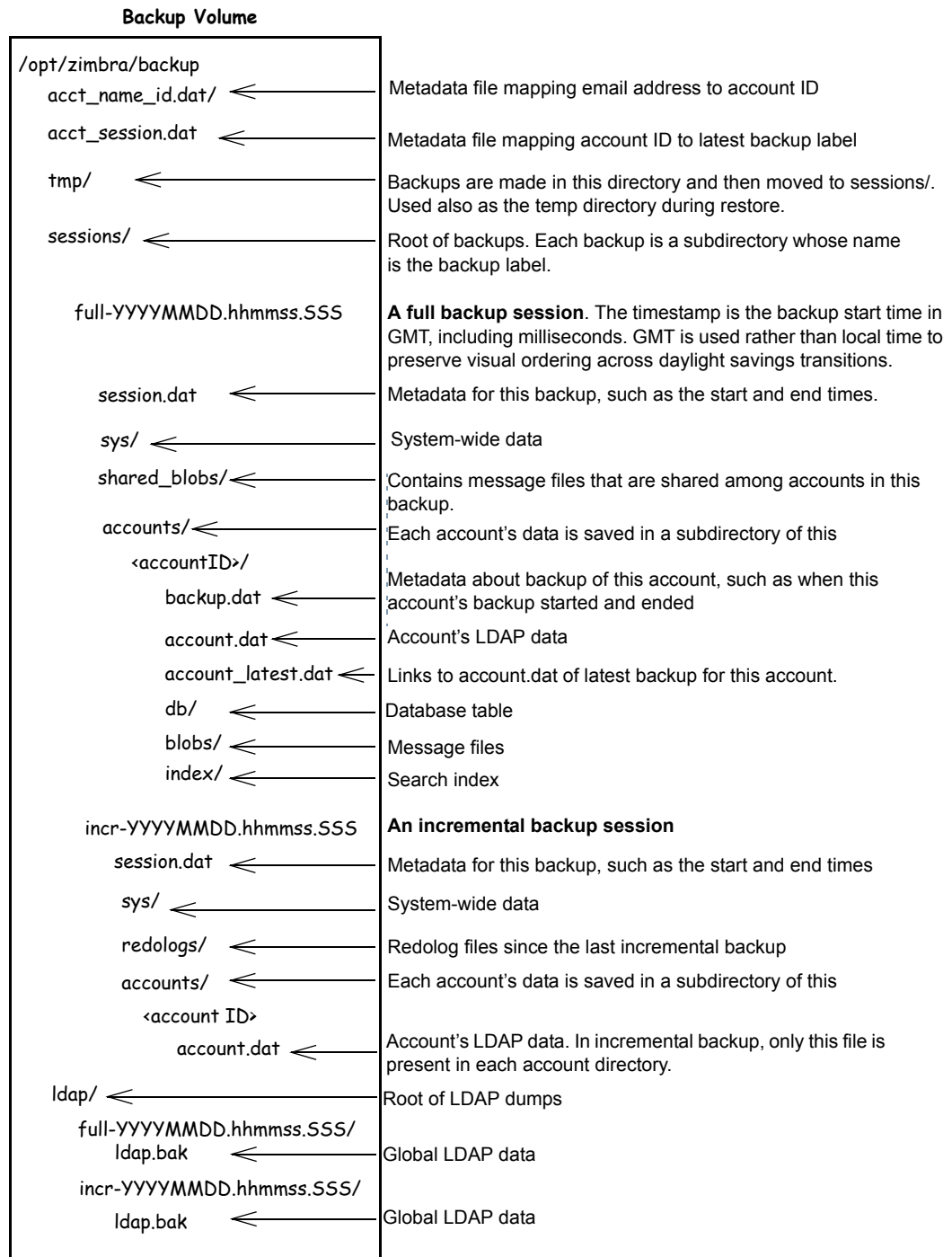
Directory Structure for Backup Files

The backup destination is known as a backup target. To the backup system, it is a path in the file system of the mail server. The Zimbra default backup directory is **/opt/zimbra/backup**.

The backup directory structure created by the backup process is shown in Figure 10. You can run regularly scheduled backups to the same target area without overwriting previous backup sessions.

Caution: Only create one backup target directory per Zimbra server. ZCS backup and restore does not support having more than one backup target.

Note: *Keeping the same backup target saves disk space, because shared binary large object files (BLOB) and other files do not have to be duplicated every time the backup process runs.*

Figure 10: Backup directory structure

The Zimbra backup process writes a consistent snapshot of mailboxes to the designated backup directory. Files are not overwritten. The default directory for the Zimbra backups is on the same mail server as is being backed up. This backup directory would be able to be used to restore one or more, or all user

accounts. A disk drive can be mounted at the path to the backup target to store backup data, which can be transferred to tapes later.

Backup and Restore from the Administration Console

Many of the backup and restore procedures can be run directly from the administration console. In the Navigation pane, **Monitoring>Backup** lists each of the servers. Select the server to perform the following backup and restore tasks.

- Immediately start a full or incremental backup
- Restore all accounts or restore specific accounts to the Zimbra server
- Abort a full backup that is in progress
- View the backup session labels, start time, end time and status
- Find a specific backup

The backup schedule is set by default during install, you can change this schedule from the command line. See [“Scheduling Backups” on page 102](#).

Backup and Restore Using the Command Line Interface

The Zimbra backup and restore procedures are run as CLI commands. The following utilities are provided to create backup schedules, perform full and incremental backups, restore the mail server, or restore the LDAP server.

- **zmschedulebackup**. This command is used to schedule full backups and incremental backups and add the backup schedule to your cron table.
- **zmbbackup**. This command executes full or incremental backup of the mail server. This is run on a live server, i.e., while the Tomcat process and the mailbox server are running. In addition to full and incremental backup of the server, the zmbbackup command can be used to backup specific accounts for archiving purposes. This command also has an option to delete old backups when they are no longer needed.
- **zmbbackupabort**. This command stops a full backup that is in process.
- **zmbbackupabort -r**. This command stops an ongoing restore.
- **zmbbackupquery**. This command lists the information about ongoing and completed backups, including labels and dates.
- **zmrestore**. This command executes a full or incremental restore to the Zimbra mail server. The zmrestore command is performed on a server that is running.
- **zmrestoreoffline**. This command restores the Zimbra mail server when the Tomcat process is stopped.
- **zmrestoreldap**. This command restores the complete LDAP directory server, including accounts, domains, servers, COS and other data.

Refer to Appendix A, CLI Commands for usage and definitions about each of these commands.

Scheduling Backups

Zimbra CLI commands, **zmschedulebackup**, is used to schedule full or incremental backups by adding the command to your cron table.

When Zimbra Collaboration Suite is installed, by default, a backup schedule is automatically added to the cron table. The default full backup is scheduled for 1:00 a.m., every Sunday. The default incremental backups are scheduled for 1:00 a.m., Monday through Saturday. This is the recommended schedule to have incremental backups run daily and a full backup run weekly. By default, backups older than a month are deleted on the first of each month at 12 a.m.

You can schedule backups for anytime or you can enter the command **zmschedulebackup -D** for the default schedule. The **zmschedulebackup** command allows you to do the following:

- Enter specific times and days for a backup
- Add a new backup time to your current schedule
- Replace a current backup schedule with another schedule
- Review your backup schedule
- Save the schedule command to a text file. This would allow you to easily recreate the same schedule after reinstall or upgrade.

Example

To set the default schedule:

```
zmschedulebackup -D
```

The following is returned.

Default schedule set

Current Schedule:

```
f    0 1 * * 0
i    0 1 * * 1-6
d 1 m 0 0 1 * *
```

Backing up the Mailbox Server

Backups are run using the Zimbra CLI command, **zmbbackup**. This command performs full backups and incremental backups for all the accounts on a designated mailbox server. By default, the backup files are saved to the server's backup directory. You can delete the backup files too.

When you initiate a backup, you can issue the command from the same server being backup up, or you can run the command remotely and specify the target server on the command line.

Full Backup Process

The full backup process goes through the following steps to backup the message store, the database, the indexes, and the LDAP directory:

1. Backs up the LDAP directory.
2. Backs up the global system data including system tables and the local config.xml file.
3. Iterates through each account to be backed up and backs up the LDAP entries for those accounts.
4. Places the account's mailbox in maintenance mode to temporarily block mail delivery and user access to that mailbox.
5. Backs up the mailbox.
 - a. Creates MySQL dump for all entries related to that mailbox.
 - b. Creates a backup of the index directory for that mailbox.
 - c. Backs up the message directory for that mailbox.
4. Returns that account's mailbox to active mode and moves on to the next one.

Full backup is usually run asynchronously. When you begin the full backup, the label of the ongoing backup process is immediately displayed. The backup continues in the background. You can use the **zmbackupquery** command to check the status of the running backup at any time.

Incremental Backup Process

Incremental backups are run using the CLI command, **zmbackup**. The process for incremental backup is as follows:

1. Backs up the LDAP directory.
2. Backs up the global system data including system tables and the local config.xml.
3. Iterates through each account to be backed up and backs up the LDAP entries for those accounts.
4. Looks in the backup target directory to find the latest full backup for the account.
5. Moves the archive redo logs, created since the last backup, to the **<backup target>/redologs** directory.

If no full backup for this account is found, the backup process performs a full backup on this account, even if only an incremental backup was specified.

Examples Backup Commands

Note:

- `-t` is not needed if the target is the default
- `-zip` can be added to the command line to zip the message blobs during backup. Zipping these can save backup storage space.
- Perform a full backup of all mailboxes on **server1** to target at **/mnt/disk**.
`zmbbackup -f -s server1.domain.com -a all -t /mnt/disk`
- Perform incremental backup of all mailboxes on **server1** since last full backup.
`zmbbackup -i -s server1.domain.com -a all -t /mnt/disk`
- Perform full backup of only **user1**'s mailbox on **server1**, to the default backup target
`zmbbackup -f -s server1.domain.com -a user1@domain.com`
- Perform incremental backup of **user1**'s mailbox on **server1**, to the default backup target.
`zmbbackup -i -s server1.domain.com -a user1@domain.com`

Delete backup sessions either by label or by date. Deleting by label deletes that session and all backup sessions before that session. Deleting by date deletes all backup session prior to the specified date.

`zmbbackup -del 7d` deletes backups older than 7 days from now. You can specify day (d), month (m), or year (y).

Finding Specific Backup Files

Each run of full or incremental backup creates a backup session, also known as the backup set.

The `zmbbackupquery` command is used to find full backup sets. The command can be used to find a specific full backup set, full backup sets since a specific date, or all backup sets in the backup directory. Each backup session is automatically labeled by date and time. For example, the label `backup200507121559510` says this is a backup from July 12, 2005 at 3:59.

Note: *If a backup session is interrupted because the server crashes during backup (not aborted), the backup session that was interrupted was saved as a temporary session file. The backup session temporary file can be found at `<backup target>/sessions_tmp`. You can use the `rm` command to delete the file.*

Aborting Full Backup In Progress

You can use the CLI command, **zmbakupabort** to stop a backup that is in progress. The backup is immediately stopped and the files are marked as a failed session.

But before you can abort a backup, you must know the backup session label. This label is displayed when **zmbakup** first starts. If you do not know the full backup label, use **zmbakupquery** to find the label name.

Example

- Stop the backup, if you know the label name
`zmbakupabort -lb backup200507121559510 -s server1`
- Stop the backup, if you do not know the label
 - a. `zmbakupquery -s server1 -l 2005/07/12`
 - b. `zmbakupabort -s server1 -lb backup200507121559510`

Restoring the Files

Three types of restore procedures can be run.

- The **zmrestore** command is used to restore the mail service while the Zimbra mailbox server is running.
- The **zmrestoreoffline** is used to restore the mail server when the mail server is down. This command is run for disaster recovery.
- The **zmrestoreldap** is used to restore the content of the LDAP directory server.

The restore process allows all accounts or individual accounts to be specified.

The speed of the full versus incremental backup is inversely proportional to the ease of restoring. Full backups take longer to run, but the restore from a full backup is much faster. Incremental backups are quicker than full backups, but restoring from incremental backups is slower, because it re-applies the transactions in the redo logs.

In addition, you can use the **zmrestore** to restore LDAP entries for an account, restore an account to a new target account, and restore system and local config files.

Restore Process

The **zmrestore** process goes through the following steps to restore the message store, the database, the indexes, and the LDAP directory.

1. Retrieves specified accounts of mailboxes to be restored, or specify **all** for all accounts that have been backed up.
2. Iterates through each mailbox:

- a. Deletes the mailbox on the server
- b. Restores the last full backup of the MySQL entries, the index directory, and the message directory for that mailbox
- c. Restores all incremental backups for that mailbox in order, since last full backup. This includes replaying the redo logs from the backup target area
- d. Replays all archived redo logs for that mailbox, from the redo log archive area on the mailbox server
- e. Replays the current redo log

Note: Before you run **zmrestore**, the accounts to be restored must be in maintenance mode. After the restore is complete, the accounts must be returned to active mode. This can be done from the administration console or from the CLI command, **zmprov ma**.

Important: After you have restored accounts, you should immediately run a full backup.

Important: Users using the ZCS Connector for Outlook must perform an initial sync on the Outlook client when they log on after the Zimbra server is restored.

Example

- Perform a full restore of all accounts on **server1**, including last full backup and any incremental backups since last full backup.

```
zmrestore -s server1.domain.com -a all
```

- Perform a single account restore on **server1**.

```
zmrestore -s server1.domain.com -a account@company.com
```

Note: A single account can be restored from the Administration Console as well.

- Restore to a specific point in time (PIT). When you perform an incremental restore, you can specify a specific point in time to restore. The following restore options affect redo log replay. If you do not specify one of these options, all redo logs since the full backup you're restoring from are replayed.

IMPORTANT: After you perform any of the following point-in-time restores, you should immediately run a complete backup for those accounts to avoid future restoration problems with those accounts.

A restore done using any of the following options is a point-in-time restore.

- **-restoreToTime <arg>** - Replay the redo logs until the time specified.
- **-restoreToIncrLabel <arg>** - Replay redo logs up to and including this incremental backup.

- `-restoreToRedoSeq <arg>` - Replay up to and including this redo log sequence
- `-br` - Replays the redo logs in backup only, which excludes archived and current redo logs of the system.
- `-rf` - Restores to the full backup only, does not include any incremental backups since that backup
- You can specify an exact time, the incremental backup label, or the redo log sequence to restore to. Restore stops at the earliest possible point in time if more than one point in time restore options are specified.

`zmrestore -s server1.domain.com -a account@company.com -restoreToTime <arg>`

- Perform an incremental restore only to last full backup, excluding incremental backups since then, for all accounts on **server1**.

`zmrestore -rf -s server1.domain.com -a all`

- Restore mailbox and LDAP data for an account

`zmrestore -ra -s server1.domain.com -a account@company.com`

- Restore to a new target account. A prefix is prepended to the original account names

`zmrestore -ca -s server1.domain.com -a account@company.com -pre restore`

The result from the above example would be an account called **restoreaccount@company.com**.

- Restore system tables in the database (db) and the local config

`zmrestore -sys -s server1.domain.com`

- Include `--continueOnError (-c)` to the command so that the restore process continues if an error is encountered. Previously deleted accounts are not restored. If previously deleted accounts still exist on the server, they are deleted.

`zmrestore -s server1.domain.com -a all -c`

When `-c` is designated, accounts that could not be restored are displayed when the restore process is complete.

- To restore a specific account. Can also be used to restore deleted accounts.

`zmrestore -s server1.domain.com -a account@company.com`

- To avoid restoring accounts that were deleted

`zmrestore -s server1.domain.com -a account@company.com -skipDeletedAccounts`

Note: The restoration of a deleted account is only possible if the account existed at the last full backup and did not exist at a subsequent incremental backup. In order to restore an account if it was deleted as of the last full backup, you will need to find the last full backup that included the account. Specify the backup label (`--lb`) to restore the account.

Stopping a Restore Process

The `zmbakupabort -r` command interrupts a restore that is in process. The restore process stops after the current account finishes being restored. The command displays a message showing which accounts were not restored before the interruption takes place.

To stop the restore type:

```
zmbakupabort -r
```

Offline Restore Process

The Zimbra offline restore process only can be run when the Tomcat server is not running. This tool is run for disaster recovery because the normal server startup sequence re-runs the latest redo log, but in a disaster recovery scenario, you would not want to do this until after performing a full restore, followed by an incremental restore. In general, offline restore is run under the following circumstances:

- Certain components of the Zimbra server are corrupted, and the server cannot be started. For example, the data in LDAP or the database are corrupted.
- A disaster requires the Zimbra software to be reinstalled on the server.

In a disaster recovery when the Zimbra software is reinstalled, if Tomcat is started before the backup files are restored, the mail server would begin to accept email messages and performing other activities, producing redo logs in the process. Since the pre-disaster data have not been restored to the server, the redo logs would be out of sequence. Once Tomcat is running, it would be too late to restore the pre-disaster data. For this reason, the offline restore must be run before the Zimbra server is started.

1. Retrieves specified accounts of mailboxes to be restored. If the command-line does not specify any mailbox address, the list of all mailboxes on the specified mail host are retrieved from Zimbra LDAP directory server.
2. Iterates through each mailbox:
 - a. Deletes the mailbox on the server
 - b. Restores the last full backup from the backup area
 - c. Restores all incremental backups for that mailbox in order, since the last full backup. This involves replaying the redo logs from the backup target area
 - d. Replays all archived redo logs for that mailbox
 - e. Replays the current redo log

You must start Tomcat after the offline restore is complete. From the command line, type `zmcontrol startup` to start Tomcat.

Example

- Restore all accounts on server1 when Tomcat is stopped

```
zmrestoreoffline -s server1 -a all
```

Restoring the LDAP Server

In a disaster recovery where you need to restore not just one server, but the entire system including all devices, you should restore your LDAP directory server first.

The `zmrestoreldap` command restores the global LDAP data including COS, distribution lists, etc. You can restore the complete LDAP server, which recreates the entire schema or you can restore specific accounts. You specify the session to restore. The restore command has to be run on the LDAP server being restored.

Examples

- To find the LDAP session labels type `-lbs`.

```
zmrestoreldap -lbs
```

- Restore the complete LDAP directory server

```
zmrestoreldap -lb full20061130135236
```

- Restore LDAP data for specific accounts

```
zmrestoreldap -lb full20061130135236 -a tac@abc.com jane@abc.com
```

Disaster Recovery for Specific Situations

This section provides general guidelines for disaster recovery.

General Steps for Disaster Recovery

The sequence of events to restore your Zimbra server in a general disaster scenario involving multiple machines would be as follows:

Preparation

1. Restore your LDAP directory server to a known good state before doing anything with the Zimbra server.
2. Put all Zimbra mailboxes into maintenance mode, to prevent mail delivery and user login while restoring the mailboxes.
3. Stop the Zimbra server, if is running.

Recovery

4. Reinstall the Zimbra software on the mailbox server, if necessary.
5. Restore mailboxes.

6. Start the Zimbra server.
7. Put all Zimbra mailboxes back in active mode.
8. Run a full backup of the server.

Crash Recovery Server Startup

When your system is unexpectedly stopped and then restarted, on startup, the server automatically searches the redo log for any uncommitted transactions, and replays any that it finds. Replaying the redo logs brings the system to a consistent state in the event that the server was stopped due to a power loss or other event.

Restore the Zimbra Collaboration Suite Servers

This would be in the case of complete computer failure.

1. Reinstall the Zimbra Collaboration Suite. See the Installation Guide.
2. Restore the LDAP server (`zmrestoreldap -lb <latest_session_label>`)
3. Run the `zmrestoreoffline` to restore all account mailbox and messages
4. Start the Zimbra server (`zmcontrol startup`)
5. Go to the Zimbra administration console to verify that the accounts are set to active. (**Accounts>General** tab)

Restoring Individual Accounts on a Live System

Use the `zmrestore` command to restore one or more selected accounts. In the event that a user's mailbox has become corrupted, you might want to restore that user from the last full and incremental backup sets.

Note: You can also restore one account at a time from Accounts on the administration console.

To restore using the CLI command

1. To put all accounts into maintenance mode, from the command line, enter `zmprov ma <account> zimbraAccountStatus maintenance`.
The maintenance mode prevents delivery of new emails during the restore. Otherwise, the emails would be overwritten during the restore process.
2. Run the `zmrestore` command to restore the accounts. Use commas between accounts.
`zmrestore -s <server> -a (account@abc.com, account@abc.com)`
3. Put all accounts into active mode, from the command line, enter `zmprov ma zimbraAccountStatus active`.

Important: *If an user account is restored and the COS that the account was assigned no longer exists, the default COS is assigned to the account.*

Restoring from Different Failure Scenarios

The restoration steps are similar for most server failures you may encounter. If a failure occurs, review the disaster recovery section to understand the process and then follow the steps below for the specific type of failure.

Zimbra LDAP server is corrupted

1. Reinstall the LDAP server. See the Zimbra Installation Guide.
2. Find the label for the LDAP session to restore. Run the `zmrestoreldap -lb <label>` command, with no arguments to restore all accounts, domains, servers, COS, etc. for the LDAP server.
3. Make sure that all accounts are in active mode. From the command line, enter `zmprov ma zimbraAccountStatus active`

Partitions become corrupted

If any partition should become corrupted, (for example, the message store partition or the index partition), run `zmrestore`, to restore the latest full and incremental backup files. The `zmrestore` process automatically retrieves the list of all mailboxes on the specified mail host from the backup date and iterates through each mailbox to restore the mailboxes to the last known good state.

Redo log is corrupted or unreadable

If the redo log becomes unreadable for any reason, the Tomcat service stops and cannot restart. If this happens, inspect the hardware and software to find the source of the problem before proceeding.

Without the latest redo log, the Zimbra mailbox server cannot be returned to the most a current state. The Zimbra mailbox data can be restored to the latest archived redo log state. A new redo log for current transactions is created after the Zimbra mailbox server is restored.

The Tomcat service must not be running and all accounts must be in maintenance mode before beginning.

1. To put all accounts into maintenance mode, from the command line, enter `zmprov ma zimbraAccountStatus maintenance`
2. With the Tomcat service not running, type `zmofflinerestore`.

The offline restore process begins by retrieving the list of all mailboxes on the specified mail host from the backup .

The offline restore then iterates through each mailbox to

- Delete the mailboxes on the server

- Restore the last full backup from the backup area
- Restore all incremental backups for that mailbox in order, since the last full backup. This involves replaying the redo logs from the backup target area
- Replay all archived redo logs

Since the redo log for current transactions is not available, the mailbox server is returned to the state of the last archived redo log.

3. Start Tomcat, after the offline restore is complete. From the command line, type **zmcontrol startup**.
4. Once the Zimbra mailbox server is up, run a full backup of the Zimbra server. The full backup must be run immediately to have the latest data backed up, as the latest redo log is not available.

Changing Local Configuration Files after Restoring Zimbra

The **localconfig.xml** file, located in the **/opt/zimbra/conf** directory, includes the core Zimbra server configuration, such as paths and passwords. This file is backed up in full and incremental backups. When you run an incremental or full restore, the backed-up version of the **localconfig.xml** is renamed **localconfig.xml.restore** and is copied to the **/opt/zimbra/conf** directory.

If you have made changes since the last backup, you may need to replace the **localconfig.xml** file with the restored copy. Compare these files, and if the **.restore** file has the latest local configuration data, delete the **localconfig.xml** file and rename the file with the **.restore** extension to **localconfig.xml**.

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*
- Back up and restore
- Start and stop a service
- Move mailboxes
- Cross mailbox searches
- 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.

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 mysqladmin 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

Table 1 Zimbra CLI Commands

CLI	Description
tomcat	Start, stop, find the status of the Tomcat server
zmaccts	Lists the accounts and gives the status of accounts on the domain
zmamavisctl	Start, stop, or find the status of the Amavis-D New
zmantispsmctl	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)
zmbackup	Performs full backups and incremental backups for a designated mail host.
zmbakupabort	Stops a backup that is in process.
zmbakupquery	Find a specific full backup set
zmcertinstall	Installs the self-signed certificate created with zmcreatecert.
zmclamctl	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
zmhsm	Start, stop and status of a HSM session.
zmjava	Execute Java with Zimbra-specific environment settings
zmldappasswd	Changes the LDAP password
zmlmtpinject	Testing tool
zmlocalconfig	Used to set or get the local configuration of a Zimbra server
zmloggerctl	Start, stop, reload, or find the status of the Zimbra logger service
zmlogswatchctl	Start, stop, status of the swatch that is monitoring logging
zmmailbox	Performs mailbox management tasks

Table 1 Zimbra CLI Commands

CLI	Description
zmmailboxctl	Start, stop, reload, or find the status of the mailbox components (Tomcat, MySQL, convert)
zmmailboxmove	Used to move selected mailboxes from one Zimbra server to another.
zmmboxsearch	Search across mailboxes to find messages and attachments
zmmsgtrace	Trace messages
zmmtaconfigctl	Start, stop, or find the status of the MTA configuration daemon
zmmtactl	Start, stop, or find the status of the MTA
zmmylogpasswd	Change logger MySQL password
zmmypasswd	Change MySQL passwords
zmmysqlstatus	Status of mailbox SQL instance
zmperditionctl	Start, stop, or find the status of the perdition IMAP proxy
zmprov	Performs all provisioning tasks in Zimbra LDAP, including creating accounts, domains, distribution lists and aliases
zmrestore	Performs full restores and incremental restores for a designated mail host
zmrestoreldap	Restore accounts from the LDAP backup
zmrestoreoffline	Performs full restore when the Zimbra server (i.e., the Tomcat process) is down
zmsaslauthdctl	Start, stop, status of saslauthd (authentication)
zmschedulebackup	Schedule backups and add the command to your cron table
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

Table 1 Zimbra CLI Commands

CLI	Description
zmvolume	Manage storage volumes on your Zimbra Mailbox server
zmzimletctl	Deploy and configure Zimlets

zmprov (Provisioning)

The **zmprov** tool performs all provisioning tasks in Zimbra LDAP, including creating accounts, aliases, domains, distribution lists, and calendar resources. Each operation is invoked through command-line options, each of which has a long name and a short name.

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

The following objects use this syntax:

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

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

```
zmprov ma user1 +zimbraZimletUserProperties testing
```

Short Name	Long Name	Syntax, Example, and Notes
-h	--help	display usage
-f	--file	use file as input stream
-s	--server	{host}[:{port}] server hostname and optional port
-l	--ldap	provision via LDAP instead of SOAP
-a	--account {name}	account name to auth as

Short Name	Long Name	Syntax, Example, and Notes
-p	--password {pass}	password for account
-P	--passfile {file}	read password from file
-Z	--zadmin	use zimbra admin name/password from localconfig for admin/password
-v	--verbose	verbose mode (dumps full exception stack trace)
-d/	--debug	debug mode (dumps SOAP messages)

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

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

Long Name	Short Name	Syntax, Example, and Notes
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
SetAccountCOS	sac	{name@domain id adminName} {cos-name cos-id} zmprov sac joe@domain.com FieldTechnician
SearchAccounts	sa	[-v] {ldap-query} [limit] [offset] [sortBy {attribute}]
RenameAccount	ra	{name@domain id} {newname@domain} zmprov ra joe@domain.com joe23@domain.com Note: After you rename an account, you should run a full backup for that account. zmbbackup -f - <servername.com> -a <newaccountname@servername.com>

Calendar Resource Provisioning Commands

CreateCalendarResource	ccr	{name@domain} [attr1 value1 [attr2 value2...]]
DeleteCalendarResource	dcr	{name@domain id}
GetAllCalendarResources	gacr	[-v] [{domain}]
GetCalendarResource	gcr	{name@domain id}
ModifyCalendarResource	mcr	{name@domain id} [attr1 value1 {attr2 value2...}]
RenameCalendarResource	rcr	{name@domain id} {newName@domain}

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

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

Long Name	Short Name	Syntax, Example, and Notes
RemoveDistributionListAlias	rdla	{list@domain id} {alias@domain}
RenameDistributionList	rdl	{list@domain id} {newName@domain}
RemoveDistributionListMember	rdlm	{list@domain id} {member@domain}
Zimbra Documents Provisioning Commands		
ImportNotebook	impn	{username} {password} {from dir}{to folder} Before importing files, any file that will become a Documents page (wiki-style page), must be renamed to include the extension ".wiki". If not it is imported as a file, accessed either as an attachment or an image. impn domainwiki@company.com test123 /tmp notebook
InitNotebook	in	{username}{password}{from dir}{to folder} in globalwiki@company.com test123 /opt/zimbra/wiki/template template
initDomainNotebook	idn	{username}{password} {domain} {directory} {folder} Creates the domain Documents account idn domainwiki@company.com test123 zimbra.com /opt/zimbra/wiki/template template
Miscellaneous Provisioning Commands		
SearchGAL	sg	{domain} {name} zmprov sg joe
AutoCompleteGal	acg	{domain} {name}
GenerateDomainPreAuthKey	gdpak	{domain id} Generates a pre-authentication key to enable a trusted third party to authenticate to allow for single-sign on. Used in conjunction with GenerateDomainPreAuth.
GenerateDomainPreAuth	gdpa	{domain id} {name} {name id foreignPrincipal} {timestamp 0} {expires 0} Generates preAuth values for comparison.
GetMailboxInfo	gmi	{account}
GetQuotaUsage	gqu	{server}

Examples

- Create one account with a password that is assigned to the default COS.
`zmprov ca name@domain.com password`
- Create one account with a password that is assigned to a specified COS. You must know the COS ID number. To find a COS ID, type `gc <COSname>`.
`zmprov ca name@domain.com password zimbraCOS
cosIDnumberstring`
- Create one account when the password is not authenticated internally.
`zmprov ca name@domain.com ''`
The empty single quote is required and indicates that there is no local password.
- Using a batch process to create accounts, see Managing the Zimbra Collaboration Suite chapter for the procedure.
- Add an alias to an account.
`zmprov aaa accountname@domain.com aliasname@domain.com`
- Create distribution list. The ID of the distribution list is returned.
`zmprov cdl listname@domain.com`
- Add a member to a distribution list. **Tip:** You can add multiple members to a list from the administration console.
`zmprov adlm listname@domain.com member@domain.com`
- Change the administrator's password. Use this command to change any password. Enter the address of the password to be changed.
`zmprov sp admin@domain.com password`
- Create a domain that authenticates against Zimbra OpenLDAP.
`zmprov cd marketing.domain.com zimbraAuthMech zimbra`
- Set the default domain.
`zmprov mcf zimbraDefaultDomain domain1.com`
- To list all COSs and their attribute values.
`zmprov gac -v`
- To list all user accounts in a domain (domain.com)
`zmprov gaa domain.com`
- To list all user accounts and their configurations
`zmprov gaa -v domain.com`
- To enable logger on a single server
`zmprov +zimbraServiceEnabled logger`
Then type `zmloggerctl start`, to start the logger.

- Modify **zimbraNewMailNotification** to customize the notification email template. A default email is sent from Postmaster notifying users that they have received mail in another mailbox. To change the template, you modify the receiving mailbox account. The variables are
 - `${SENDER_ADDRESS}`
 - `${RECIPIENT_ADDRESS}`
 - `${RECIPIENT_DOMAIN}`
 - `${NOTIFICATION_ADDRESSES}`
 - `${SUBJECT}`
 - `${NEWLINE}`

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

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

zmmailbox

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

You can invoke the `zmmailbox` command from within the `zmprov` command. You enter `selectMailbox` within `zmprov` to access the `zmmailbox` command connected to that specified mailbox. You can then enter `zmmailbox` commands until you type `exit`. `Exit` returns you to `zmprov`. This is useful when you want to create accounts and also pre-create some folders, tags, or saved searches at the same time.

Syntax

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

Description

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

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

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

<code>zmmailbox help search</code>	help on search-related commands
<code>zmmailbox help tag</code>	help on tag-related commands

Examples

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

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

zmacccts

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

Syntax

`zmacccts`

zmbackup

This tool performs full backups and incremental backups for a designated mail host. You can either specify specific accounts, or, if no accounts are specified, all accounts are included.

This utility has short option names and full names. The short option is preceded by a single dash, the full option is preceded by a double dash. For example, `-fb` is the same as `--fullBackup`.

Syntax

One of `-f`, `-i`, or `-del` must be specified.

`zmbackup {-f | -i | del} -acct (account) [options]`

Description

Long Name	Short Name	Description
<code>--fullBackup</code>	<code>-f</code>	Starts a full backup.
<code>--incrementalBackup</code>	<code>-i</code>	Starts an incremental backup.
<code>--account</code>	<code>-a</code>	Specifies the account email addresses. Separate accounts with a blank space. Enter <code>all</code> to backup all accounts. Required.
<code>--delete</code>	<code>-del</code>	<code><label date></code> Deletes the backup session on or prior to the specified label/date.
Common Options		
<code>--fullBackup</code>	<code>-f</code>	Starts full backup.
<code>--incrementalBackup</code>	<code>-i</code>	Starts incremental backup.
<code>--server</code>	<code>-s</code>	<code><arg></code> Mail server host name. For format, use either the plain host name or the <code>server.domain.com</code> name. The default is the localhost name.
<code>--sync</code>	<code>-sync</code>	Runs full backup synchronously.
<code>--target</code>	<code>-t</code>	<code><arg></code> Specifies the target backup location. The default is <code><zimbra_home>/backup</code> .
<code>--zip</code>	<code>-z</code>	Zips email blobs in backup.
<code>--help</code>	<code>-h</code>	Displays the usage options for this command.

Examples

In these examples, the server (`-s`) is `server1.domain.com`. The (`-t`) is not required if the target is the default directory, (`zimbra_home/backup`).

- Perform a full backup of all mailboxes on **server1**.

```
zmbbackup -f -a all -s server1.domain.com
```

- Perform incremental backup of all mailboxes on **server1** since last full backup.

```
zmbbackup -i -a all -s server1.domain.com
```

- Perform full backup of only **user1**'s mailbox on **server1**. Note that hostname does not need full domain if account is used.

```
zmbbackup -f -s server1 -a user1@domain.com
```

- Perform incremental backup of **user1**'s mailbox on **server1**.

```
zmbbackup -i -s server1 -a user1@domain.com
```

zmschedulebackup

This command is used to schedule backups and add the command to your cron table.

The default schedule is as follows:

- Full backup, every Sunday at 1:00 a.m. (0 1 * * 0)
- Incremental backup, Monday through Saturday at 1:00 a.m. (0 1 * * 1-6)

Each crontab entry is a single line composed of five fields separated by a blank space. Specify the fields as follows:

minute 0 through 59
hour 0 through 23
day of month 1 through 31
month 1 through 12
day of week 0 through 7 (0 or 7 is Sunday)

Type an asterisk (*) in the fields you are not using.

This command automatically writes the schedule to the crontab.

Syntax

```
zmschedulebackup [-q] [-s] [-A] [-R] [-F] [-D] [schedule] [schedule...]
```

Description

Name	Command Name	Description
	i:	Incremental backup.
	f:	full backup.
	-d <arg>	Delete backups
Common Options		
Query	-q	Default command, displays the existing Zimbra backup schedule.
Save	-s	Save the schedule. Allows you to save the schedule command to a text file so that you can quickly regenerate the backup schedule when the system is restored.

Name	Command Name	Description
Flush	-F	Removes the current schedule and cancels all scheduled backups.
Append	-A	Adds an additional specified backup to the current schedule.
Replace	-R	Replaces the current schedule with the specified schedule.
Default	-D	Replaces the current schedule with the default schedule.
Help	-h	Displays the usage options for this command.

Examples

- To schedule the default full and incremental backup
`zmschedulebackup [-D]`
- To replace the existing schedule with a new schedule
`zmschedulebackup -R f [schedule] [schedule]`
- To add an additional full backup to the existing schedule
`zmschedulebackup -A f [schedule]`
- To add an additional incremental backup to the existing schedule
`zmschedulebackup -A i [schedule]`
- To display the existing schedules a
`zmschedulebackup -q`
- To display the schedules on one line as a command, so that they can be copied to a text file and saved to be used if the application needs to be restored.
`zmschedulebackup -s`

zmbakupabort (Aborting a Full Backup)

The `zmbakupabort` command can be used to stop a backup process. Before you can abort an account you must know backup label. This label is displayed after you start the backup procedure. If you do not know the label, use the `zmbakupquery` to find the label name.

To stop the restore process. The `zmbakupabort -r` interrupts an on going restore. The restore process is stopped after the current account is restored. The command displays message showing which accounts were not restored.

Syntax

zmbakupabort -lb (label) -acct (email addresses) -s (hostname) -t (zimbra-home/backup)

Description

Long Name	Short Name	Description
--label <label>	-lb	Label of the full backup to be aborted. Use the zmbakupquery , to find the file name.
--account	-acct	Specifies the account email addresses. Separate accounts with a blank space. If accounts are omitted, all accounts are backed up.
Common Options		
--server	-s	Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name.
--target	-t	Specifies the target backup location. The default is <zimbra_home>/backup.
--help	-h	Displays the usage options for this command.

zmbakupquery

The **zmbakupquery** command is used to find full backup sets. The command can be used to find a specific full backup set, full backup sets since a specific date, or all backup sets in the backup directory.

Syntax

zmbakupquery <options>

Description

Long Name	Short Name	Description
account <arg>	-a	Account email addresses separated by white space or all for all accounts.
--label <label>	-lb	The label of the full backup session to query. An example of a label is backup200507121559510 .

Long Name	Short Name	Description
<code>--list <date></code>	<code>-l</code>	If a date is used, the query returns a list of full backup sets since the specified date. Enter date as YYYY/MM/DD hh:mm:ss . The hours, minutes, and seconds are not required.
Common Options		
<code>--server</code>	<code>-s</code>	Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name.
<code>--target</code>	<code>-t</code>	Specifies the backup target location. The default is <code><zimbra_home>/backup</code> .
<code>--help</code>	<code>-h</code>	Displays the usage options for this command.

zmrestore

This tool performs full restores and incremental restores for a designated mail host. You can either specify specific accounts, or, if no accounts are specified, all accounts in the backup are restored. In addition, you can restore to a specific point in time.

This utility has short option names and full names. The short option is preceded by a single dash, the full option is preceded by a double dash. For example, `-rb` is the same as `--restorefullBackupOnly`.

Syntax

`zmrestore {-f | -i} -a (account) <options>`

Description

Long Name	Short Name	Description
<code>--label <arg></code>	<code>-lb</code>	The label of the full backup to restore. Restores to the latest full backup if this is omitted.
<code>--restorefullBackupOnly</code>	<code>-rf</code>	Restores to the full backup only, not any incremental backups since that backup.

Long Name	Short Name	Description
--restoreAccount	-ra	Restores the account in directory service.
-restoreToIncrLabel <arg>		Replay redo logs up to and including this incremental backup
-restoreToRedoSeq <arg>		Replay up to and including this redo log sequence
-restoreToTime <arg>		Replay redo logs until this time
--prefix	-pre	<prefix> The prefix to pre-pend to the original account names.
--systemData	-sys	Restores global tables and local config.
--createAccount	-ca	Restores accounts to new target accounts whose names are pre-pended with <prefix>.
--backedupRedolog Only	-br	Replays the redo logs in backup only, which excludes archived and current redo logs of the system.
--continueOnError	-c	Continue to restore other accounts when an error occurs.
--account	-a	Specifies the account email addresses. Separate accounts with a blank space or Type all to restore all accounts.
Common Options		
--server	-s	Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name.
-skipDeletedAccounts	--skipDeletedAccounts	Do not restore if named accounts were deleted or did not exist at backup time. (This option is always enabled with "-a all")
--target	-t	Specifies the backup target location. The default is <zimbra_home>/backup.
--help	-h	Displays the usage options for this command.

Examples

- Perform complete restore of all accounts on **server1**, including last full backup and any incremental backups since last full backup.

```
zmrestore -acct all -s server1.domain.com
```

- Perform restore only to last full backup, excluding incremental backups since then, for all accounts on **server1**.

```
zmbakup -rf -acct all -s server1.domain.com
```

zmrestoreoffline (Offline Restore)

This tool is run when the Zimbra server (i.e., the Tomcat process) is down. The MySQL database for the server and the OpenLDAP directory server must be running before you start the `zmrestoreoffline` command.

Syntax

```
zmrestoreoffline <options> [<accounts>]
```

Description

Long Name	Short Name	Description
--label	-lb	The label of the full backup to restore. Type this label to specify a backup file other than the latest.
--restorefullBackupOnly	-rf	Restores to the full backup only, not any incremental backups since that backup.
--restoreAccount	-ra	Restores the account in directory service.
--prefix	-pr	<prefix> The prefix to pre-pend to the original account names.
--createAccount	-ca	Restores accounts to new target accounts whose names are pre-pended with <prefix>.
--account	-a	<arg> Specifies the account email addresses. Separate accounts with a blank space or state all for restoring all accounts. Required.
--backedupRedolog Only	-br	Replays the redo logs in backup only, which excludes archived and current redo logs of the system.
--continueOnError	-c	Continue to restore other accounts when an error occurs.
--systemData	-sys	Restores global tables and local config.
Common Options		

Long Name	Short Name	Description
<code>--server</code>	<code>-s</code>	Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name. If -s is specified, this must be localhost.
<code>--target</code>	<code>-t</code>	Specifies the backup target location. The default is <zimbra_home>/backup.
<code>--help</code>	<code>-h</code>	Displays the usage options for this command.

Examples

Before you begin `zmrestoreoffline`, the LDAP directory server must be running

- Perform a complete restore of all accounts on **server1**, including last full backup and any incremental backups since last full backup.

```
zmrestoreoffline -s server1.domain.com
```

zmrestoreldap

This tool is run to restore accounts from the ldap backup.

Syntax

```
zmrestoreldap -lb session -t target <options>
```

Description

Long Name	Short Name	Description
	<code>-lb</code>	Session label to restore from. For example, full200612291821113.
<code>--target</code>	<code>-t</code>	Specifies the backup target location. The default is /opt/zimbra/backup.
Options		
	<code>-lbs</code>	Lists all session labels in backup
	<code>-l</code>	Lists accounts in file.
	<code>-a</code>	Restores named account(s). List account names separated by white space.

zmcontrol (Start/Stop Service)

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

Syntax

zmcontrol [-v -h] **command** [args]

Description

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

zmmailboxmove (Move Mailbox)

This command is used to move a mailbox from one Zimbra server to another. Mailboxes can be moved between Zimbra servers that share the same LDAP server. All the files are copied to the new server and LDAP is updated. After the mailbox is moved to a new server, a copy still remains on the older server, but the status of old mailbox is closed. Users cannot log on and mail is not delivered. You should check to see that all the mailbox contents were moved successfully before purging the old mailbox.

Syntax

To move a mailbox to a new server, type

```
zmmailboxmove -a <email@address> -ow -s <servername> -t <movetoservername>
```

To purge the mailbox from the old server, type

```
zmmailboxmove -a <email@address> -po.
```

The mailbox and its contents and references are deleted from the server.

Description

Long Name	Short Name	Description
--account <arg>	-a	Email address of account to move.
--help	-h	Displays the usage options for this command.
--overwriteMailbox	-ow	Overwrite target mailbox, if it exists.
--purgeOld	-po	Purge old mailbox on previous server. After a mailbox has been successfully moved to a new server, perform purgeOld to remove the mailbox and its contents from the previous server.
--server <arg>	-s	Mail server hostname. The default is the localhost. Server where the --account mailbox is located.
--targetServer <arg>	-t	Server where mailbox is moved to.

-t and **-po** options are mutually exclusive. Use **-t** option to move a mailbox from the current server to the new server specified by the option. If **-ow** is specified, if a mailbox already exists for the target server, it is overwritten. After successfully moving the mailbox, use **-po** option to purge the old mailbox on the original server.

zmmailboxsearch (Cross mailbox search)

zmmailboxsearch is the CLI command used to search across mailboxes. You can search across mailboxes to find messages and attachments that match specific criteria and save copies of these messages to a directory.

Syntax

```
zmmailboxsearch -q <querystring> -m <mailboxids> -s <server> [-d directory]
```

Description

Long Name	Short Name	Description
--dir (optional)	-d	<arg> Directory to write the messages to. If none is specified, then only the headers are fetched. Files names are generated in the form RESULTNUM_ACCOUNT-ID_MAILITEMID .
--limit (optional)	-l	Sets the limit for the number of results returned. The default is 25.
--mbox	-m	<arg> Comma-separated list of mailboxes to search. UIDs or email-address or /SERVER/MAILBOXID or *.
--offset (optional)	-o	<arg> Specify where the hit list should start. The default is 0.
--query	-q	<arg> The query string for the search.
--server	-s	<arg> Mail server hostname. default is the localhost.
--verbose (optional)	-v	Request that the status message print while the search is being executed.

Example

The following example is to do a cross-mailbox search in the inbox folder of two different mailboxes on the specified server and put a copy of the message in to the specified directory.

```
zmmboxsearch -q "in:inbox" -m user1@yourdomain.com,user2@yourdomain.com -d /var/tmp
```

zmcreatecert and zmcertinstall (For a Certificate)

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

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

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

1. As root, type:

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

2. Type `su - zimbra`, then type the following all on one line
`keytool -delete -alias my_ca -keystore /opt/zimbra/java/jre/lib/security/cacerts -storepass changeit`
3. Next, type the following on one line
`keytool -delete -alias tomcat -keystore /opt/zimbra/tomcat/conf/keystore -storepass zimbra`
4. Type `zmcreateca`, press **Enter**
5. Type `zmcreatecert`, press **Enter**
6. Type `zmcertinstall mailbox`, press **Enter**
7. Type `tomcat stop`, press **Enter**
8. Type `tomcat start`, press **Enter**

zmlocalconfig (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
<code>--config <arg></code>	<code>-c</code>	File in which the configuration is stored.
<code>--default</code>	<code>-d</code>	The default values for the keys listed in [args] is listed.
<code>--edit</code>	<code>-e</code>	Edit the configuration file, change keys and values specified. The [args] is in the key=value form.
<code>--force</code>	<code>-f</code>	Edit the keys whose change is known to be potentially dangerous.
<code>--help</code>	<code>-h</code>	Shows the help for the usage options for this tool.
<code>--info</code>	<code>-i</code>	Shows the documentation for the keys listed in [args].
<code>--format <arg></code>	<code>-m</code>	Shows the values in one of these formats: plain (default), xml, shell, nokey.

Long Name	Short Name	Description
--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.
--quiet	-q	Suppress logging.
--show	-s	Forces the display of the password strings.
--unset	-u	Removes the local setting for a variable, which causes it to fallback to the default.
--expand	-x	Expand values.

zmtlsctl

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

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

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

Syntax

zmtlsctl [mode]

mode = http, https, or mixed

Steps to run

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

zmhsm

This command is to start, stop (abort), and see the status of a HSM session. The threshold for when messages are moved to a storage volume is configured from the administration console, Servers>Volume tab.

Syntax

zmhsm {abort|start|status} {server} <name>

Description

Long Name	Short Name	Description
--abort	-a	Aborts the current HSM session.If all the messages in a mailbox being processed were not moved before you clicked Abort , no messages from that mailbox are moved from the primary volume. Messages for mailboxes that have completed the move to the secondary volume are not moved back to the primary volume.
--help	-h	Shows the help for the usage options for this tool.
--server <arg>	-s	The mail server host name. The default is the localhost [args].
--start	-t	Manually starts the HSM process.
--status	-u	The status of the last HSM session is displayed.

zmlicense

This command is used to view and install your Zimbra license. The license can be viewed and installed from the administration console, Global Settings, License tab.

Long Name	Short Name	Description
--check	-c	Check to see if a valid license is installed.
--help	-h	Shows the help for the usage options for this tool.
--install <arg>	--i <arg>	Installs the specified license file.[arg] This is the Zimbra license file that you received.
--print	-p	Displays the license information.

zmmsgtrace

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

Syntax

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

Description

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

zmmylogpasswd

This command is used to change the zimbra_logger_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 43.

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 10, 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 mailbox server.

MDA

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

Metadata

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

MIME

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

MTA

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

MX Record

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

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

- abort backup, CLI 129
- aborting backup 105
- account
 - assign to mailbox server 66
 - configure default settings 71
 - deleting 67
 - restoring 105
- account authentication 31
- account distribution by COS 65
- account quota and MTA 42
- account quotas 78
- account status 66
- account, password restriction 66
- account, provision with zmprov 123
- accounts
 - batch provisioning 64
- accounts object 33
- accounts, list all 123
- accounts, number used 57
- accounts, setting up and configuring 64
- accounts, user 49
- account
 - general configuration settings 78
- active status 67
- address book quota, enforcing 67
- address book, features 75
- addresses, search for 69
- admin console, tasks 50
- admin extensions 62
- admin password, change 123
- administration console 47
- administration functions 14
- administration tasks 63
- administrator password, change 48
- alias, add with zmprov CLI 123
- anti-spam component 15
- anti-spam protection 42
- anti-spam settings 56
- anti-spam statistics 90
- anti-spam training filter 43
- anti-virus component 15
- anti-virus protection 42
- anti-virus settings 57
- anti-virus statistics 90

- anti-virus updates 42, 57
- application packages, Zimbra 15
- attachment extension, blocking 54
- attachment viewing, setting account options 81
- attachments
 - global settings 54
- authentication 31
- authentication modes 58

B

- backup 26, 101
 - aborting 105
 - incremental 103
 - interrupted 104
 - scheduling 102
- backup directory structure 99
- backup process, overview 17
- backup, CLI commands 126
- batch provisioning new accounts 64
- blocking attachments 54
- blocking by extension 54
- bounced delivery report 92

C

- calender, features 76
- change administrator password 48
- changing account status 66
- changing password 66
- Clam AntiVirus software 42
- class of service 65
 - about 34, 65
- class of service object 34
- class of service, COS 49
- CLI command to move
 - mailbox, zmmailboxmove 63
- CLI commands, provisioning 117
- CLI commands, start/stop service 135
- CLI for account management
 - zmmailbox 63
 - zmmboxsearch 63
 - zmprov 63
- CLI utilities 113
- closed status 67
- company directory 35
- components, Zimbra 15

- configuration, typical example 20
- contact 10
- core functionality 13
- COS, denying access from a zimlet 87
- COS, list all 123
- COS, password restriction 66
- creating accounts 64
- cross mailbox search, CLI 136

D

- daily mail report 92
- data store 16, 25
 - about 25
 - file location 19
- deleting accounts 67
- directory structure 18
- disaster recovery 109
 - basic steps 109
- distribution list, create with zmprov CLI 123
- disk layout 24
- distribution lists object 34
- distribution lists, group sharing 68
- distribution lists, managing 68
- documentation 10
- Documents application 59
- Documents, features 77
- domain, create with zmprov CLI 123
- domain, set default with zmprov CLI 123
- domains
 - authentication modes 58
 - virtual hosts 59
- domains object 34
- domains, global address list mode 58
- domains, managing 58
- domains, Documents account 59
- DSPAM 42

E

- edge MTA 40
- email messaging, features 71
- equipment resources 69
- error report, daily 92
- external AD account authentication 32
- external LDAP account authentication 32

F

- failed login policy, setting 80
- features, administrative 14
- features, core 13
- features, web client 14
- full backup 103

G

- GAL 35
 - LDAP search filter used 36
 - search options 36
 - search parameter settings 37
- GAL attributes 36
- GAL mode 58
- global configuration object 35
- global Documents account 59
- global settings 50
 - anti-spam 56
 - anti-virus 57
 - HSM 58
 - license 57
 - MTA 55
 - POP and IMAP 55
- group sharing, using distribution lists for 68

H

- ham mailbox 43
- high availability support 13
- horizontal scalability 13
- HSM
 - scheduling 61
- HSM, CLI 139
- HSM, global setting 58
- HTML conversion 16

I

- IMAP global settings 55
- IMAP proxy server 55
- IMAP, class of service 65
- incoming mail routing 24
- incremental backup 103
- index store 16, 25
 - file location 19
- index volume 61
- index/search
 - back-end technologies used 25
- indexing 25
- install certificate, CLI 137
- internal account authentication 32
- internal authentication mechanism 32

K

- kill percent for spam 42

L

- LDAP
 - directory traffic 30
 - hierarchy 30

- implementation 30
- overview 29
- schema include files for Zimbra 31
- Zimbra schema, overview 34

LDAP schema 31

LDAP server, restoring 109

license 9

license ID 57

license information 57

license, extended trial 9

license, number of accounts used 57

license, renew within 57

local configuration, CLI 138

location resources 69

lockout status 67

log files 27

logger 89

logging levels 95

logging on to admin console 48

Lucene 25

M

mail report 92

mail report, change 93

mailbox management tool 63

mailbox move, CLI 135

mailbox quota, enforcing 67

mailbox quotas

- setting 78
- specifying 67

mailbox quotas, monitoring 94

mailbox search 63

mailbox server

- overview 23

mailbox server, backing up 102

mailbox, move 63, 67

mailbox, reindexing 66

mailbox, view from admin console 66

main.cf file 40

management tasks 50

management tasks from CLI 51

master.cf file 40

message count 90

message search 63

message store 16, 24

- file location 20
- single-copy 24

message store, MIME format 16

message trace 90

message trace, CLI 140

message volume 61, 90

messages received and sent report 92

modes, set with `zmtoolsctl` CLI 139

monitoring quotas 94

monitoring tool 89

move mailbox 63, 135

moving a mailbox 67

MTA 16

MTA functionality 40

MTA package, Zimbra 16

MTA queues 45

MTA settings, how to configure 55

MySQL 16

N

navigation pane, description 49

O

offline restore tool 101

offline restore, CLI 133

open source components 15

P

password policy, setting 78

password restriction 66

password, admin change 123

password, changing admin 48

password, failed login policy 80

point-in-time restore 106

POP 55

POP proxy server 55

ports, proxy server 56

Postfix 39

Postfix configuration files 40

postfix error report 92

product overview 13

protocol, set with CLI 139

provisioning, CLI commands 117

proxy server 55

proxy server port mapping 56

Q

query backup, CLI 130

queues 45

quotas 78

quotas and message delivery 42

quotas, mailbox 67

quotas, monitoring 94

R

recipient object 34

recipients, most active report 92

redo log 26

reindexing a mailbox 66

reject messages 54

- relay host settings 41
- removing zimlets 87
- report, daily mail 92
- resources, managing 69
- restore 101
 - process description 105
- restore backup, CLI 131
- restore process 105
- restore, point-in-time 106
- restoring an account 105
- restoring files 105
- restoring LDAP server 109

S

- schedule backups, CLI 128
- schema, LDAP 31
- search 69
- search across mailboxes 63
- self-signed certificate, CLI 137
- senders, most active report 92
- server
 - admin extensions 62
 - managing zimlets 62
 - volume settings 61
- server mode, changing 139
- server pool by COS 65
- server settings
 - services 60
- server statistics, statistics 90
- server status 90
- server, Zimbra
 - managing 60
- service,start/stop 135
- session lifetime, setting 80
- setting up zimlets 85
- single-copy message storage 24
- single-copy store 24
- skins 82
- skype 88
- smart host 41
- SMTP authentication 41
- SMTP restrictions 41
- SNMP monitoring 96
- SNMP package, Zimbra 17
- SNMP traps, error 96
- spam configuration settings 42
- spam mailbox 43
- spam training filter 43
- spam training, CLI 142
- spam, turning on/off training attributes 43
- SpamAssassin 42
- start service 135
- statistics 50

- status 50
- stop service 135
- store package 16
- support 10
- system architecture 15
- system architecture graphic 18

T

- tasks from admin console 50
- themes 82
- themes, setting account options 82
- third-party software bundled with 15
- tracing messages 90
- transaction log 26
- trial license 9

U

- updating anti-virus software 42, 57

V

- view mailbox from admin console 66
- virtual host 59
- volume settings 61
- volumes, managing with CLI 142

W

- Web client features 14
- wiki 59

Z

- Zimbra applications 71
- Zimbra logger 89
- Zimbra mobile 82
- Zimbra monitor host 89
- Zimbra MTA 39
- Zimbra objects
 - ldap 33
- Zimbra Schema 31
- Zimlets 85
- Zimlets included with ZCS 88
- Zimlets, configure 87
- Zimlets, configuring for accounts 83
- Zimlets, disabling 87
- Zimlets, managing 62
- Zimlets, managing form the administration console 85
- Zimlets, remove 88
- Zimlets, specify COS to use 86
- zmbbackup 126, 131
- zmprov CLI 117
- zmtrainsa spam training tool 43

