



Zimbra™ Collaboration Suite Administrator's Guide

Release 6.0

**Network Edition
Rev: March 2010**

Legal Notices

Copyright 2005-2010 Zimbra. All rights reserved.

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

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 a division of VMware, Inc.

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

September 2009 - ZCS 6.0

Revised for 6.0.6

March 1, 2010

Table of Contents

Chapter 1	Introduction	11
	Intended Audience	11
	Zimbra Collaboration Suite License	11
	Available Documentation	12
	Support for Recommended Third-Party Components	12
	Support and Contact Information	12
Chapter 2	Product Overview	15
	Core Functionality	15
	Zimbra Components	17
	System Architecture	17
	Zimbra Packages	18
	Backup Process Overview	21
	Zimbra System Directory Tree	21
	Example of a Typical Multi-Server Configuration	23
Chapter 3	Zimbra Mailbox Server	27
	Zimbra Licenses	27
	Incoming Mail Routing	28
	Disk Layout	28
	Message Store	28
	Data Store	29
	Index Store	29
	Backup	30
	Redo Log	30
	Log	30
Chapter 4	Zimbra Directory Service	31
	Directory Services Overview	31
	LDAP Hierarchy	32
	Zimbra Schema	33
	Account Authentication	33
	Internal Authentication Mechanism	34
	External LDAP and External Active Directory Authentication Mechanism	34
	Custom Authentication - zimbraCustomAuth	35
	Kerberos5 Authentication Mechanism	36
	Zimbra Objects	37
	Company Directory/GAL	40
	Flushing LDAP Cache	41
	Themes and Locales	42
	Accounts, COS, Domains, and Servers	42
	Global Configuration	42
Chapter 5	Zimbra MTA	45
	Zimbra MTA Deployment	45

Postfix Configuration Files	46
MTA Functionality	46
SMTP Authentication	47
SMTP Restrictions	47
Relay Host Settings	47
MTA-LDAP Integration	47
Account Quota and the MTA	48
MTA and Amavisd-New Integration	48
Anti-Virus Protection	48
Anti-Spam Protection	48
Receiving and Sending Mail through Zimbra MTA	51
Zimbra MTA Message Queues	52
 Chapter 6 Working with Zimbra Proxy	55
Zimbra Proxy Components	55
Zimbra Proxy Architecture and Flow	55
Customizing Zimbra Proxy Configuration	56
Zimbra IMAP/POP Proxy	56
Zimbra Proxy Ports for POP/IMAP	56
Setting up IMAP/POP Proxy after HTTP Proxy	57
Configuring ZCS HTTP Proxy	59
Setting up HTTP Proxy after IMAP/POP Proxy is set up	60
Configuring Zimbra Proxy for Kerberos Authentication	62
 Chapter 7 Managing Legal Requests for Information	65
Legal Intercept for Law Enforcement	65
Legal Intercept attributes	65
Configuration	66
Create Mailbox Snapshots for Legal Discovery	67
 Chapter 8 Using the Administration Console	69
Logging In	69
Changing Administrator Passwords	70
About the Administration Console	70
Managing Tasks from the Administration Console	72
Tasks Not Available from Administration UI	73
Creating Message of the Day for Administrators	73
Checking for ZCS Software Updates	74
 Chapter 9 Delegated Administration	77
Delegated Administration Terminology	77
How Delegated Administration Rights are Granted	78
Selecting Target Types	78
Rights	80
Implementing Delegated Administration	85
Creating Administrator Groups and Administrators	85
Configure Grants on Administrator Accounts or Admin Groups	88
Granting ACLs to a Target	88
Revoking Rights	88
Viewing Rights Granted to Administrators	89
Predefined Delegated Administrator Role	89

Domain Administration Group	89
Distribution List Administration Group	91
Specific Access Rights	91
Chapter 10 Managing ZCS Configuration	99
Managing Global Configurations	99
General Global Settings	100
Global Settings to Block Mail Attachments	100
Global MTA Settings	102
Global IMAP and POP Settings	103
Anti-spam Settings	103
Anti-virus Settings	104
Zimbra Free/Busy Interoperability	104
Backup/Restore	106
Customizing Themes	106
Global HSM	106
License Information	107
Managing Domains	108
General Information	108
Global Address List (GAL) Mode	110
Authentication Modes	111
Virtual Hosts	111
Documents	112
Free/Busy Interoperability	112
Zimlets on the Domain	113
Customizing Themes for Domains	113
Setting Account Limits	113
Renaming a Domain	114
Managing Servers	115
General Server Settings	115
Services Settings	116
MTA Server Settings	116
IMAP and POP Server Settings	116
Volume Settings	116
Backup and Restore - selecting the backup mode	117
Managing Other Functions	118
Zimlets	118
Admin Extensions	118
Chapter 11 Managing User Accounts	119
Setting up and Configuring Accounts	120
Configuring One Account	120
Configuring Many Accounts at Once	121
Manage Aliases	122
Class of Service	122
Changing Passwords	123
Directing Users to Your Change Password Page	123
View an Account's Mailbox	124
Reindexing a Mailbox	124
Changing an Account's Status	124
Deleting an Account	125
Moving a Mailbox	125
Managing Distribution Lists	126

Using Distribution Lists for Group Sharing	127
Managing Resources	127
Searching for Addresses	129
Chapter 12 Customizing Accounts, Setting General Preferences and Password Rules	131
Zimbra Web Client Versions	131
Zimbra Messaging and Collaboration Applications	131
Email messaging	132
Address Book	138
Calendar	139
Tasks	141
Documents	141
Briefcase	142
Instant Messaging (Beta)	143
Other Configuration Settings for Accounts	143
Enabling Sharing	144
Disabling Preferences	145
Setting Account Quotas	145
Setting Password Policy	145
Setting Failed Login Policy	147
Setting Session Timeout Policy	148
Setting Email Retention Policy	148
Setting Attachment Viewing Options	149
Zimbra Web Client UI Themes	150
Zimbra Mobile	150
Configuring Zimlets for Accounts	151
Other Account Configuration Preferences	152
Chapter 13 Zimbra Mobile	153
Setting Up Mobile Devices	154
Setting up Mobile Device Security Policies	154
Setting Mobile Device Policies Attributes	156
Users' Mobile Device Self Care Features	156
Changing Mobile Device Password Policy	157
Chapter 14 Working with Zimlets	159
Setting Up Zimlets in ZCS	159
Managing Zimlets from the Administration Console	160
Managing Zimlets from the Command Line	160
Viewing Zimlet List	161
Configuring a Zimlet	162
Upgrading a Zimlet	162
Disabling or Removing a Zimlet	163
Zimlets enabled by default in ZCS	163
The Zimlets Gallery	164
Chapter 15 Monitoring Zimbra Servers	165
Zimbra Logger	165
Reviewing Server Status	166
Server Performance Statistics	166
Generating Daily Mail Reports	167

Monitoring Disk Space	168
Monitoring Servers	168
Monitoring Mail Queues	169
Flushing the Queues.	171
Monitoring Mailbox Quotas	171
Monitoring Authentication Failures	171
Log Files	172
Syslog	173
Using log4j to Configure Logging	173
Logging Levels	173
Reviewing mailbox.log Records	175
Reading a Message Header	179
SNMP	180
SNMP Monitoring Tools	180
SNMP Configuration	180
Errors Generating SNMP Traps	180
Checking MySQL	180
Checking for Latest ZCS Software Version	181
 Chapter 16 Backup and Restore	 183
Zimbra Backup Methods	184
Standard Backup Method	184
Auto-Grouped Backup Method	185
Directory Structure for Backup Files	185
Backup and Restore Using the Administration Console	186
Standard Backup Method	187
Auto-grouped Backup Method	187
Configure Backup from the Admin Console	187
Backup and Restore Using the Command Line Interface	188
Backing up using the Standard Method	189
Scheduling Backups	189
Full Backup Process	191
Incremental Backup Process	192
Finding Specific Backups	193
Aborting Full Backup In Progress	193
Backing up using the Auto-Grouped Method	194
Configure Auto-Grouped Backup from the CLI	194
Scheduling Backups	194
Backup Options	195
Restoring Data	196
Restore Process	196
Stopping a Restore Process	198
Offline Restore Process	198
Restoring Individual Accounts on a Live System	199
Selectively Restore Items	199
Restoring the LDAP Server	200
Disaster Recovery for Specific Situations	200
General Steps for Disaster Recovery	200
Crash Recovery Server Startup	201
Restore the Zimbra Collaboration Suite Servers	201
Preparing the New Server	202
Restoring from Different Failure Scenarios.	204
Changing Local Configuration Files after Restoring Zimbra	205

Using snapshots to backup and restore	206
Chapter 17 Zimbra Archiving and Discovery	209
How Archiving Works	209
How Discovery Works	211
Installing Archiving Package as an Update to ZCS	211
Installing zimbra-archiving in a Single-Server Environment	211
Installing zimbra-archiving in a Multi-Server Environment	212
Enable archiving on each MTA	213
Creating Dedicated Archive COS in a Multi-Server Environment	214
Using the Administration Console	214
Using CLI	214
Archiving Attribute	215
Attributes configured on users' account	215
Archive Account Name Templates	216
Creating Archive Mailboxes	216

zmcontrol (Start/Stop Service)	259
zmmailboxmove (Move Mailbox)	260
zmmailboxsearch (Cross Mailbox Search)	261
zmcertmgr	262
zmgsautil	263
zmldappasswd	264
zmlocalconfig	265
zmmailbox	266
zmlocalconfig	268
zmhsm	269
zmlicense	270
zmmetadump	271
zmmypasswd	271
zmplayredo	271
zmproxycongen	272
zmproxypurge	273
zmredodump	274
zmskindeploy	275
zmsoap	275
zmstat-chart	276
zmstat-chart-config	277
zmstatctl	277
zmthrdump	278
zmtrainsa	278
zmtzupdate	279
zmvolume	279
zmzimletctl	280
zmproxyconfig	281
 Appendix B ZCS Crontab Jobs	 285
How to read the crontab	285
ZCS Cron Jobs	286
Jobs for crontab.store	286
Jobs for crontab.logger	287
Jobs for crontab.mta	287
Single Server Crontab -I Example	288
 Appendix C The zmlocalconfig Settings	 291
 Appendix D Glossary	 295
 Index	 301

Chapter 1 Introduction

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

Intended Audience

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

Readers of this guide should 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 Mailbox Server chapter, Zimbra Mailbox Server](#).

Go to Zimbra's Website to obtain a trial license from the Network Downloads link. Contact Zimbra Sales to purchase a regular license by emailing sales@zimbra.com or calling 1 408-349-8000.

Available Documentation

The following ZCS documentation is available:

- **Installation Guides.** Installation guides for single server and multi-server installation, include system requirements and server configuration instructions.
- **Administrator Guide.** This guide provides a comprehensive product overview, including architecture, server functionality, administration tasks, configuration options, and monitoring tools.
- **ZCS 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 ZCS servers and mailbox accounts from the administration console.
- **Zimbra Web Client Help.** The Help topics describes how to use the features of the ZCS 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**](http://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 Forums](#), to participate and learn more about the Zimbra Collaboration Suite.

Let us know what you like about the product and what you would like to see in the product. 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[®], Jetty, Postfix, MySQL[®], OpenLDAP[®].
- **Uses industry standard open protocols.** SMTP, LMTP, SOAP, XML, IMAP, POP.
- **Modern technology design.** Java, JavaScript thin client, DHTML.
- **Horizontal scalability.** Because each mailbox server includes its own data store, message store, and set mailbox accounts, you don't change anything on existing servers in order to scale the system. To scale for additional mail accounts, add more servers.
- **High availability support.** For cluster integration to provide high availability, ZCS can integrate with either Red Hat[®] Enterprise Linux[®] Cluster Suite version 4, Update 5 or later or with Veritas[™] Cluster Server by Symantec (VCS) version 5.0 with maintenance pack 1 or later.
- **Browser based client interface.** Zimbra Web Client gives users easy access to all the ZCS features.
- Administration console to manage accounts and servers.

Core Functionality

The Zimbra Collaboration Suite is an innovative messaging and collaboration application that offers the following state-of-the-art messaging and collaboration solutions:

- Email
- Group Calendars
- Address Books

- Task Management
- Web document management and authoring.

The core functionality within ZCS 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.

- Manage classes of service
- Add accounts and domains
- Set account restrictions either for an individual account or by COS
- Delegate users as domain administrators
- Move mailboxes from one server to another
- Create and edit distribution lists
- Import Microsoft Exchange user accounts
- Set up virtual hosts on a domain
- Manage servers
- View and manage system status
- Define policies for moving older messages to secondary storage
- Backup and restore accounts
- Monitor usage

Zimbra offers two browser based web clients, Advanced Zimbra Web Client that offers a state-of-the-art Ajax web client; and Standard Zimbra Web Client as an HTML client. Some of the features that can be found in the web client include:

- 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 calendar, email folders, address book lists with others
- Create address books and share with others
- Set mailbox usage preferences, including defining mail filtering options
- Use ZCS Documents to create, organize and share web documents
- Use the Tasks feature to create to-do lists and manage tasks through to completion.

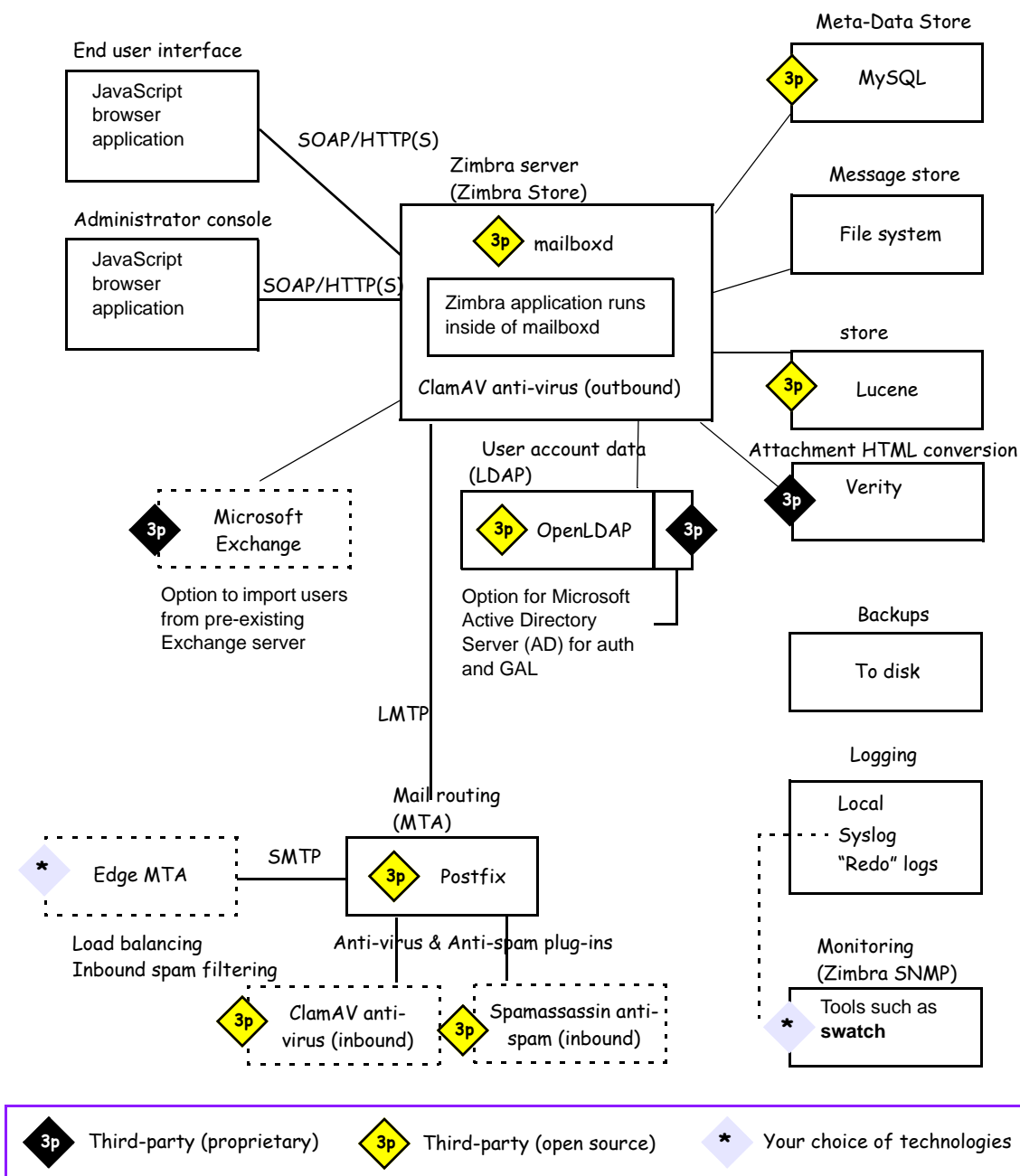
Zimbra Components

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

- Jetty, the web application server that Zimbra software runs in.
- 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 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 mail filter 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.

Figure 1: Zimbra Collaboration Suite System Architecture

Zimbra Packages

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 Convertd

Zimbra-convertd package is installed on the zimbra-store server. Only one zimbra-convertd package needs to be present in the ZCS environment.

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 Jetty, which is the servlet container the Zimbra software runs within. Within ZCS, this servlet container is called **mailboxd**.

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

The mailbox server includes the following components:

- Data store
- Message store
- Index store
- HTML attachment conversion utility

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

As each email arrives, the Zimbra server (convertd) extracts the text from the attachments to be indexed along with the mail body.

Attachments are converted to HTML when users click on the **view as HTML** link on the Zimbra Web Client.

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

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

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

Zimbra-SNMP

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

Zimbra Logger

Installing the Zimbra Logger package is optional and is installed on one mailbox server. The Zimbra logger installs tools for syslog aggregation, reporting. If you do not install Logger, 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.

Zimbra Proxy

Installing the Zimbra Proxy is optional. Use of an IMAP/POP proxy server allows mail retrieval for a domain to be split across multiple Zimbra servers on a per user basis.

Note: *The Zimbra Proxy package can be installed with the Zimbra LDAP, the Zimbra MTA, the Zimbra Mailbox server, or on its own server.*

Zimbra Memcached

Memcached is a separate package from zimbra-proxy and is automatically selected when the zimbra-proxy package is installed. One server must run zimbra-memcached when the proxy is in use. All installed zimbra-proxies can use a single memcached server.

Zimbra Archiving

The Zimbra Archiving and Discovery feature is an optional feature for Zimbra Network Edition. Archiving and Discovery offers the ability to store and search all messages that were delivered to or sent by Zimbra. This package includes the cross mailbox search function which can be used for both live and archive mailbox searches. Note: Using Archiving and Discovery can trigger additional mailbox license usage. To find out more about Zimbra Archiving and Discovery, contact Zimbra sales.

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 16, Backup and Restore](#).

Zimbra System Directory Tree

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

The directories not listed in this table are libraries used for building the core Zimbra software

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 utilities described in Appendix A, Command -Line Utilities
	clamav	Clam AV application files for virus and spam controls
	conf/	Configuration information
	contrib	Third party scripts for conveyance
	convertd	Convert service
	cyrus-sasl	SASL AUTH daemon

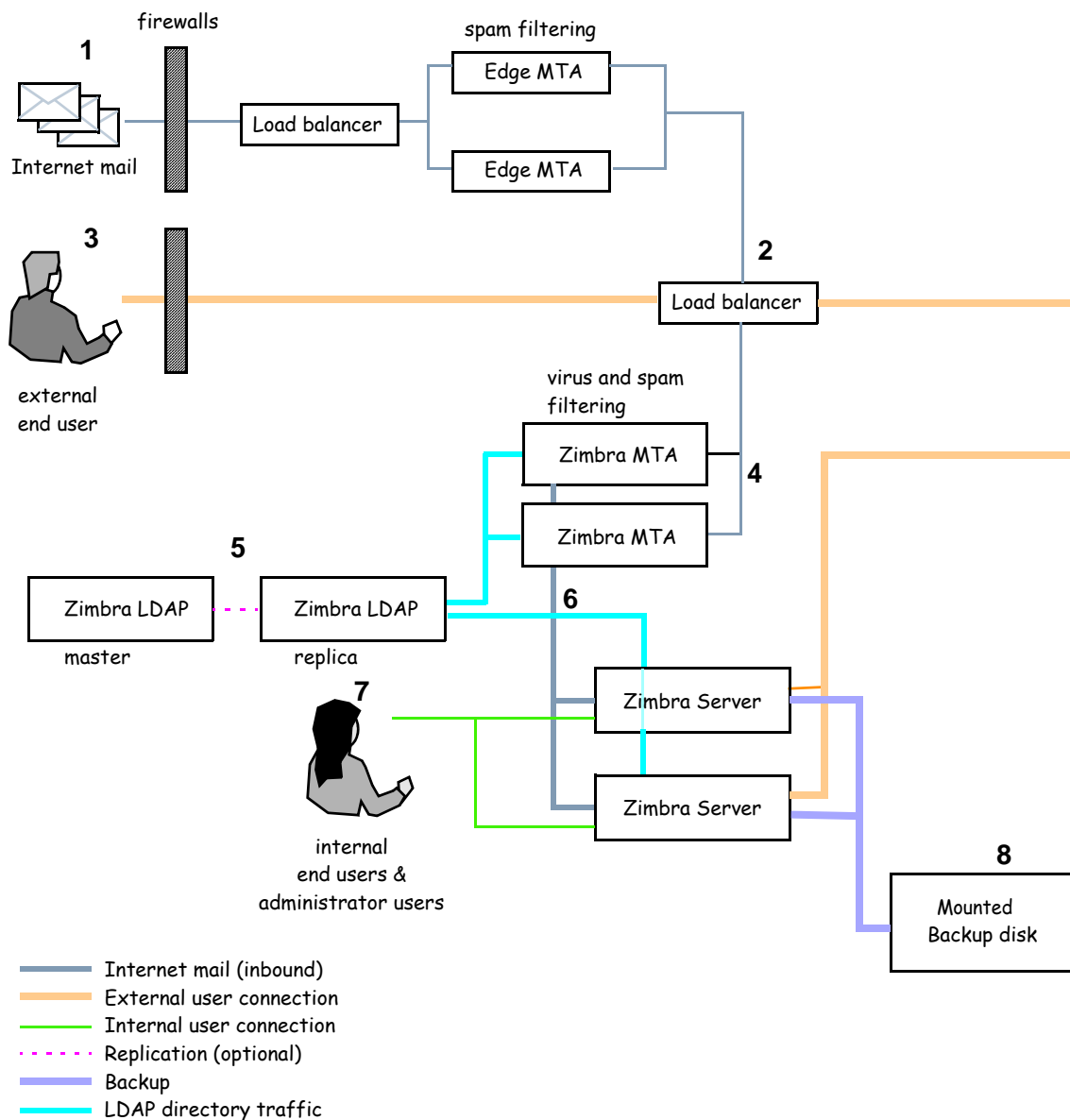
Parent	Directory	Description
	data/ldap/hdb	OpenLdap data directory
	db/	Data Store
	doc/	SOAP txt files
	dspam	DSPAM antivirus
	httpd	Spell server
	/	Store
	java/	Contains Java application files
	jetty/	mailboxd application server instance. In this directory, the webapps/Zimbra/skins directory includes the Zimbra UI theme files.
	lib/	Libraries
	libexec/	Internally used executables
	log/	Local logs for Zimbra server application
	logger/	RRD and SQLite data files for logger services
	mysql/	MySQL database files
	openldap/	OpenLDAP server installation, pre-configured to work with Zimbra
	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
	wiki	Contains the Zimbra Documents global template file

Parent	Directory	Description
	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.
	zmstat	mailboxd statistics are saved as .csv files

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 Mailbox Server

The Zimbra mailbox 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 ZCS 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 ZCS multi-server environment, the LDAP and 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 11 for a description of the license types.

The regular license can only be installed on the Zimbra 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 mailbox server.

When you purchase, renew, or change the Zimbra license, you must update the Zimbra mailbox 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 270 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. See "Global HSM" on page 106.

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 stand alone data store containing data for the mailboxes on that server.

The Data Store contains:

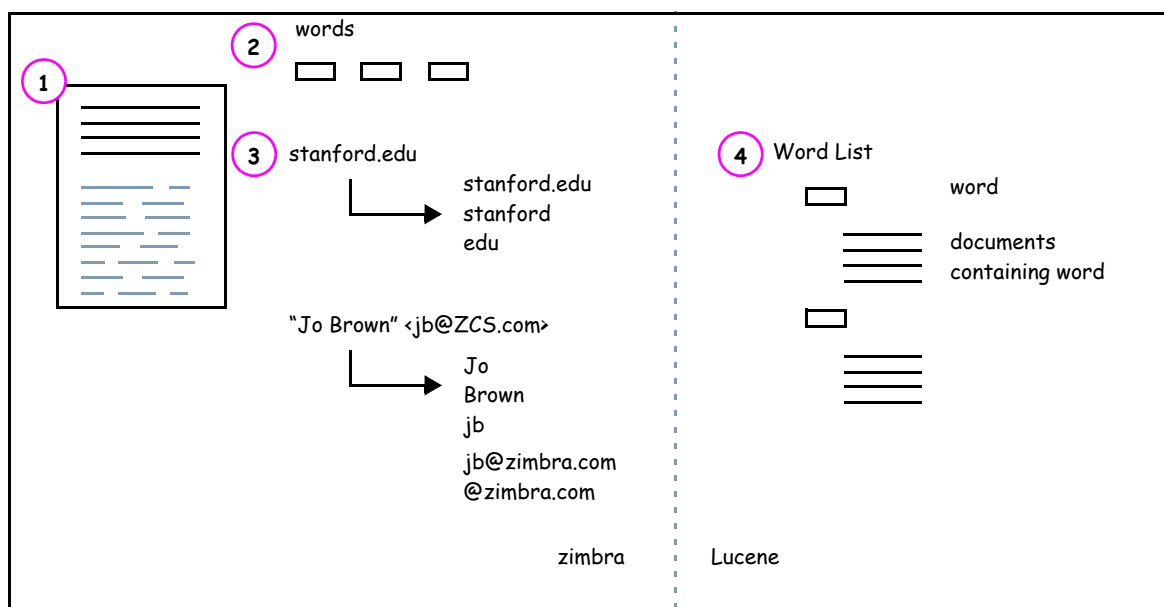
- Mailbox-account mapping. The primary identifier within the Zimbra database is the mailbox ID, rather than a user name or account name. The mailbox ID is only unique within a single mailbox server. The Data Store maps the Zimbra mailbox IDs to the users' OpenLDAP accounts.
- Each user's set of tag definitions, folders, and contacts, calendar appointments, tasks notebooks, and 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.

Figure 3: Message tokenization



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

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 16, Backup and Restore](#).

Redo Log

Each Zimbra mailbox server generates redo logs that contain current and archived transactions processed by the message store server since the last incremental backup.

When 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.

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 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 15, 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 ZCS 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.

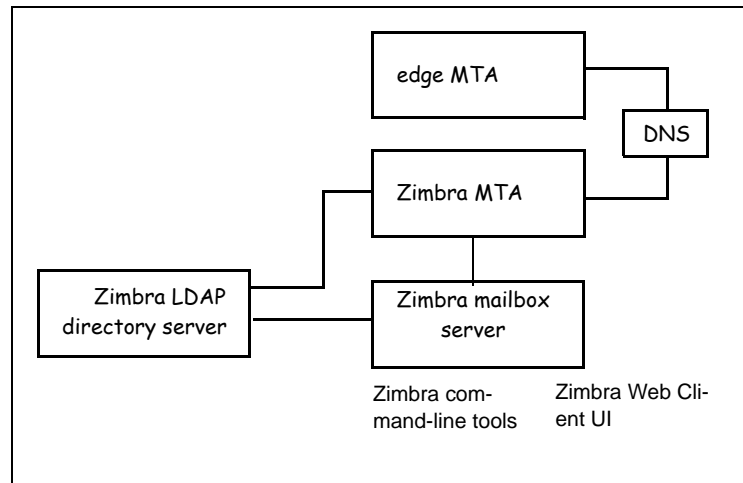
Directory Services Overview

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.

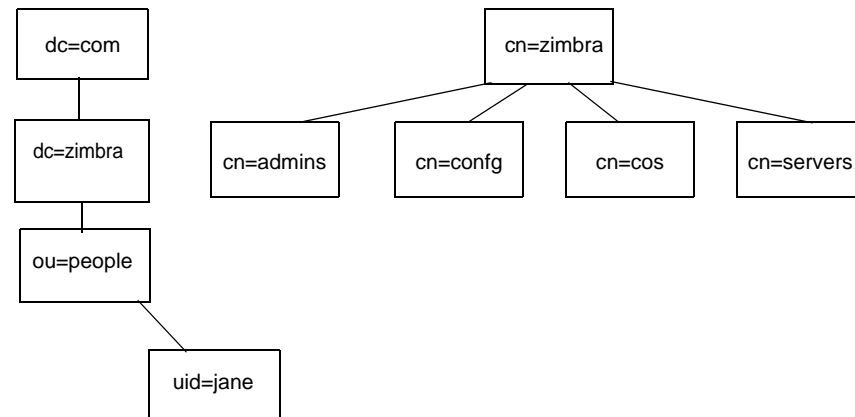
The object classes determine what type of object the entry refers to and what type of data can be stored for that entry. An entry's object class that determines what kind of entry it is, is called a structural object class and cannot be changed. Other object classes are called auxiliary and may be added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

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.

Custom Authentication - zimbraCustomAuth

You can implement a custom authentication on your domain. Custom authentication allows external authentication to your proprietary identity database. When an AuthRequest comes in, Zimbra checks the designated auth mechanism for the domain. If the auth mechanism is set to custom auth, Zimbra invokes the registered custom auth handler to authenticate the user.

To set up custom authentication, prepare the domain for the custom auth and register the custom authentication handler.

Preparing a domain for custom auth

To enable a domain for custom auth, set the domain attribute, **zimbraAuthMech** to **custom:{registered-custom-auth-handler-name}**.

For example:

```
zmprov modifydomain {domain|id} zimbraAuthMech custom:sample.
```

In the above example, “sample” is the name under which a custom auth mechanism is registered.

Registering a custom authentication handler

To register a custom authentication handler, invoke **ZimbraCustomAuth.register [handlerName, handler]** in the init method of the extension.

- Class: **com.zimbra.cs.account.ldap.zimbraCustomAuth**
- Method: **public synchronized static void register [String handlerName, zimbraCustomAuth handler]**

Note: *Definitions*

- **handlername** is the name under which this custom auth handler is registered to Zimbra's authentication infrastructure. This is the name that is set in the domain's `zimbraAuthMech` attribute. For example, if the registered name is "sample", then `zimbraAuthMech` must be set to `custom:sample`.
- **handler** is the object on which the `authenticate` method is invoked for this custom auth handler. The object has to be an instance of `zimbraCustomAuth` (or subclasses of it).

Example

```
public class SampleExtensionCustomAuth implements ZimbraExtension {
    public void init() throws ServiceException {
        /*
         * Register to Zimbra's authentication infrastructure
         *
         * custom:sample should be set for domain attribute zimbraAuthMech
         */
        ZimbraCustomAuth.register("sample", new SampleCustomAuth());
    }
    ...
}
```

How Custom Authentication Works

When an `AuthRequest` comes in, if the domain is specified to use custom auth, the authenticating framework invokes the `authenticate` method on the **ZimbraCustomAuth** instance passed as the handler parameter to **ZimbraCustomAuth.register ()**.

The account object for the principal to be authenticated and the clear-text password entered by the user are passed to the **ZimbraCustomAuth.authenticate ()** method. All attributes of the account can be retrieved from the account object.

Kerberos5 Authentication Mechanism

Kerberos5 Authentication Mechanism authenticates users against an external Kerberos server. To set up Kerberos5 auth set the domain attribute `zimbraAuthMech` to `kerberos5`. Then set the domain attribute `zimbraAuthKerberos5Realm` to the Kerberos5 realm in which users in this domain are created in the Kerberos database.

When users log in with an email password and the domain, **zimbraAuthMech** is set to **kerberos5**, the server constructs the Kerberos5 principal by **{localpart-of-**

the-email}@{value-of-zimbraAuthKerberos5Realm} and uses that to authenticate to the kerberos5 server.

Kerberos5 can be supported for individual accounts. This is done by setting the account's `zimbraForeignPrincipal` as `kerberos5`. Set the account's **`zimbraForeignPrincipal`** as **`kerberos5:{kerberos5-principal}`**. For example: `kerberos5:user1@MYREALM.COM`. If **`zimbraForeignPrincipal`** starts with "kerberos5:", the server uses `{kerberos5-principal}` as the Kerberos5 principal instead of the algorithm of grabbing the realm from the `zimbraAuthKerberos5Realm` as mentioned in the previous paragraph.

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
- Zimlet
- CalendarResource
- Identity
- Data Source
- Signature

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@example.domain`

- A unique ID that never changes and is never reused
- A set of attributes, some of which are user-modifiable (preferences) 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 11, 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**.

Domains Object

A Domains object represents an email domain such as **example.com** or **example.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 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 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.

Zimlet Object

Zimlet Object defines Zimlets that are installed and configured in Zimbra. 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**.

Identity Object

Identity object represents a persona of a user. A persona contains the user's identity such as display name and a link to the signature entry used for outgoing emails. A user can create multiple personas. Identity entries are created under the user's LDAP entry in the DIT. The object class name is **zimbralidentity**.

Data Source Object

Data source object represents an external mail source of a user. The two types of data source are POP3 and IMAP. A data source contains the POP3/IMAP server name, port, and password for the user's external email account. The data source also contains persona information, including the display name and a link to the signature entry for outgoing email messages sent on behalf of the external account. Data Source entries are created under the user's ldap entry in the DIT. The object class name is **zimbraDataSource**.

Signature Object

Signature object represents a user's signature. A user can create multiple signatures. Signature entries are created under the user's LDAP entry in the DIT. The object class name is **zimbraSignature**.

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

Table 1 Attributes Mapped to Zimbra contact

Standard LDAP Attribute	Zimbra Contact Field
initials	initials
l	workCity
street, streetaddress	workStreet
postalCode	workPostalCode
telephoneNumber	workPhone
st	workState
title	jobTitle
mail	email
objectClass	Not currently mapped

Zimbra GAL Search Parameters

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

Modifying Attributes

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

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

Administrators can also modify LDAP attributes using the command-line tools described in [“Appendix A Command-Line Utilities” on page 227](#).

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

Flushing LDAP Cache

The Zimbra LDAP server caches the following types of entries

- Themes (skins)
- Locales
- Account
- COS
- Domains

- Global configuration
- Server
- Zimlet configuration

Themes and Locales

When you add or change skin (themes) properties files and local resource files for ZCS on a server, you flush the cache to reload the new content. Until you do this, the new skins and locales are not available in the COS or Account.

- To flush skins, type **zmprov flushCache skin**
- To flush locales, type: **zmprov flushCache locale**

Note: *Flushing the skin/locale cache only makes the server aware of the resource changes. It does not automatically modify any COS or account's LDAP **zimbraAvailableSkin** and **zimbraAvailableLocal** settings. The LDAP attributes must be modified separately either from the administration console or with the **zmprov ma** command.*

Accounts, COS, Domains, and Servers

When you modify Account, COS, Domain, and Server attributes, the change is effective immediately on the server to which the modification is done. On the other servers, the LDAP entries are automatically updated after a period of time if the attributes are cached. Use **zmprov flushCache** to make the changes available immediately on a server.

Note: *The default ZCS setting for updating the server is 15 minutes.*

- To flush accounts, COS, domain, and server caches, type **zmprov flushCache [account|cos|domain|server] [name|id]**

If you do not specify a name or ID along with the type, all entries in cache for that type are flushed and the cache is reloaded.

Note: *Some server attributes are not effective until after a server restart, even after the cache is flushed. For example, settings like bind port or number of processing threads.*

Global Configuration

When you modify global config attributes, the changes are effective immediately on the server to which the modification is done. On other mailbox servers, you must flush the cache to make the changes available or restart the server. LDAP entries for global config attributes do not expire.

Note: *Some global config attributes are computed into internal representations only once per server restart. For efficiency reasons, changes to those attributes are not effective until after a server restart, even after the cache is flushed. Also, some global configuration settings and server settings*

that are inherited from global config are only read once at server startup, for example port or number of processing threads. Modifying these types of attributes requires a server restart.

To make a global config change effective on all servers do the following:

1. Modify the setting using **zmprov mcf**. For example, type **zmprov mcf zimbralmapClearTextLoginEnabled**.

Note: *The change is only effective on the server*

zimbra_zmprov_default_soap_server, port zimbra_admin-service_port.

2. Flush the global config cache on all other servers, **zmprov flushCache** must be issued on all servers, one at a time. For example:

zmprov -s server-1 flushCache config

zmprov -s server-2 flushcache config

zmprov -s server-3 flushcache config

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, a mail filter that attempts 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).

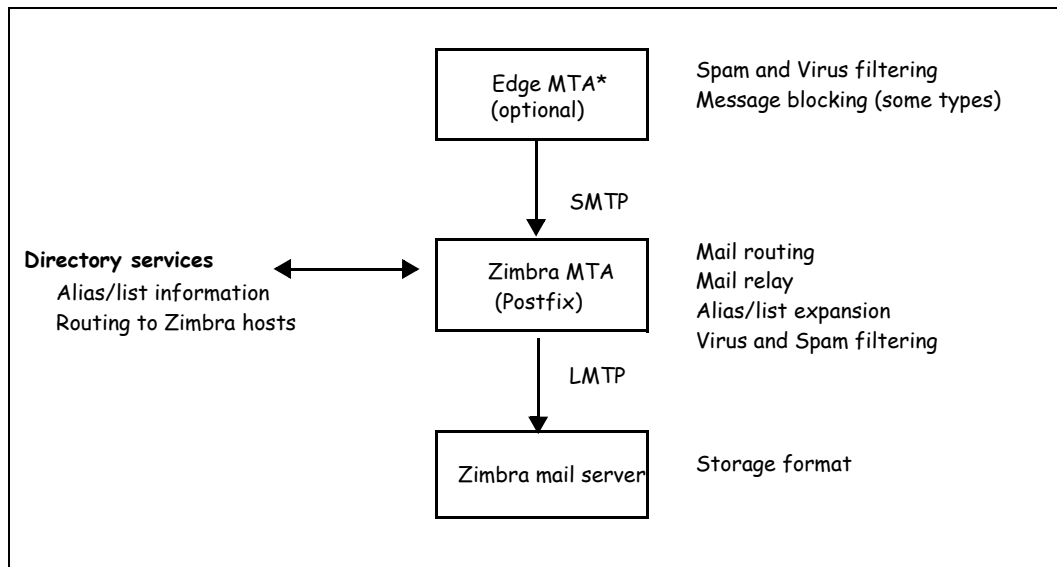
MTA configuration is stored in LDAP and a configuration script automatically polls the LDAP directory every two minutes for modifications, and updates the Postfix configuration files with the changes.

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, address books, calendars, tasks, Documents notebook pages and Briefcase files 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 temporarily sends the message to the deferred queue to be delivered when the mailbox has space. The MTA server's bounce queue lifetime is set for five days. The deferred queue tries to deliver a message until this bounce queue lifetime is reached before bouncing the message back to the sender. You can change the default through the CLI `zmlocalconfig`, `bounce_queue_lifetime` parameter.

Note: To permanently have messages bounced back to the sender, instead of being sent to the deferred queue first, set the server global config attribute `zimbraLmtpPermanentFailureWhenOverQuota` to `TRUE`.

You can view individual 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 for each server during installation. 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

Zimbra utilizes SpamAssassin to control spam. SpamAssassin uses predefined rules as well as a Bayes database to score messages with a numerical range. Zimbra uses a percentage value to determine "spaminess" based on a SpamAssassin score of 20 as 100%. Any message tagged between 33%-75% is considered spam and delivered to the user's Junk folder. Messages tagged above 75% are always considered spam and discarded.

Note: The DSPAM spam filter is also included with ZCS but the default is to not enable DSPAM. You can enable DSPAM by setting the `localconfig` attribute `amavis_dspam_enabled` to `TRUE` on the MTA servers.

```
zmlocalconfig -e amavis_dspam_enabled=true
```

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 (referred to as 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 (ham). The SpamAssassin filter can learn what is spam and what is not spam from messages that users specifically mark as Junk or Not Junk by sending them to their Junk (Spam) folder in the web client or via Outlook for ZCO and IMAP. A copy of these marked messages is sent to the appropriate spam training mailbox. The ZCS spam training tool, `zmtrainsa`, is configured to automatically retrieve these messages and train the spam filter.

In order to correctly train the spam/ham filters, when ZCS is installed, spam/ham cleanup is configured on only the first MTA. The `zmtrainsa` script is enabled through a crontab 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.

Note: New installs of ZCS limit spam/ham training to the first MTA installed. If you uninstall or move this MTA, you will need to enable spam/ham training on another MTA, as one host should have this enabled to run `zmtrainsa --cleanup`. To do this, set `zmlocalconfig -e zmtrainsa_cleanup_host=TRUE`.

The ZCS default is that all users can give feedback in this way. If you do not want users to train the spam filter, you can modify the global configuration attributes, `ZimbraSpamIsSpamAccount` and `ZimbraSpamIsNotSpamAccount`, and remove the account addresses from the attributes. To remove, type as:

```
zmprov mcf <attribute> ""
```

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

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

The **zmtrainsa** command can be run manually to forward any folder from any mailbox to the spam training mailboxes. If you do not enter a folder name when you manually run **zmtrainsa** for an account, for spam, the default folder is Junk. For ham, the default folder is Inbox.

Protecting Alias Domains From Backscatter Spam

A milter that runs a Postfix SMTP Access Policy Daemon that validates **RCPT To:** content specifically for alias domains can be enabled to reduce the risk of backscatter spam.

Note: See the Zimbra wiki article about creating Domain Alias, Managing Domains at <http://wiki.zimbra.com/index.php?title=ManagingDomains>. To learn about the Postfix Policy Daemon, go to http://www.postfix.org/SMTPD_POLICY_README.html.

This functionality is enabled using the CLI, **zmlocalconfig**.

1. To set the Postfix LC key, type

```
zmlocalconfig -e postfix_enable_smtpd_policyd=yes
```

2. Stop postfix, type **postfix stop**

3. Type

```
zmprov mcf +zimbraMtaRestriction "check_policy_service unix:private/policy"
```

4. Restart, type **postfix start**

The policy daemon runs after you set the bits in steps 1 and 3 above and then restart Postfix. The **postfix_policy_time_limit** key is because the Postfix spawn (8) daemon by default kills its child process after 1000 seconds. This is too short for a policy daemon that may run as long as an SMTP client is connected to an SMTP process.

Disable Postfix Policy Daemon

To disable the Postfix Policy Daemon, type the following:

1. **zmlocalconfig -e postfix_enable_smtpd_policyd=no**

2. **zmprov mcf -zimbraMtaRestriction "check_policy_service unix:private/policy"**

3. Stop postfix, type **postfix stop**

- Restart, type `postfix start`

Turning On or Off RBLs

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

The three RBLs that are enabled during installation are the following:

- `reject_invalid_hostname`
- `reject_non_fqdn_hostname`
- `reject_non_fqdn_sender`

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

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

To turn RBL on:

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

```
zmprov mcf zimbraMtaRestriction [RBL type]
```

To add all the possible restrictions, the command would be

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

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

Receiving and Sending Mail through Zimbra MTA

The Zimbra MTA delivers both the incoming and the outgoing mail messages. For outgoing mail, the zimbra MTA determines the destination of the recipient address. If the destination host is local, the message is passed to the zimbra

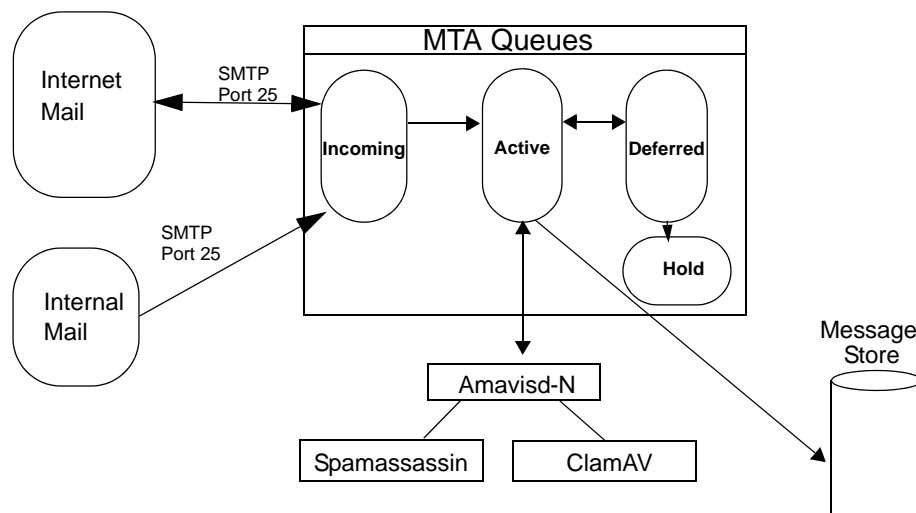
server for delivery. If the destination host is a remote mail server, the Zimbra MTA must establish a communication method to transfer the message to the remote host. For incoming messages, the MTA must be able to accept connection requests from remote mail servers and receive messages for the local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

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

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

Zimbra MTA Message Queues

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



Incoming. The incoming message queue holds the new mail that has been received. Each message is identified with a unique file name. Messages in the incoming queue are moved to the active queue when there is room in the active queue. If there are no problems, message move through this queue very quickly.

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

Deferred. Messages 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. The default for the bounce queue lifetime is 5 days. You can change the default MTA value for **bounce_queue_lifetime** from the **zmlocalconfig** CLI.

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 Mail Queues” on page 169.

Chapter 6 Working with Zimbra Proxy

Zimbra Proxy is a high performance proxy server that can be configured as a POP and IMAP proxy server and for reverse proxy HTTP requests.

The Zimbra proxy package is installed and configured during the ZCS installation. This package can be installed on mailbox servers, MTA servers or on their own independent servers. When the zimbra-proxy package is installed, the proxy feature is enabled. In most cases, no modification is necessary.

Note: *Zimbra Mobile Connector for BlackBerry Enterprise Server does not support Zimbra Proxy.*

Zimbra Proxy Components

Zimbra Proxy is designed to provide a proxy that is quick, reliable, and scalable. Zimbra Proxy includes the following:

- **Nginx.** A high performance IMAP/POP3 proxy server which handles all incoming POP/IMAP requests.
- **Memcached.** A high performance, distributed memory object caching system. Route information is cached for further use in order to increase performance.
- **Zimbra Proxy Route Lookup Handler.** This is a servlet located on the ZCS mailbox server. This servlet handles queries for the user account route information (the server and port number where the user account resides).

Zimbra Proxy Architecture and Flow

The following sequence shows the architecture and flow of Zimbra Proxy.

1. End clients connect to Zimbra Proxy using POP/IMAP ports or HTTP requests to a backend server.
2. When Zimbra Proxy receives an incoming connection, the Nginx component sends an HTTP request to the Zimbra Proxy Route Lookup Handler component.

3. Zimbra Proxy Route Lookup Handler locates the route information for the account being accessed and returns this information to Nginx.
4. The Memcached component stores the route information for the configured period of time. By default, this time is one hour. Nginx will use this route information until the default period of time has expired, instead of querying the Zimbra Proxy Route Lookup Handler .
5. Nginx uses the route information to connect to Zimbra Mailbox.
6. Zimbra Proxy connects to Zimbra Mailbox and initiates the mail proxy session. The end client behaves as if it is connecting directly to Zimbra Mailbox.

Customizing Zimbra Proxy Configuration

When Zimbra proxy is configured, the Zimbra proxy config performs keyword substitution as necessary with values from the ZCS LDAP configuration and localconfig.

If changes are required after the Zimbra Proxy is set up, you modify the Zimbra LDAP attributes or localconfig values, and run **zmmtaconfig** to generate the updated Zimbra Proxy configuration. The Zimbra proxy configuration file is in **/opt/zimbra/conf/nginx.conf**. The nginx.conf includes the main config, memcache config, mail config, and web config files.

Common changes to Zimbra Proxy configuration are:

- IMAP/POP configuration changes from the original default setup
- HTTP reverse proxy configuration changes from the original default setup
- GSSAPI authentication for Kerberos. In this case you manually identify the location of the Kerberos Keytab file, including Zimbra Proxy password

Zimbra IMAP/POP Proxy

Zimbra IMAP/POP Proxy allows end users to access their Zimbra Collaboration Suite (ZCS) account using end clients such as Microsoft Outlook, Mozilla Thunderbird, or other POP/IMAP end client software. End users can connect using POP3, IMAP, POP3S (Secure POP3), or IMAPS (Secure IMAP).

For example, proxying allows users to enter `imap.example.com` as their IMAP server. The proxy running on `imap.example.com` inspects their IMAP traffic, does a lookup to determine which backend mailbox server a user's mailbox lives on and transparently proxies the connection from user's IMAP client to the correct mailbox server.

Zimbra Proxy Ports for POP/IMAP

The following ports are used either by Zimbra Proxy or by Zimbra Mailbox. If you have any other services running on these ports, turn them off.

End clients connect directly to Zimbra Proxy, using the Zimbra Proxy Ports. Zimbra Proxy connects to the Route Lookup Handler or Zimbra Mailbox using the Zimbra Mailbox Ports.

Zimbra Proxy Ports	Port
POP3	110
POP3S (Secure POP3)	995
IMAP	143
IMAPS (Secure IMAP)	993
Zimbra Mailbox Ports	Port
Route Lookup Handler	7072
POP3 Proxy	7110
POP3S Proxy	7995
IMAP Proxy	7143
IMAPS Proxy	7993

Setting up IMAP/POP Proxy after HTTP Proxy

Zimbra Proxy is installed with ZCS and is set up during Installation from the ZCS configuration menus. Zimbra proxy must be installed on the identified proxy nodes in order to set up HTTP proxy. No other configuration is usually required.

To set up IMAP/POP proxy after you have already installed Zimbra http proxy, set up the Zimbra mailbox server and the proxy node as described in the following two sections.

Note: You can run the command as **zmpoxyconfig -r**, to run against a remote host. Note that this requires the server to be properly configured in the LDAP master.

Setting Up IMAP/POP Proxy With Separate Proxy Node

When your configuration includes a separate proxy server follow these steps.

Setup Zimbra Mailbox Servers

1. On each Zimbra mailbox server that you want to proxy with, enable the proxy for IMAP/POP proxy. Type

```
/opt/zimbra/libexec/zmpoxyconfig -e -m -H mailbox.node.service.hostname
```

This configures the following:

- **zimbralmapBindPort** to 7143
- **zimbralmapProxyBindPort** to 143
- **zimbralmapSSLBindPort** to 7993

- **zimbralmmapSSLProxyBindPort** to 993
- **zimbraPop3BindPort** to 7110
- **zimbraPop3ProxyBindPort** to 110
- **zimbraPop3SSLBindPort** to 7995
- **zimbraPop3SSLProxyBindPort** to 995
- **zimbralmmapCleartextLoginEnabled** to TRUE
- **zimbraReverseProxyLookupTarget** to TRUE
- **zimbraPop3CleartextLoginEnabled** to TRUE

2. Restart services on the proxy and mailbox servers, run
 - a. **zmcontrol stop**
 - b. **zmcontrol start**

Setup Proxy Node

1. On each proxy node that has the proxy service installed, enable the proxy for the web. Type

```
/opt/zimbra/libexec/zmproxyconfig -e -m -H proxy.node.service.hostname
```

This configures the following:

- **zimbralmmapBindPort** to 7143
- **zimbralmmapProxyBindPort** to 143
- **zimbralmmapSSLBindPort** to 7993
- **zimbralmmapSSLProxyBindPort** to 993
- **zimbraPop3BindPort** to 7110
- **zimbraPop3ProxyBindPort** to 110
- **zimbraPop3SSLBindPort** to 7995
- **zimbraPop3SSLProxyBindPort** to 995
- **zimbraReverseProxyMailEnabled** to TRUE

Setting Up a Single Node

When Zimbra proxy is installed along with ZCS on the same server, follow this step.

1. Enable the proxy for the web. Type

```
/opt/zimbra/libexec/zmproxyconfig -e -m -H mailbox.node.service.hostname
```

This configures the following:

- **zimbralmmapBindPort** to 7143
- **zimbralmmapProxyBindPort** to 143
- **zimbralmmapSSLBindPort** to 7993

- **zimbralmapSSLProxyBindPort** to 993
 - **zimbraPop3BindPort** to 7110
 - **zimbraPop3ProxyBindPort** to 110
 - **zimbraPop3SSLBindPort** to 7995
 - **zimbraPop3SSLProxyBindPort** to 995
 - **zimbralmapCleartextLoginEnabled** to TRUE
 - **zimbraReverseProxyLookupTarget** to TRUE
 - **zimbraPop3CleartextLoginEnabled** to TRUE
 - **zimbraReverseProxyMailEnabled** to TRUE
2. Restart services on the proxy and mailbox servers, run
 - a. **zmcontrol stop**
 - b. **zmcontrol start**

Configuring ZCS HTTP Proxy

In addition to IMAP/POP3 proxying, the Zimbra proxy package based on nginx is also able to reverse proxy HTTP requests to the right backend server.

Using an nginx-based reverse proxy for HTTP helps to hide names of backend mailbox servers from end users.

For example, users can always use their web browser to visit the proxy server at <http://mail.example.com>. The connection from users whose mailboxes live on `mbs1.example.com` is proxied to `mbs1.example.com` by the proxy running on the `mail.example.com` server. In addition to the ZCS web interface, clients such as REST and CalDAV clients, Zimbra Connector for Outlook, and Zimbra Mobile Sync devices are also supported by the proxy.

HTTP reverse proxy routes requests as follows:

- If the request has an auth token cookie (**ZM_AUTH_TOKEN**), the request is routed to the backend mailbox server of the authenticated user.
- If the requesting URL can be examined to determine the user name, then the request is routed to the backend mailbox server of the user in the URL. REST, CalDAV, and Zimbra Mobile Sync are supported through this mechanism.
- If the above methods do not work, the IP hash method is used to load balance the requests across the backend mailbox servers which are able to handle the request or do any necessary internal proxying.

Setting up HTTP Proxy after IMAP/POP Proxy is set up

Zimbra Proxy is installed with ZCS and is set up during Installation from the ZCS configuration menus. Zimbra proxy must be installed on the identified proxy nodes in order to set up HTTP proxy. No other configuration is usually required.

To set up http (s) proxy after you have already installed zimbra proxy for IMAP/POP, set up the Zimbra mailbox server and the proxy node as described in the following two sections.

Note: You can run the command as **zmproxyconfig -r**, to run against a remote host. Note that this requires the server to be properly configured in the LDAP master.

Setting Up HTTP Proxy With Separate Proxy Node

When your configuration includes a separate proxy server follow these steps.

Setup Zimbra Mailbox Servers

1. On each zimbra mailbox server that you want to proxy with, enable the proxy for the web. Type

```
/opt/zimbra/libexec/zmproxyconfig -e -w -H mailbox.node.service.hostname
```

This configures the following:

- **zimbraMailReferMode** to reverse-proxied. See Note below.
- **zimbraMailPort** to 8080, to avoid port conflicts.
- **zimbraMailSSLPort** to 8443, to avoid port conflicts.
- **zimbraReverseProxyLookupTarget** to TRUE
- **zimbraMailMode** to http. This is the only supported mode.

2. Restart services on the proxy and mailbox servers, run

a. **zmcontrol stop**

b. **zmcontrol start**

3. Configure each domain with the public service host name to be used for REST URLs, commonly used in sharing Document Notebooks, email and Briefcase folders. Run

```
zmprov modifyDomain <domain.com> zimbraPublicServiceHostname  
<hostname.domain.com>
```

Setup Proxy Node

1. On each proxy node that has the proxy service installed, enable the proxy for the web. Type

```
/opt/zimbra/libexec/zmproxyconfig -e -w -H proxy.node.service.hostname
```

This configures the following:

- **zimbraMailReferMode** to reverse-proxied. See Note below.
- **zimbraMailProxyPort** to 80, to avoid port conflicts.
- **zimbraMailSSLProxyPort** to 443, to avoid port conflicts.
- **zimbraReverseProxyHttpEnabled** to TRUE to indicate that Web proxy is enabled.
- **zimbraReverseProxyMailMode** defaults to both.

If you want to set the proxy server mail mode, add to the command the **-x** option with the mode you desire: **http**, **https**, **both**, **redirect**, **mixed**.

Setting Up a Single Node for HTTP Proxy

When Zimbra proxy is installed along with ZCS on the same server, follow this step.

1. On each zimbra mailbox server that you want to proxy with, enable the proxy for the web. Type

```
/opt/zimbra/libexec/zmproxyconfig -e -w -H mailbox.node.service.hostname
```

This configures the following:

- **zimbraMailReferMode** to reverse-proxied. See Note below.
- **zimbraMailPort** to 8080, to avoid port conflicts.
- **zimbraMailSSLPort** to 8443, to avoid port conflicts.
- **zimbraReverseProxyLookupTarget** to TRUE
- **zimbraMailMode** to http. This is the only supported mode.
- **zimbraMailReferMode** to reverse-proxied. See Note below.
- **zimbraMailProxyPort** to 80, to avoid port conflicts.
- **zimbraMailSSLProxyPort** to 443, to avoid port conflicts.
- **zimbraReverseProxyHttpEnabled** to TRUE to indicate that Web proxy is enabled.
- **zimbraReverseProxyMailMode** defaults to both.

If you want to set the proxy server mail mode, add to the command the **-x** option with the mode you desire: **http**, **https**, **both**, **redirect**, **mixed**.

2. Restart services on the proxy and mailbox servers, run
 - a. **zmcontrol stop**
 - b. **zmcontrol start**
3. Configure each domain with the public service host name to be used for REST URLs, commonly used in sharing Document Notebooks, email and Briefcase folders. Run

```
zmprov modifyDomain <domain.com> zimbraPublicServiceHostname  
<hostname.domain.com>
```

REST URL Generation

When HTTP proxy is enabled, the following attributes can be set globally or by domain for REST URL

- **zimbraPublicServiceHostname**
- **zimbraPublicServiceProtocol**
- **zimbraPublicServicePort**

When generating REST URL's:

- If domain.**zimbraPublicServiceHostname** is set, use **zimbraPublicServiceProtocol + zimbraPublicServiceHostname + zimbraPublicServicePort**
- Otherwise it falls back to the server (account's home server) attributes:
 - protocol is computed from server.**zimbraMailMode**
 - hostname is **server.zimbraServiceHostname**
 - port is computed from the protocol.

Note: Why use **zimbraMailReferMode** - In earlier versions of Zimbra, a local config variable called **zimbra_auth_always_send_refer** was used to determine what the backend server did when a user whose mailbox did not reside on that server logged in on that server. the default value of **FALSE** meant that the backend server would only redirect the user if the user was logging in on the wrong backend host.

On a multi-server ZCS, however, if a load balanced name was needed to create a friendly landing page, a user would always have to be redirected. In that case, **zimbra_auth_always_send_refer** was set to **TRUE**.

Now with a full-fledged reverse proxy, users do not need to be redirected. The localconfig variable **zimbraMailReferMode** is used with nginx reverse proxy.

Configuring Zimbra Proxy for Kerberos Authentication

If you use the Kerberos5 authenticating mechanism, use the following steps to configure IMAP and POP proxy.

Note: Make sure that your Kerberos5 authentication mechanism is correctly configured before you do this. See the *Zimbra Directory Service chapter, Kerberos5 Authentication Mechanism*.

1. To set the default Kerberos domain for authentication, on each proxy node, set the **zimbraReverseProxyDefaultRealm** server attribute to the realm name corresponding to the proxy server. For example, enter as:

```
zmprov ms [DNS name.isp.net] zimbraReverseProxyDefaultRealm [ISP.NET]
```

2. Each proxy IP address where email clients connect must be configured for GSSAPI authentication by the mail server. On each proxy node for each of the proxy IP addresses, enter the following command:

```
zmprov mcf +zimbraReverseProxyAdminIPAddress [IP address]
```

3. On each proxy server, run the following commands:

```
zmprov ms [proxyexample.net] zimbraReverseProxyImapSaslGssapiEnabled TRUE
```

```
zmprov ms proxyl.isp.net zimbraReverseProxyPop3SaslGssapiEnabled TRUE
```

4. Restart the proxy server(s), type:

```
zmproxyctl stop
```

```
zmproxyctl start
```

Chapter 7 Managing Legal Requests for Information

Legal Intercept for Law Enforcement

The ZCS legal intercept feature is used to obtain copies of email messages that are sent, received, or saved as drafts from targeted accounts and send these message to a designated “shadow” email address. Legal Intercept can be configured to send the complete content of the message or to send only the header information. When a targeted account sends, receives, or saves a draft message, an intercept message is automatically created to forward copies of the messages as attachments to the specified email address.

Legal Intercept attributes

The legal intercept feature can be configured either for a Class of Service or for individual accounts. The feature is configured from the CLI, using **zmprov**.

The following attributes are used to configure the feature:

zimbralInterceptAddress	Intercepted messages are sent to this address. When this attributes is empty, legal intercept is off. You can have multiple recipients for an intercepted message
zimbralInterceptSendHeadersOnly	The default is False . Change to True to have only the message headers sent, not the message body
zimbralInterceptFrom	Used to construct the From: header content used in the intercept message. The default is Postmaster@<address.com>

zimbralInterceptSubject	The template used to construct the subject -line the intercept message should show. The default subject line reads "Intercept message for account@example.com <intercepted message subject> "
zimbralInterceptBody	The template used to construct the body of the intercept message. The default message is "Intercepted message for < account@example.com. Operation=<type of message>, folder=<folder>, folder ID=<#>. "

The following parameters can be used in the From, Subject, and Body templates to modify the default intercept message:

- **ACCOUNT_DOMAIN.** Domain of the account being intercepted.
- **ACCOUNT_ADDRESS.** Address being intercepted.
- **MESSAGE_SUBJECT.** Subject of the message being intercepted.
- **OPERATION.** Operation that the user is performing, "add message", "send message", or "save draft"
- **FOLDER_NAME.** Name of the folder to which the message was saved.
- **FOLDER_ID.** ID of the folder to which the message was saved.
- **NEWLINE.** Used for formatting multi-line message bodies.

Configuration

The only required configuration to setup legal intercept is to enable the feature on the target accounts. You can enable the attribute to send only the header information of the email message, not the complete message.

The default intercept cover email message and the name in the **From** field can also be modified.

How to set up legal intercept

1. Define the intercept address

- If enabling by COS, type **zmprov mc <cosname> zimbralInterceptAddress <account@intercept_example.gov>**
- If enabling by account, type **zmprov ma <accountname@domain.com> zimbralInterceptAddress <account@intercept_example.gov>**

If you are going to use the default intercept message template and From name, legal intercept is set up.

To enable the attribute so that only header information is forwarded, go to step 2.

To modify the attributes of the intercept message continue with step 3.

2. To send only the header information, not the complete message, type

```
zmprov ma <accountname@example.com>
zimbraInterceptSendHeadersOnly TRUE
```

3. To change the From name, type

```
zmprov ma <accountname@example.com> zimbraInterceptFrom
<newname@example.com>
```

4. To change the text of the Subject line, type

```
zmprov ma <accountname@example.com> zimbraInterceptSubject
<Intercepted message subject text> parameter parameter
```

5. To change the text in the message body, type

```
zmprov ma <accountname@example.com> zimbraInterceptBody
<Intercepted message text> parameter <text> parameter
```

Note: To modify by COS, type `zmprov mc`.

Create Mailbox Snapshots for Legal Discovery

You can create a query for the user's mailbox using the REST URL format to search for specific types of email messages and attachments and have these messages zipped and saved to your computer. This zip file can be forwarded to a requesting law enforcement agency.

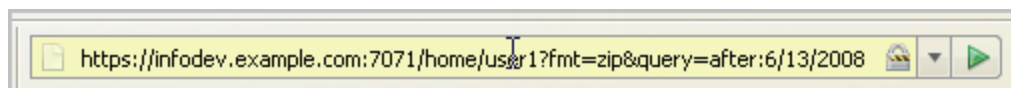
When the file is unzipped, each messages is displayed as an .eml file. The attachments are saved in the format they were delivered.

How to create a mailbox snapshot zip file

You must be logged into the ZCS administration console to create the zip file. You create a zip file for one account at a time.

1. In the address field of the browser, after **7071/** type:

home/<username>?fmt=zip&query=<criteria_name>



In the above example, a zip file of all email messages and attachments in the Inbox after June 13, 2008 is created for an account called user1.

You can use any search operators that are used for searching in ZCS. For example you can search by folder (in:<folder_name>), by sender's name (from:<someone>), and you can use multiple search terms. See the **Search Tips** wiki page for keyword examples, http://wiki.zimbra.com/.php?title=Search_Tips.

2. Press **Enter** or the arrow to create the zip. A Confirm box displays, asking if you want to navigate away from this page. You do not leave the admin console page.
3. Click **OK**. The zip file is made that includes the messages and attachments, a browser download dialog opens and you are asked to save it to disk.

This zip file is ready to be delivered. The names of the .eml files are the subject lines from the messages.

Chapter 8 Using the Administration Console

The Zimbra administration console is the browser-based user interface ZCS administrators use to centrally manage Zimbra servers and user accounts.

When you log onto the administration console, the tasks you are authorized to perform display on the console's Navigation pane. These tasks are based on the rights assigned to the administrator role.

Two types of administrator accounts can be created to manage ZCS:

- **Global Administrators**, who have full privileges to manage servers, global settings, domains, accounts and create other administrators. One global administrator account is initially created when the software is installed. Additional global administrator accounts can be created. Administration tasks can be performed either from the administration console or using the Zimbra command line interface tools.
- **Delegated Administrators**, who are administrators that are granted customized administrator roles by the global administrator to manage different tasks from the administration console. To understand how delegated administration works, see the [Delegated Administration](#) chapter.

Logging In

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.

Note: A different login and logout page can be configured either as a global setting or as a domain setting. The attributes to modify are **zimbraAdminConsoleLoginURL** to specify a URL to redirect administrators if their log in is not authenticated or authentication has expired, and **zimbraAdminConsoleLogoutURL** to specify a URL to redirect administrators when they log out.

Changing Administrator Passwords

The first global administrator password is created when the ZCS 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

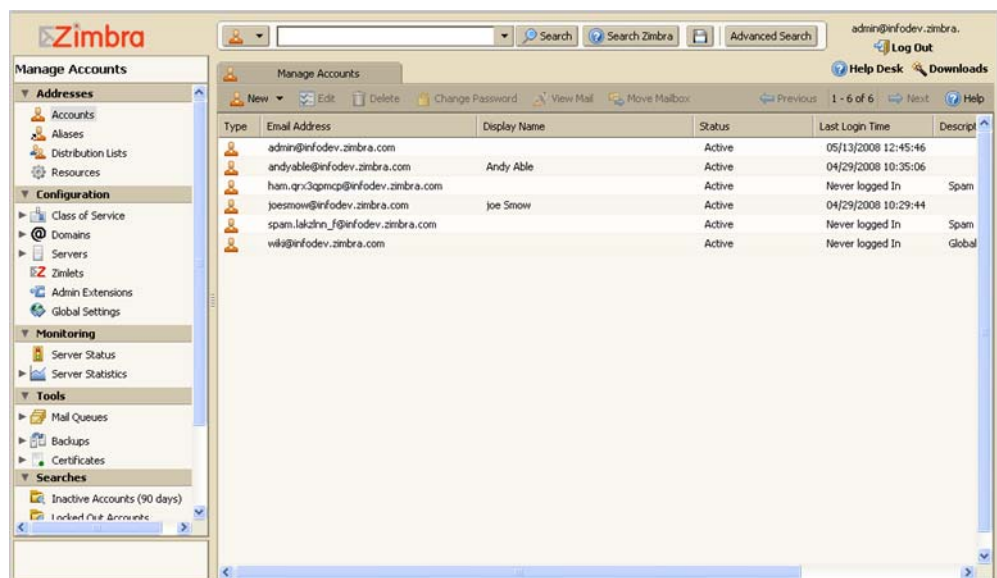
About the Administration Console

When global administrators log on to the administration console, the right Content pane displays the Server Status and the left Navigation pane displays all the functions exposed through the console.

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

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

Administration Console - Managing Accounts Page



The Navigation pane includes the following sections and folders:

Addresses

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

Configuration

- **Class of Service.** Lists classes of service (COS) that have been created. As a minimum, the default COS is displayed. You can create, edit, or delete COS definitions.
- **Domains.** Lists the domain in the ZCS 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.
- **Rights.** This folder displays the system-defined rights that can be granted to delegated administrators. The name of the right, the target types associated with that right, the right type and a brief description of the right are displayed. System administrators can review this to select the correct system-defined right when granting rights to delegated administrators.
- **Global ACL.** (ACL is Access Control List) For delegated administration this folder displays the global rights that have been granted. Global ACLs are granted to all entries in a target type. For example, when the +listAccount right is granted to an administrator that administrator can view the Accounts list for all domains in the ZCS environment.

Monitoring

- **Server Status.** Shows the current status, either **On** or **Off**, for all servers that are running Zimbra MTA, Zimbra LDAP, Zimbra Store, SNMP, and the anti-virus service.
- **Server Statistics.** Shows both system-wide and server specific data about the inbound message volume, inbound message count, anti-spam/anti-virus activity and disk usage for messages processed in the last 48 hours, 30 days, 60 days, and the last year. Server specific data includes a Session tab that shows active session information for the Web Client, Administrators, and IMAP, and a Mailbox Quota tab that shows quotas for individual accounts.

Tools

- **Mail Queues.** Shows the number of messages on the Zimbra MTA that are in the Deferred, Incoming, Active, and Hold queues.
- **Certificates.** You can easily install, manage, and view self-signed and commercial certificate details for Zimbra servers from the administration console.
- **Backups.** You can start a backup session, view the back sessions and their status, and restore mailboxes from specific backup sessions.
- **Search Mail.** This is a cross mailbox search for content across live and archive mailboxes and is only displayed if the Archive Mailbox feature is installed. Note: The Archive Mailbox feature is an optional package.
- **Software Updates.** The Software Updates feature can be set up to notify administrators when newer ZCS updates are available. Software Updates is configured with how often to check for updates and the email address that receives the notification.

Searches

- In the **Searches** section of the Navigation pane, several popular search queries, including search for inactive accounts, search for locked out accounts, and search for closed accounts, are available.

Managing Tasks from the Administration Console

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

- Create and manage end-user accounts
- Create many accounts at once using the Build Provisioning Wizard
- Monitor server status and performance statistics
- Create and manage delegated administrators
- 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.
- Move a mailbox
- Cross mailbox searches
- Check to see if new ZCS updates are available
- Easily access the Zimbra migration tools from the administration console's downloads page.

See the [Chapter 10, Managing ZCS Configuration](#), for information about how to configure these functions.

Tasks Not Available from Administration UI

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

Use CLI command utilities for the following. See “[Appendix A Command-Line Utilities](#)” on page 227 for details about the commands.

- Start and stop services, CLI **zmcontrol**
- Manage local server configuration, CLI **zmlocalconfig**
- Create a message of the day to display on the administration console, CLI **zmprov**. See [Setting up a Message of the Day](#).

Creating Message of the Day for Administrators

Global administrators can create messages of the day (MOTD) that can be viewed when global and delegated administrators log into the administration console.

A global or domain multi-value attribute, **zimbraAdminConsoleLoginMessage**, is used to create a MOTD. The message is created from the CLI **zmprov**.

Every time an admin logs in the message displays at the top left on the administration console. They can close the message. The message displays until it is replaced or removed.

Example of a Message of the Day



To create a message of the day

You can create a message globally or for a specific domain.

1. To create by domain type:

```
zmprov md domainexample.com zimbraAdminConsoleLoginMessage  
"message to display"
```

The quotes must be used.

You can create more than one message to display. Run the command again to create additional messages, but add a plus sign (+) before the attribute, as in this example

```
zmprov md domainexample.com +zimbraAdminConsoleLoginMessage  
"second message to display"
```

To remove a message of the day

To remove a specific message, type the attribute, adding a minus sign (-) before the attribute and type the message as it is shown.

```
zmprov md domainexample.com -zimbraAdminConsoleLoginMessage  
"message to display"
```

To remove all messages, type the attribute and add a single quote at the end.

```
zmprov md domainexample.com zimbraAdminConsoleLoginMessage `
```

Checking for ZCS Software Updates

When ZCS is installed, the ZCS software update utility is automatically configured to check for the latest ZCS version once a day and if there is an update to send notification to the address that is configured in the administration console's Server Updates tab.

From this tab, you can configure the following:

- **Server that checks for updates.** The pull-down tab lists all available servers. Only one server is configured. The selected server checks for updates and the result of the update response from www.zimbra.com is stored in LDAP.
- **Check for updates every ____.** The default is to check once a day. You can change the frequency interval to check every x hours, minutes, or seconds. A cron job is configured to check for new updates. If the frequency interval is less than 2 hours, the crontab file must be modified.
- **Updates URL.** This address is the URL that the server connects to when checking for updates. When a ZCS server checks for updates, it transmits its version, platform, and build number to Zimbra. Normally, this URL is not changed.
- To be notified of updates, check the **Send notification email when updates are available** and enter the send to and send from addresses. The default address is the administrator's address.
- A generic email is created. The subject and content of the email can be changed.

When a server polls the URL specified, the response is displayed in the Updates tab.

Chapter 9 Delegated Administration

The Delegated Administration feature lets you create different delegated administrator roles to manage your ZCS environment. Accounts or distribution lists are assigned administrator rights. These administrator accounts/distribution lists are granted rights to perform administrator tasks on a specific target.

ZCS delegated administration is flexible. Delegated administrator roles can be as simple as having the rights to manage one or more distribution lists or reset forgotten passwords for one or more users, to having domain administration rights on one or more domains.

This chapter explains how the delegated administration feature can be used to create any type of delegated administrator role.

Two frequently used delegated administrators roles, domain administrators and distribution list administrators, are already defined. You can add administrators to these pre-defined roles with no other configuration necessary.

The global administrator provisions these accounts and configures the delegated administrator access rights from the administration console.

Delegated Administration Terminology

The following are delegated administration terms and concepts you should understand.

Admin Group. An admin group is a distribution list that has been assigned an administrator role. Administrator accounts that are part of the admin group distribution list inherit the rights that are assigned to the admin group. Non-administrator accounts can coexist in the same group but these accounts do not inherit rights.

Admin Account. An admin account is an individual user account that has been assigned an administrator role to administer specific targets.

Grantee. Grantee refers to the admin user who has been granted specific permissions (rights) to administer a target. This can be a individual user account (Admin Account) or a group defined as an Admin Group.

Rights. Rights are the functions that the delegated administrator can or cannot perform on a target. Both positive and negative rights can be set. Rights can be either a System Defined Right or Attribute Right.

Target. A target is a ZCS object on which rights can be granted. The following are the specific types of targets that can be specified: Account, Calendar Resource, Class of Service (COS), Distribution List (DL), Domain, Global Config, Global Grant, Server, and Zimlet.

Grant. A grant specifies the specific grantee who can or cannot view or modify the right on a target. A grant is stored in the LDAP attribute, **zimbraACE**, on the target entry.

Access Control Entry (ACE). A grant is represented by an ACE. An access control entry is the specific access granted on a target. An ACE is stored in an LDAP attribute on the target entry. The ACE includes the following information: Zimbra ID of the grantee, type of grantee - either user (usr) or group distribution list (grp), and the allowed or denied right. A grant is serialized in the form of an ACE stored in LDAP.

Access Control List (ACL). Access control list is a list of the access control entries (ACE) set on a specific target. Each target type includes a ACL tab which shows a list of ACEs set on the current target. An ACE defines what an grantee can do on the current target. In the administration console, the ACL tab on each target lists all the ACEs granted to that target.

Admin View. An admin view refers to the tabs and content on the administration console a delegated administrator sees when he logs in. The admin view is configured when an administrator or administrator group is created. A directly assigned admin view is the view set on the admin account. An inherited admin view is the view set on the admin group the account belongs to.

How Delegated Administration Rights are Granted

Delegated administration provides a way to define access control limits on targets and grant rights to administrators to perform tasks on the target.

Selecting Target Types

A target is a ZCS object on which rights can be granted. Each target is associated with a target type that identifies the type of access control entries you can grant on the target. When selecting a target type for a target consider:

- Which specific target (ZCS object) are you configuring?
- Have you chosen the correct target type for the rights you want to grant?
- What is the scope of targets in which granted rights are effective?

Selecting a Target

Which specific target are you granting rights? For example, if the target type you select is “domain”, which domain do you mean? You specify a specific domain’s name (Target Name = example.com). ACEs are granted on that target.

Do the Rights Work with the Target Type

Is the right you want to grant applicable to the selected target type? A right can only be applied on the type or types of object that are relevant to the target type.

For example, creating an account can only apply to a domain target type and the setting passwords can only apply to accounts and calendar resources target types. If a right is granted on a target that is not applicable to the target, the grant is ignored.

Scope of Rights Across Selected Target Type

When defining rights, you need to consider the scope of targets in which granted rights are effective. Domain targets can include account, calendar resource, and distribution list rights, as well as specific rights on the domain. For example, the right to set the password is applicable only to accounts and calendar resources, but if this right is included in the domain targets list of rights, it is effective for all accounts or calendar resource in the domain.

Target Type	Description of Target Scope
Account	An account entry (a specific user)
Calendar Resource	A calendar resource entry
COS	COS entry
Distribution List	<p>If the right is applicable to distribution lists, the distribution list and all distribution lists under this distribution list.</p> <p>If the right is applicable to accounts and calendar resources, all accounts and calendar resources that are direct or indirect members of this distribution list.</p>
Domain	<p>Domain entry is only applicable to a specific domain, not to any sub-domains.</p> <p>Sub-domains must be explicitly marked as targets.</p> <p>When domain is the target, the rights granted can be given for all accounts, calendar resources and distribution lists in the domain.</p>
Config	Grants specific to global config

Target Type	Description of Target Scope
Global ACL	<p>The global ACL is used to grant administrator rights for all entries in a target type. For example, you could add an ACE to the Global ACL that grants the right to create accounts on domains.</p> <p>Delegated administrator accounts that are granted this right can create accounts in all domains in the system.</p>
Server	The server entry
Zimlet	A Zimlet entry

Rights

Rights are the functions that a delegated administrator can or cannot perform on a named target. Right types can be either system-defined rights or attribute rights.

System-defined rights

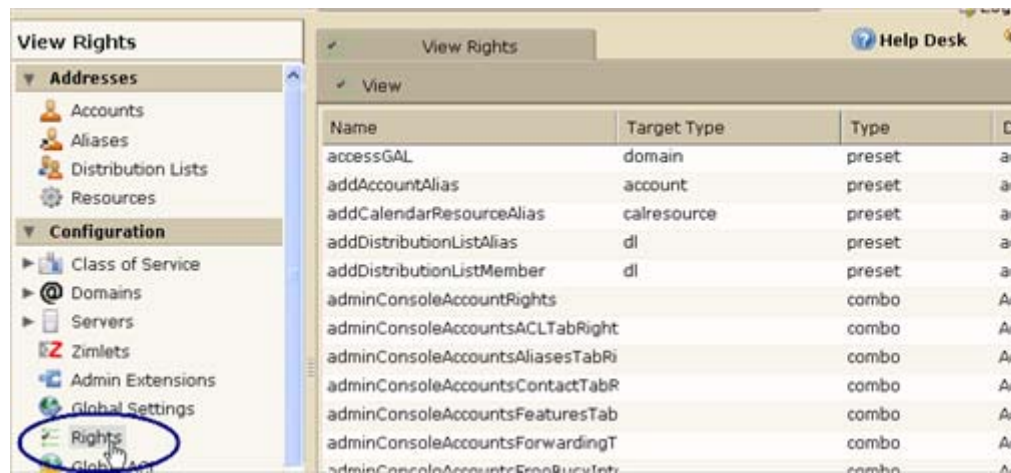
Four types of system defined rights can be granted: preset, setAttrs, getAttrs, and combo.

- Preset rights (**preset**) are described as:
 - Having predefined, fixed implication on targets. For example, createAccount creates an account; renameDomain, renames the domain.
 - Associated with a fixed target type. For example, createAccount is a right only on a domain; renameAccount is a right on an account; see Server is a right on a server
 - Independent of other rights on the same target. No other rights are required to administer that action on the target.
 - Possibly requires granting rights on multiple targets in order for the right to be valid. If the right involves accessing multiple targets, the grantee needs to have adequate rights on all pertinent targets. For example, to create an alias for an account, the grantee must have rights to add an alias to an account and to create an alias on a domain.
- The set attribute (**setAttrs**) rights allows the domain administrator to modify and view an attribute value. For example, the **modifyAccount** right would allow the domain administrator to modify all attributes of the account.
- Get attribute rights (**getAttrs**) lets the domain administrator view an attribute value. For example, the getAccount right would show all the attributes for a user's account.
- Combo right is a right that contains other rights. Combo rights can be assigned to any target type. You can use combo right to grant multiple attribute rights quickly on targets.

System rights are listed and described in the Rights folder in the administration console Overview pane.

You can use the Rights folder to help you define which system-defined rights to grant to delegated administrators. This folder displays the name of the right, the target types associated with that right, the right type and a brief description.

System-Defined Rights List on Administration Console

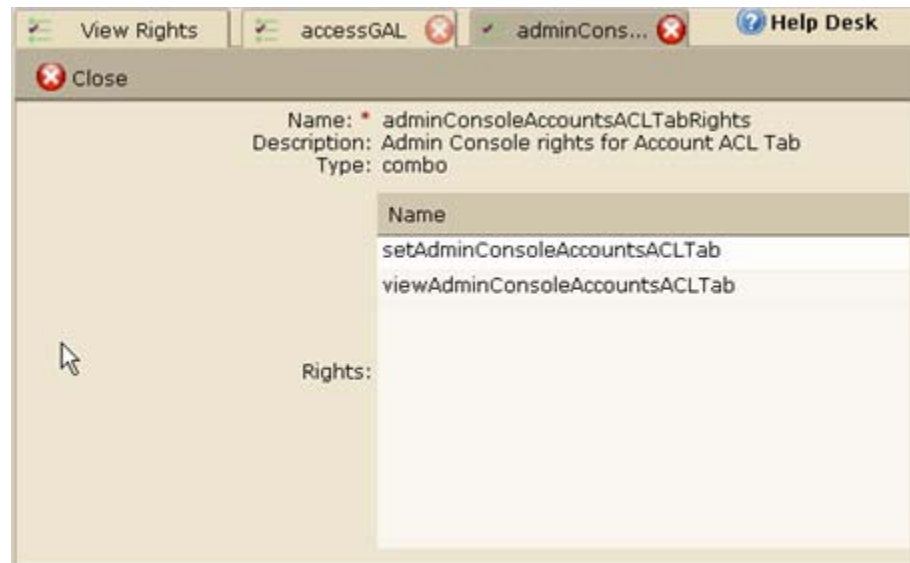


Name	Target Type	Type	D
accessGAL	domain	preset	ai
addAccountAlias	account	preset	ai
addCalendarResourceAlias	calresource	preset	ai
addDistributionListAlias	dl	preset	ai
addDistributionListMember	dl	preset	ai
adminConsoleAccountRights		combo	ai
adminConsoleAccountsACLTabRight		combo	ai
adminConsoleAccountsAliasesTabRi		combo	ai
adminConsoleAccountsContactTabR		combo	ai
adminConsoleAccountsFeaturesTab		combo	ai
adminConsoleAccountsForwardingT		combo	ai
adminConsoleAccountsGroupTabRi		combo	ai

When you select a right on the page and click on it, another page displays more information

- For combo rights, a list of the rights associated with the combo right are listed
- For the other system rights, a list of attributes associated with the right are listed

Detailed View of Combo Rights



System-defined rights can be granted as positive or negative rights. This lets you negate some right from a combo right or attributes from the other system-defined rights.

System Defined Rights Lists. You can use the `zmprov` CLI to see system defined rights for a specific target.

- Account, type as `zmprov gar account`
- Calendar Resources, type as `zmprov gar calresource`
- COS, type as `zmprov gar cos`
- Distribution List, type as `zmprov gar dl`

All rights for account and calendar resources can also be granted on distribution list targets. When these rights are granted on a distribution list, the ACEs apply the right to all direct or indirect account or calendar resource members of the distribution list.

- Domain, type as `zmprov gar domain`

All rights for accounts and calendar resources can also be granted on domain targets.

All rights for distribution list can also be granted on domain targets.

When rights are granted on a domain, the ACEs apply the right to all direct or indirect account calendar resource, and members of the distribution list in the domain.

- Global Config, type `zmprov gar config`
- Global Grant, type `zmprov gar global`

All rights for all other targets can also be granted on the global targets. When any rights are granted on a global grant entry, the ACEs apply the right to all entries on the system. For example, if you grant a createAccount (which is a domain right) to AdminA on the global grant entry, AdminA can create accounts in all domains on the system.

- Server, type **zmprov gar server**
- Zimlets, type, **zmprov gar zimlet**

Attribute Right

An attribute right is specific to a defined attribute. Granting rights at the attribute level allow a delegated administrator/administrator group to modify or view (or not modify or view) a specific attribute on a target.

The specific attribute being granted is configured on the target and the type of permission, read (get) or write (set), is specified. To create an ACE based on an attribute right:

- Select the target to add the ACE.
- Select the delegated administrator as the Grantee Name.
- Select Attribute Right instead of System-Defined Right.
- Select whether the grant should be to Read (view) or Write (view and change).
- Select the attribute target type.
- Type the attribute name. As you do this the Right name is automatically entered in the text field.

*Note: If you want to see a list of all the attributes, use the **zmprov desc CLI**. Note that this list also contains attributes that cannot be granted as rights.*

- Select whether this is a positive or negative right.

The example below is adding the right to view the status of accounts on a domain.

Add ACE

Grantee Name:* da20@example.com

Target Type: domain

Target Name:* example.com

Right Type:* Attribute Right

Attribute Right Verb:* Read

Attribute Right Target Type:* domain

Attribute Name:* zimbraMailStatus

Right Name:* get.domain.zimbraMailStatus

☒ Is Positive Right (Allow)

☐ Can grant the right to other admins

Help Cancel Add and More Add and Finish

Attribute rights can be granted in any combination of attributes to grant positive or negative rights. This lets you negate some attributes from a grant.

Positive or Negative Rights

Rights can be either positive or negative. Negative rights are rights specifically denied to a grantee. Negative rights can be granted to administrator groups and individual administrators. The purpose of having negative rights is to be able to revoke a right granted to a wider scope of grantees or granted on a wider scope of targets.

- When a negative right is granted to an admin group, all administrators in the group are denied that right for the target and sub-targets on which the right is granted.
- When a negative right is granted to an administrator who may or may not be in an admin group, the specific administrator is denied that right for the target and sub-targets on which the right is granted.

Example of applying a negative right to remove certain rights to specific administrators in an admin group

An admin group is granted domain administrator rights, including the right to create accounts on Domain1. AdminA is in this admin group, but you want AdminA to have all domain administrator rights, except the right to create accounts. You would grant a negative **createAccount** right to AdminA on the target Domain1.

Example of applying a negative right to remove a right on certain sub-targets

If an admin group is granted the right to view accounts in a domain from the administration console but you did not want the admins in this group to view specific executive accounts, such as the CEO and CFO accounts, you would grant a negative **adminLoginAs** right to this admin group directly on each target account. In this case, to the CEO and CFO's accounts. No one in this admin group can log in as an admin to these two accounts.

For grants on the same level, negative rights always take precedence. For example, AdminGroup1 is granted a positive right to view accounts in a domain; AdminGroup2 is granted a negative right to view accounts in the same domain. AdminA is a member in both admin groups. AdminA cannot view any account in this domain because the negative right takes precedence.

For grants on different levels, the most specific grant takes precedence. For example, AdminA is granted the negative right to view accounts in GroupDistributionList1 which User1 is a member. AdminA is also granted the positive right to view account directly on User1's account. In this case, AdminA can view User1's account as the grant on the account target is more specific than the grant on the distribution list.

Implementing Delegated Administration

The global administrator provisions delegated administrators and delegated administrator groups.

Before you create delegated administrators and grant rights, you define the role and which rights to assign to the targets the administrator will manage. If you do not add the correct rights when you create the delegated administrator, you can edit the account later.

For more efficient management of delegated administrators, create administrator groups and add individual administrator accounts to the group. An administrator group allows you to create role-based access control. Administrators with the same or almost the same responsibilities can be grouped into an admin group.

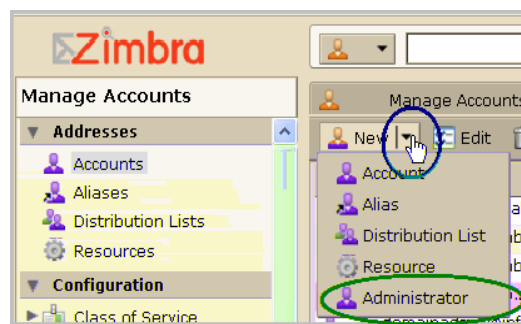
Note: Accounts that are configured as global administrator accounts cannot be granted ACLs. Global administrator accounts automatically have full rights on ZCS. If an ACL is added to a global administrator account, it is ignored. If a delegated administrator account is changed to a global administrator account, any ACLs associated with the account are ignored.

Delegated administration rights can be set up in one of the following methods:

- **Create admin accounts.** Create an administrator or an administrator group and grant rights to the account using the Administrator Wizard.
- **Configure grants** on existing administrator accounts. Add new rights or modify rights to an existing delegated administrator or administrator group account.
- **Set ACEs directly on a target.** Add, modify and delete rights directly in a target's Access Control List tab.

Creating Administrator Groups and Administrators

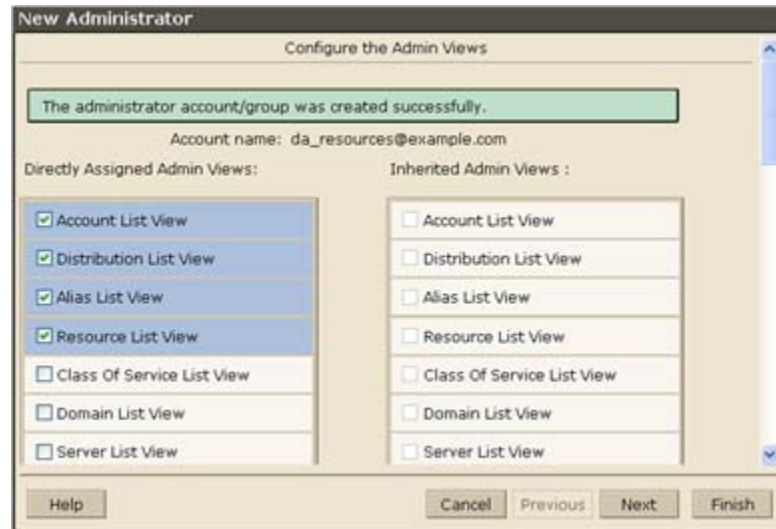
In the administration console Manage Accounts section, you use the Administrator wizard to create new administrator or group administrator accounts, add views and grant rights. On the Accounts toolbar, select **Administrator** from the New drop-down menu.



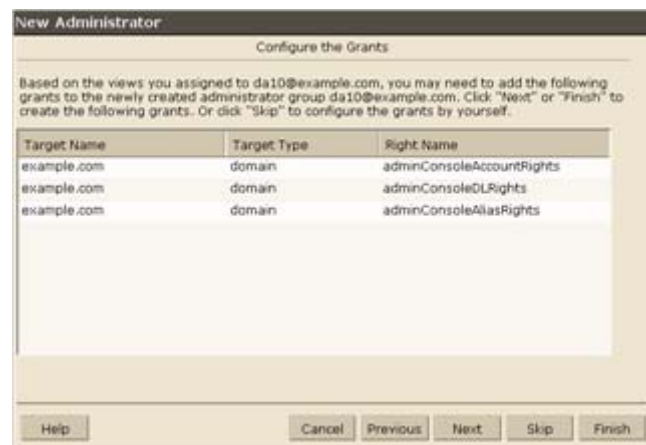
The wizard walks you through the following steps.

4. An admin view represents the items the delegated administrator sees when logged on to the administration console. You select the views from the Directly Assigned Admin views list.

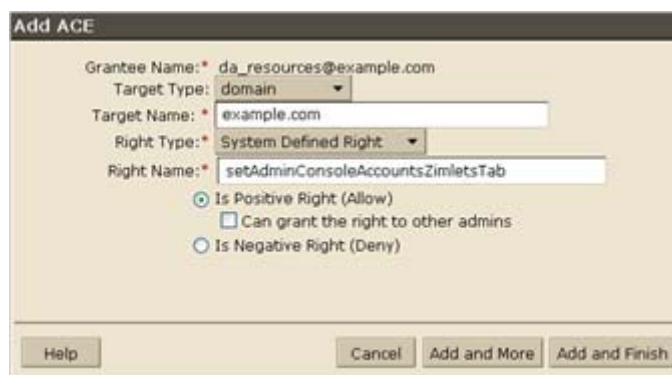
If you had assigned an Administrator Role when you created the account, the Inherited Admin Views column would highlight the views that are inherited from the role you assigned.



5. Click Next. The **Configure the Grants** dialog displays a list of all the grants necessary to display all the items you selected in the directly assigned views column. You can click Next to accept these rights and add additional rights, Skip to not configure these rights, or Finish to accept these rights and quit the wizard.

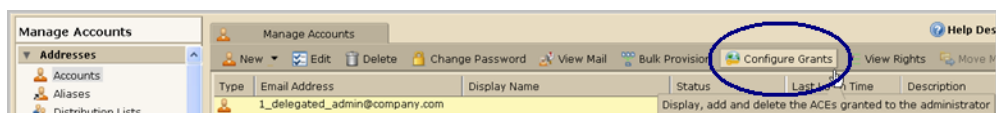


6. Click Next to accept the rights and add additional rights. Add access rights (ACE) to the account. Select the target type, the target name to administer, and the rights to be granted. You can add multiple rights and they can be either positive or negative.



Configure Grants on Administrator Accounts or Admin Groups

You can manage the rights granted to an administrator or an administrator group through the Configure Grants link on the accounts toolbar. When you click **Configure Grant** on the Manage Accounts Addresses toolbar, the Content pane shows a list of direct and interited grants. You can grant rights, modify rights or delete rights on existing administrator accounts.



Granting ACLs to a Target

When you want to add a specific grantee or specific rights on a target you can edit the target directly. Each target has an ACL tab which lists the granted ACLs. You can add, edit or delete the target's grants. The administration account (grantee) is updated to reflect the change.

Revoking Rights

Global administrators can revoke any rights granted to an administrator.

1. Open the administrator account and click **Configure Grants**.
2. Select the right to revoke and click **Delete**.
3. When the dialog asks if are sure, click **Yes**.

To temporarily revoke rights to a delegated administrator account, you can edit the administrator account and remove the check next to the Administrator field. The ACLs are not removed from the account.

Delegated administrators can revoke rights if the right was created with the **Can Grant the right to other admins** enabled.

The 'Add ACE' dialog box contains the following fields and options:

- Grantee Name: * delegatedadmin@example.com
- Target Type: [Dropdown]
- Target Name: *
- Right Type: *
- Right Name: *
- Is Positive Right (Allow) ☐
- ☒ Can grant the right to other admins
- Is Negative Right (Deny) ☐
- Buttons: Help, Cancel, Add and More, Add and Finish

Viewing Rights Granted to Administrators

The View Rights link from an admin account or admin group account toolbar displays the granted rights, readable attributes and modifiable attributes associated with a specific target. Click on the tabs to view rights for different targets.

Viewing Rights for Domain Administrator Account View

The 'View Rights' window shows the following information:

- Accounts | Distribution Lists | Domains | Class of Service | Global ACL | Zimlets | Global Settings | Servers | Resources
- All the effective rights zimbradomainadmins@infodev.lab.zimbra.com has on the "account" target.
- By Domains: infodev.lab.zimbra.com
- Grantee: zimbradomainadmins@infodev.lab.zimbra.com
- Accounts in domain(s) infodev.lab.zimbra.com
- Granted Rights: addAccountAlias, deleteAccount, getAccountInfo, getAccountMembership, getMailboxInfo, listAccount, removeAccountAlias, renameAccount, setAccountPassword, viewAccountAdminUI
- Readable Attributes: cn, co, company, description, displayName, givenName, initials, l, postalCode, sn, st, street, telephoneNumber, uid, zimbraAccountStatus, zimbraAdminSavedSearches, zimbraDomainAdminMaxMailQuota, zimbraFeatureMailForwardingEnabled, zimbraHideInGal, zimbraIsDelegatedAdminAccount, zimbraLastLogonTimestamp, zimbraMailAlias, zimbraMailCanonicalAddress, zimbraMailForwardingAddress, zimbraNotes, zimbraPasswordMustChange, zimbraPrefMailForwardingAddress, zimbraPrefMailLocalDeliveryDisabled
- Modifiable Attributes: co, company, description, displayName, givenName, initials, l, postalCode, sn, st, street, telephoneNumber, zimbraAccountStatus, zimbraAdminSavedSearches, zimbraDomainAdminMaxMailQuota, zimbraFeatureMailForwardingEnabled, zimbraHideInGal, zimbraIsDelegatedAdminAccount, zimbraMailAlias, zimbraMailCanonicalAddress, zimbraMailForwardingAddress, zimbraNotes, zimbraPasswordMustChange, zimbraPrefMailForwardingAddress, zimbraPrefMailLocalDeliveryDisabled

Predefined Delegated Administrator Role

The following preconfigured administrator groups are created automatically. You can assign administrator accounts to these groups.

Domain Administration Group

The **zimbradomainadmins** delegated admin group grants all the rights necessary to support ZCS domain administration for accounts, aliases,

distribution lists and resources. You add the individual administrator accounts to this administration group DL.

Administrators who are part of the zimbradomainadmins group can create and manage accounts including setting the account quota, aliases, distribution lists, and resources accounts in their domain.

Domain Administration Console View

When domain administrators log onto the administration console, only the functions they are authorized to manage are displayed on the console's Navigation pane.

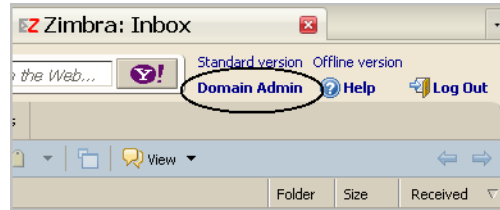


In addition, the domain administrator can access the following utilities on the Downloads page to be used for accounts on domains they administer:

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

Quick access to the administration console.

For domain administrators, all tasks are performed from the administration console. To facilitate easy log in, when a delegated administrator account is created, their ZWC account can be configured with a quick link to the administration console.



The link is created from the zmprov CLI. To create the link to the admin console login page, you configure the URL.

```
zmprov md <server.domainexample.com> zimbraWebClientAdminReference <https://server.domainexample.com:7071/
```

Distribution List Administration Group.

The **zimbradladmin** delegated admin group grants all the rights necessary to log on to the administration console and manage distribution lists. You add administrator accounts to this administration group DL.

Administrators who are part of this group can

- View the account list
- Create new distribution lists and edit and delete distribution lists
- Add, edit and remove members in a distribution list

Specific Access Rights

Frequently requested access rights are described below. The steps to set up an administrator to manage multiple domains are described in this section.

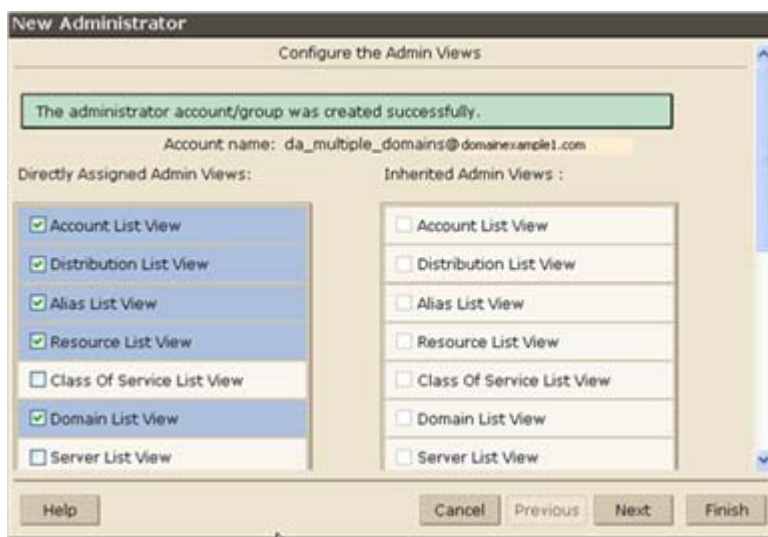
Manage multiple domains

To have one domain administrator manage more than one domain, you assign the rights to manage individual domains to the administrator account or administrator group.

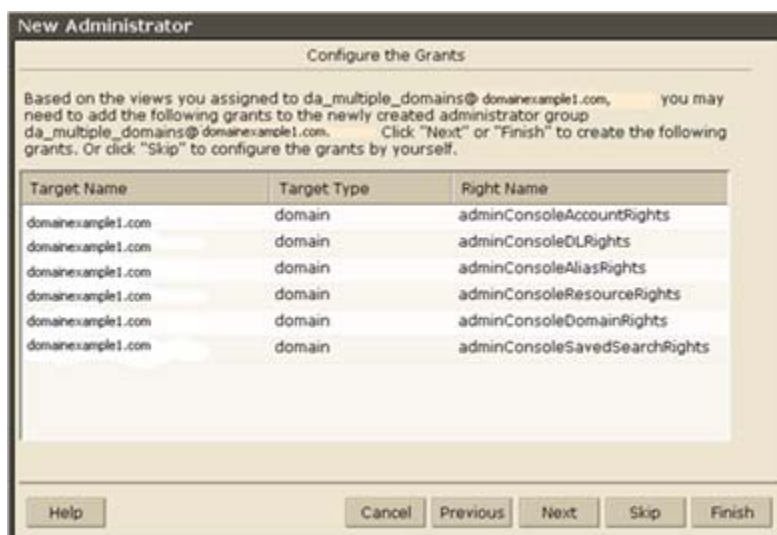
For example, to set up domanadministrator1@example.com to manage domainexample1 and domainexample2.com. Create a new administrator account on one of the domains to be managed.

1. Click **New>Administrator** and create the administrator account on one of the domains to be managed (domainexample1.com)
2. Select the following views that domain administrators need to manage a domain:
 - Account List View

- Distribution List View
- Alias List View
- Resource List View
- Domain List View
- Saved Searches View



3. Click **Next** to configure the grants for this domain. When the views are selected, the rights associated with these views automatically display on the Configure the Grants dialog.



Click **Next**. The informational box shows the grants were created.

Click **OK** in the Informational window.

The Configure Grants dialog displays again

4. Now you add another domain to be managed (domainexample2.com).
 - On the Configure Grants page, click **Add**
 - Select the target type as **domain**
 - Enter the target's domain name (domainexample2.com)
 - Right Type, select System Defined Right
 - Right Name type, adminConsoleAccountRights. **Is Positive Right** should be selected.
 - Click **Add and More**

Add ACE

Grantee Name: * da_multiple_domains@infodev.lab.zimbra.com

Target Type: domain

Target Name: * domainexample2.com

Right Type: * System Defined Right

Right Name: * adminConsoleAccountRights

☒ Is Positive Right (Allow)

☐ Can grant the right to other admins

☐ Is Negative Right (Deny)

Help Cancel Add and More Add and Finish

- The **Add ACE** page displays again and the Right Name field is empty. Type, **adminConsoleDLRights** and click **Add and More**
- Continue to add the following right names:
 - **adminConsoleAliasRights**
 - **adminConsoleResourceRights**
 - **adminConsoleSavedSearchRights**
 - **adminConsoleDomainRights**
- After the last right, click **Add and Finish**. The Configure the Grants dialog displays these rights associated with the target domain. If you are adding another domain to manage, click **Add and More**. Repeat Step 4. If not, click **Finish**.

Manage Distribution Lists

To assign a user to manage a distribution list, you create a distribution list and enable Admin Group, select the view, grant the distribution list rights, add the user to the list and make that user an administrator.

1. Create a new distribution list and include the following:
 - Check **Admin Group**

- Add the user who will be the administrator as a member of the DL.
- Go to the Admin Views tab and check **Distribution List View** so the admin can view the distribution list.
- Click **Save**.

2. In the Configure Grants page add the following rights.

Right Name	Target Type	Target	Right Type
The following right let the administrator manage distribution lists.			
listdistributionlist	dl	DL email address	SD Right
adddistributionlistalias	dl	DL email address	SD Right
adddistributionlistmember	dl	DL email address	SD Right
modifyDistributionlist	dl	DL email address	SD Right
getdistributionlistmembership	dl	DL email address	SD Right
RemoveDistributionlistmember	dl	DL email address	SD Right
This domain right displays user account list that the administrator can select from to add to a distribution list.			
listAccount	domain	DL email address	SD Right

Change Passwords

To create delegated administrators who only change passwords, you create the admin or admin group, select the views and grant the taskSetPassword combo right.

1. Select the following views
 - **Account List** view to be able to select accounts to change passwords
 - **Alias List** view to be able to find users who use an alias instead of account name.
2. The Configure the Grants page displays recommended grants for the views you have chosen. For Change Password rights, do not configure these grants. Select **Skip**. Click **Add** to add the following right:

Right Name	Target Type	Target	Right Type
taskSetPassword	domain	domain address	SD Right

View Mail Access Right

View Mail access right can be granted on accounts, domains, and distribution lists.

Right Name	Target Type	Target	Right Type
adminLoginAs	Either: account domain dl	account, domain, or distribution list address	SD Right*

*To deny the View Mail right on the target, check the box for **Is Negative Right (Deny)**

To prevent administrators from viewing an account with a domain or distribution list, assign the **Is Negative Right** to the account.

Manage Class of Service Assigned to Users

You can expand the domain administrator role to be able to view and change the class of service (COS) assigned to a user. To add the rights to manage the COS for a domain, add the following rights to the domain administrator account or domain administrator admin group.

Add the System Defined Rights to each COS in the domain.

Right Name	Target Type	Target	Right Type
listCos	cos	COS name	SD Right
getCos	cos	COS name	SD Right
assignCos	cos	COS name	SD Right
This domain right displays the COS information in the user account's General Information page.			
zimbraCOSId	domain	domain address	Attribute Right Verb: Write AR Target: domain

Manage Cross Mailbox Search

This role creates a delegated administrator role that can run the Search Mail tool to search mail archives or live mail for accounts. This also allows the administrator to create, abort, delete, purge or get status of a cross mailbox search request.

Note: The Archiving and Discovery feature must be installed for this feature to work.

Right Name	Target Type	Target	Right Type
adminConsoleCrossMailboxSearchRights	(combo)	server name where cross mailbox searches can be run	SD Right

For full functionality, this role includes the ability to create new accounts so that the admin can create the target mailbox to receive the search results. If you do not want this role to have the ability to create accounts, grant the following negative right as well.

Right Name	Target Type	Target	Right Type
CreateAccount	domain	domain address	SD Right*

*To deny the Create Account right on the target, check the box for **Is Negative Right (Deny)**

If you want this admin to also view the target mailbox with the results of the cross mailbox search, grant the right to view that mailbox only.

Right Name	Target Type	Target	Right Type
adminLoginAs	account	cross mailbox search target account name	SD Right*

Manage Zimlets

This role creates a delegated administrator role that can create, deploy and view Zimlets.

Right Name	Target Type	Target	Right Type
adminConsoleZimletRights	server domain	server name or domain address	SD Right
adminConsoleAccountsZimletsTabRights	server domain	server name or domain address	SD Right

Manage Resources

This role creates a delegated administrator that can create and manage resources.

Right Name	Target Type	Target	Right Type
adminConsoleResourceRights	combo	server name or domain address	SD Right

Access to the Saved Searches

This role creates a delegated administrator that can access all the searches saved in the administration console Navigation pane, Search section.

Right Name	Target Type	Target	Right Type
adminConsoleSavedSearchRights	combo	server name or domain address	SD Right

Access to the Server Status Pages

This role creates a delegated administrator that can access the Server Status page. In addition to granting this right, you must also select the Admin View, **Global Server Status View**.

Right Name	Target Type	Target	Right Type
adminConsoleServerStatusRights	global		SD Right

Chapter 10 Managing ZCS Configuration

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

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

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

Managing Global Configurations

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

Global settings that can be configured include:

- Defining the default domain
- Setting the number of results returned for GAL searches
- Setting how users view email attachments and what type of attachments are not allowed
- Configuring authentication process, setting the Relay MTA for external delivery, enabling DNS lookup and protocol checks
- Enabling Pop and IMAP and the port numbers

Note: *If IMAP/POP proxy is set up, making sure that the port numbers are configured correctly.*

- Set the spam check controls

- Set anti-virus options for messages received that may have a virus
- Configure Backup default directory and backup notification information
- Set the global HSM schedule for when messages should be moved to a secondary storage space
- View the current Zimbra license information, update the license if necessary and view the number of accounts created

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, they override the global settings.

General Global Settings

In the General tab configure the following:

- **Most results returned by GAL search field.** This sets a global ceiling for the number of GAL results returned from a user search. The default is 100 results per search.
- **Default domain.** The default domain displays. This is the domain that user logins are authenticated against.
- **Number of scheduled tasks that can run simultaneously.** This controls how many threads are used to process fetching content from remote data sources. The default is 20. If this is set too low, users do not get their mail from external sources pulled down often enough. If the thread is set too high, the server may be consumed with downloading this mail and not servicing "main" user requests.
- **Sleep time between subsequent mailbox purges.** The duration of time that the server should "rest" between purging mailboxes. By default, message purge is scheduled to run every 1 minute. See the Customizing Accounts chapter, section "Setting Email Retention Policy" on page 148.

Note: If the message purge schedule is set to 0, messages are not purged even if the mail, trash and spam message life time is set.

- **Maximum size of an uploaded file for Documents or Briefcase (kb).** This is the maximum size of a file that can be uploaded into Documents or Briefcase. **Note:** the maximum message size for an email message and attachments that can be sent is configured in the Global Settings MTA tab.

Global Settings to Block Mail Attachments

The **Attachments** tab can be configured with global rules for handling attachments to an email message. You can also set rules by COS and for individual accounts. 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.

You can also reject messages with certain types of files attached. You select which file types are unauthorized from the **Common extensions** list. You can also add other extension types to the list. Messages with those type of files attached are rejected. By default the recipient and the sender are notified that the message was blocked. If you do not want to send a notification to the recipient when messages are blocked, you can disable this option from the Global Settings>Attachments tab.

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 information about the Zimbra MTA, see [Chapter 5, Zimbra MTA](#).

- | | |
|-----------------------|--|
| Authentication | <ul style="list-style-type: none">• 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. |
| Network | <ul style="list-style-type: none">• 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.• If your MX records point to a spam-relay or any other external non-Zimbra server, enter the name of that server in the Inbound SMTP host name field. This check compares the domain MX setting against the <code>zimbraInboundSmtpHostname</code> setting, if set. If this attribute is not set, the domain MX setting is checked against <code>zimbraSmtpHostname</code>.• 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.• If Allow domain administrators to check MX records from Admin Console is checked, domain administrators can check the MX records for their domain. |

- | | |
|------------------------|--|
| Messages | <ul style="list-style-type: none"> • Set the Maximum messages size for a message and its attachments that can be sent. Note: To set the maximum size of an uploaded file to Documents or Briefcase, go to the General Information tab. • You can enable the X-Originating-IP header to messages checkbox. The X-Originating-IP header information specifies the original sending IP of the email message the server is forwarding. |
| Protocol checks | <ul style="list-style-type: none"> • The Protocol fields are checked to reject unsolicited commercial email (UCE), for spam control. |
| DNS checks | <ul style="list-style-type: none"> • The DNS fields are checked to reject mail if the client's IP address is unknown, the hostname in the greeting is unknown, 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 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 IMAP, users can access their mail from any computer as the mail is stored on the Zimbra server.

When you make changes to these settings, you must restart ZCS before the changes take effect.

Anti-spam Settings

ZCS utilizes SpamAssassin to control spam. SpamAssassin uses predefined rules as well as a Bayes database to score messages with a numerical range. ZCS uses a percentage value to determine spaminess based on a SpamAssassin score of 20 as 100%. Any message tagged between 33%-75% is considered spam and delivered to the user's Junk folder. Messages tagged above 75% are always considered spam and discarded.

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 48](#).

RBL (Real time black-hole lists) can be turned on or off in SpamAssassin from the Zimbra CLI. See the section [“To turn RBL on:” on page 51](#).

SpamAssassin's sa-update tool is included with SpamAssassin. This tool updates spamassassin rules from the SA organization. The tool is installed into /opt/zimbra/zimbramon/bin.

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.

Zimbra Free/Busy Interoperability

When ZCS is deployed in a mix of ZCS servers and Microsoft Exchange servers and Calendar is an important feature with your users, you can set up free/busy scheduling across the mix so that users can efficiently schedule meetings.

ZCS can query the free/busy schedules of users on Microsoft Exchange 2003/2007 servers and also can propagate the free/busy schedules of ZCS users to the Exchange servers.

To set free/busy interoperability, the Exchange systems must be set up as described in the Exchange Setup Requirements section, and the ZCS Global Config, Domain, COS and Account settings must be configured. The easiest way to configure ZCS is from the administration console.

Note: You can use the *zmprov CLI*. For more information about using *zmprov* to set this up, see the wiki article, [Free Busy Interop for Exchange](#).

Exchange 2003/2007 Setup Requirements.

For Exchange 2003, the following is required:

- Either a single Active Directory (AD) must be in the system or the global catalog must be available.
- The ZCS server must be able to access the HTTP(S) port of IIS on at least one of the Exchange servers.

- Web interface to Exchange public folders needs to be available via IIS. (<http://server/public/>)
- ZCS users must be provisioned as a contact on the AD using the same administrative group for each mail domain. This is required only for ZCS to Exchange free/busy replication.
- The Exchange user name must be provisioned in the account attribute **zimbraForeignPrincipal** for all ZCS users. This is required only for ZCS to Exchange free/busy replication.

Configuring Free/Busy on ZCS

To set Free/Busy Interoperability up from the administration console, configure the following:

- Either globally or by domain configure the Exchange server settings as described in Global Config Setup below.
- Add the **o** and **ou** values that are configured in the **legacyExchangeDN** attribute for Exchange in either the Global Config or Domain Interop tab or in the Class of Service (COS) Advanced tab. The **o** and **ou** values correspond to the ZCS domain attribute **zimbraFreebusyExchangeUserOrg**.
- In the Accounts Free/Busy Interop tab, configure the foreign principal for the account. The **cn** setting in the **legacyExchangeDn** attribute corresponds to the **zimbraForeignPrincipal** attribute. This sets up a mapping from the ZCS account to the corresponding object in the AD.

Note: To find these settings on the Exchange server, you can run the Exchange ADSI Edit tool and search the **legacyExchangeDN** attribute for the **o=** , **ou=** , and **cn=** settings.

Global Config Setup The ZCS Global Config Settings are configured from the Interop tab on the administration console. Here you configure the Exchange server settings as follows:

- Exchange Server URL. This is the Web interface to the Exchange.
- Exchange Authentication Scheme, either Basic or Form.
 - Basic is authentication to Exchange via HTTP basic authentication.
 - Form is authentication to Exchange as HTML form based authentication.
- Exchange user name and password. This is the name of the account in Active Directory and password that has access to the public folders. These are used to authenticate against the Exchange server on REST and WebDAV interfaces.
- The **O** and **OU** used in the **legacyExchangeDN** attribute. Set at the global level this applies to all accounts talking to Exchange.

Backup/Restore

Two distinct backup methods are available.

- The standard backup (default) method is to run a weekly full backup session and daily incremental backup sessions to backup all mailboxes daily.
- The auto-grouped backup method is recommended for large ZCS environments where running a full backup of all accounts at one time would take too long. The auto-grouped backup method runs a full backup session for a different group of mailboxes at each scheduled backup.

During ZCS install, by default, backups are scheduled to run daily. The target backup directory and the email notification address to receive backup session results are set up during ZCS installation. You can change the backup method and schedule from the administration console.

For information about backups and schedules see [Chapter 16, Backup and Restore](#)

Customizing Themes

You can change the logo and base colors of the Zimbra Web Client themes (skin) from the administration console without having to customize individual ZCS themes. Customized themes can be created as a global setting or as a domain setting. If you customize themes in both settings, the domain values are displayed for the domain.

This also changes the base colors for the administration console. Read the [Changing ZWC Theme Colors and Logo](#) chapter to understand what you can change and what attributes are modified.

Global HSM

Hierarchical Storage Management (HSM) is a process of moving older data to a secondary storage device, called the secondary message volume in ZCS. One message volume is configured on each mailbox server. This is the primary message volume. Additional secondary message volume can be configured for HSM.

To manage your disk utilization, implement a global HSM policy or a HSM policy for each mailbox server. The policy configured on individual servers overrides the policy configured as the global policy.

Email messages, documents stored in Documents or Briefcase, and the other items in the account are moved from the primary volume to the current secondary volume based on the HSM policy. The items are still accessible. Users are not aware of any change and do not see any noticeable differences when opening older items that have been moved.

The default global HSM policy moves messages and document files more than 30 days old to the secondary volume. You can also select to move tasks,

appointments, contacts, chats, and notes. The schedule for moving can be set for items older than a specified number of days, months, weeks, hours, minutes.

In addition to selecting different items to move, you can use the search query language to set up other HSM policies. For example:

- If you wanted all messages marked as junk to be included in messages moved to the current secondary volume, you would add the following to the policy: **message:in:junk before:-[x] days**.
- To move or consolidate messages from one volume to another

Note: *The search string can be added to the default policy or you can write a new policy.*

Sessions to move items to the secondary volume are scheduled in your cron table. You can manually start an HSM session from the Servers, Edit toolbar.

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 270 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.

Updating Your License

When you renew or change the Zimbra license, you update ZCS mailbox servers with the new license information. This can be done from either the administration console or using the **zmlicense** CLI command.

From the administration console:

1. Save the license on the computer you use to access the administration console.

2. Log on to the administration console, go to **Global Settings>License** tab and on the toolbar click **Update License**. The License Installation Wizard opens.
3. Browse to select the ZCS license file. Click **Next**. The license file is uploaded.
4. Click **Install** to install the license file.
5. To make the license effective on all mailbox servers in your environment, you must flush the cache on each mailbox server.
From the command line for each mailbox server type:

zmprov fc config.

Note: This step is not necessary if there is only one mailbox server in your environment.

Your license information is updated automatically. The cached account license count is automatically refreshed on each mailbox server.

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 following. These settings can be set from the admin console:

- Global Address List mode
- Authentication mode
- Virtual hosts for the domain to establish a default domain for a user login
- Public service host name that is used for REST URLs, commonly used in sharing.
- Domain Documents account if you are setting up Zimbra Documents.
- The maximum number of accounts that can be created on the domain
- Free/Busy Interop settings for use with Microsoft Exchange.

A domain can be renamed and all account, distribution list, alias and resource addresses are changed to the new domain name. The CLI utility is used to changing the domain name. See “Renaming a Domain” on page 114.

General Information

In this tab you configure the following:

- The default time zone for the domain. If a time zone is configured in a COS or for an account, the domain time zone setting is ignored.
- Public service host name. Enter the host name of the REST URL. This is commonly used for sharing. See “Setting up a Public Service Host Name” on page 109.

- Inbound SMTP host name. If your MX records point to a spam-relay or any other external non-zimbra server, enter the name of the server here.
- Default Class of Service (COS) for the domain. This COS is automatically assigned to accounts created on the domain if another COS is not set.
- Domain status. The domain status is active in the normal state. Users can log in and mail is delivered. Changing the status can affect the status for accounts on the domain also. The domain status is displayed on the Domain General tab. Domain status can be set as follows :
 - **Active.** Active is the normal status for domains. Accounts can be created and mail can be delivered. Note: If an account has a different status setting than the domain setting, the account status overrides the domain status.
 - **Closed.** When a domain status is marked as closed, Login for accounts on the domain is disabled and messages are bounced. The closed status overrides an individual account's status setting.
 - **Locked.** When a domain status is marked as locked, users cannot log in to check their email, but email is still delivered to the accounts. If an account's status setting is marked as maintenance or closed, the account's status overrides the domain status setting.
 - **Maintenance.** When the domain status is marked as maintenance, users cannot log in and their email is queued at the MTA. If an account's status setting is marked as closed, the account's status overrides the domain status setting.
 - **Suspended.** When the domain status is marked as suspended, users cannot log in, their email is queued at the MTA, and accounts and distribution lists cannot be created, deleted, or modified. If an account's status setting is marked as closed, the account's status overrides the domain status setting.

Setting up a Public Service Host Name

You can configure each domain with the public service host name to be used for REST URLs. This is the URL that is used when sharing Documents Notebooks, email folders and Briefcase folders, as well as sharing task lists, address books, and calendars.

When users share a ZCS folder, the default is to create the URL with the Zimbra server hostname and the Zimbra service host name. This is displayed as **http://server.domain.com/service/home/username/sharedfolder**. The attributes are generated as follows:

- Hostname is server.zimbraServiceHostname
- Protocol is determined from server.zimbraMailMode
- Port is computed from the protocol

When you configure a public service host name, this name is used instead of the server/service name, as **http://publicservicename.domain.com/home/username/sharedfolder**. The attributes to be used are:

- **zimbraPublicServiceHostname**
- **zimbraPublicServiceProtocol**
- **zimbraPublicServicePort**

You can use another FQDN as long as the name has a proper DNS entry to point at 'server' both internally and externally.

Global Address List (GAL) Mode

The Global Address List (GAL) is your company-wide listing of users that is available to all users of the email system. See [Chapter 4, Zimbra Directory Service](#).

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.). When you configure the external GAL mode, you can configure GAL search and GAL sync separately.
- **Both.** Internal and external directory servers are used for GAL lookups.

GAL sync accounts

When you configure an internal or external GAL, you create a GAL sync account with an address book where the LDAP contact data can be synced. Syncing the LDAP to this account gives users faster access to the GAL data and makes it easier for them to search the GAL.

If **Both** is selected, a GAL sync account with an address book is created for each LDAP data source. These accounts display in the administration console's Accounts list.

You enter the GAL datasource for each account. When a datasource is configured on an account, the GAL configuration on the domain is overridden.

The internal GAL polling interval for the GAL sync determines how often the GALsync account syncs with the LDAP server. The sync intervals can be in x days, hours, minutes, or seconds.

When the GAL sync account syncs to the LDAP, all GAL contacts from the LDAP are added to the GAL address book. During the sync, the GAL sync account is updated with new contact, modified contact and deleted contact information. You should not modify the GAL sync account address book

directly. When the LDAP syncs the GAL to the account, changes you make to the address book are deleted.

If the GALsync account is not available for some reason, the traditional LDAP based search is run.

See Appendix A Command-Line Utilities, the CLI **zmgsautil** for information about the GALsync CLI command.

Configuring GAL Search for External GALs

When you configure an external GAL, you can configure different search settings and sync settings. You may want to configure different search settings if your LDAP environment is set up to optimize LDAP searching by setting up an LDAP cache server, but users also will need to be able to sync to the 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 to use DN password to bind to the external server.
- **External Active Directory.** The user name and password is the authentication information supplied to the Active Directory server. You identify the Active Directory domain name and URL.

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

Virtual Hosts

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

Virtual hosts are entered on the **Domains>Virtual Hosts** tab on the administrator's console. The virtual host requires a valid DNS configuration with an A record. Not required for Virtual Hosts.

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 that includes the Document templates and the global notebook, one optional Documents account per domain, and individual accounts' Documents notebooks. The global Documents account is automatically created when ZCS is installed. The domain Documents account is not automatically created.

One Documents account can be created per domain. You can easily add the account from the administration console when you create a domain. When you create the account, you configure who can access this Documents account and what access rights these users can have.

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

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

Except for Public, which is view-only, you can select the access privileges these users can have: view, edit, remove, and add pages to the Documents notebook. You can view and change these access permissions from the administration console.

Free/Busy Interoperability

The Zimbra Free/Busy Module to connect with Microsoft Exchange pulls the free/busy schedule of users on Exchange and also pushes the free/busy schedule of ZCS users to the Exchange server. You complete the Interop tab for the domain to enable this feature for the domain. For more information see [“Zimbra Free/Busy Interoperability” on page 104](#).

You configure the following on the domain Interop tab:

- Exchange server URL. This is the Web interface to the Exchange public folders.
- Exchange authorization schema, either Basic or Form.
 - Basic is authentication to Exchange via HTTP basic authentication.

- Form is authentication to Exchange as HTML form based authentication.
- Exchange user name and password. This is the name of the account and password that has access to the public folders.

Note: *Domain settings overwrite Global settings.*

Zimlets on the Domain

Zimbra Collaboration Suite includes pre configured Zimlets, see Chapter 14, Working with Zimlets. These Zimlets are enabled in the default COS. Additional Zimlets can be added and enabled by COS or by account. All Zimlets that are deployed are displayed in the **Domain>Zimlets** tab. If you do not want all the deployed Zimlets made available for users on the domain, select from the list the Zimlets that are available for the domain. This overrides the Zimlet settings in the COS or for an account.

Customizing Themes for Domains

If you want the domain to have a customized theme different from the global setting, you can customize the base colors for the ZWC themes and change the logo that displays on specific domains from the domain's Themes tab. Read the [Changing ZWC Theme Colors and Logo](#) chapter to understand what you can change and what attributes are modified.

Note: *If global settings and domain-level settings for theme base colors or logos are not the same, the domain values are displayed for the domain.*

Setting Account Limits

You can limit the number of accounts that can be provisioned on a domain. The maximum number of accounts that can be provisioned for the domain can be set when the domain is created. You can also edit the domain configuration to add or change the number. In the administration console this is set in the Domain>Account Limits tab. If this tab is not configured, no limits on the domain are set.

Resources, domain wiki, spam, and ham accounts are not counted against this limit.

Note: *You cannot exceed the account limit set by the ZCS license.*

When multiple Classes of Service (COS) are available, you can select which classes of service can be configured and how many accounts on the domain can be assigned to the COS. This is configured in the Domain>Account Limits tab. The number of COS account types used is tracked. The limits for all COSs cannot exceed the number set for the maximum accounts for the domain.

The number of COS assigned to accounts is tracked. You can see the number assigned/number remaining from any account's General Information tab.

Renaming a Domain

When you rename a domain you are actually creating a new domain, moving all accounts to the new domain and deleting the old domain. All account, alias, distribution list, and resource addresses are changed to the new domain name. The LDAP is updated to reflect the changes.

How to Rename a Domain

Before you rename a domain

- Make sure MX records in DNS are created for the new domain name
- Make sure you have a functioning and current full backup of the domain

After the domain has been renamed

- Update external references that you have set up for the old domain name to the new domain name. This may include automatically generated emails that were sent to the administrator's mailbox such as backup session notifications
- Immediately run a full backup of the new domain

You rename the domain using the CLI utility **zmprov**. To rename a domain, type

```
zmprov -l rd [olddomain.com] [newdomain.com]
```

Domain Rename Process

When you run this **zmprov** command, the domain renaming process goes through the following steps:

1. The status of the old domain is changed to an internal status of shutdown, and mail status of the domain is changed to suspended. Users cannot login, their email is bounced by the MTA, and accounts, calendar resources and distribution lists cannot be created, deleted or modified.
2. The new domain is created with the status of shutdown and the mail status suspended.
3. Accounts, calendar resources, distribution lists, aliases, and resources are all copied to the new domain.
4. The LDAP is updated to reflect the new domain address.
5. The old domain is deleted.
6. The status for the new domain is changed to active. The new domain can start accepting email messages.

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 ZCS Installation program must be used to add new servers because the installer packages are designed to register the new host at the time of installation.

The server settings include:

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

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 Information tab includes the following configuration information:

- Server display name and a description field
- Server hostname
- LMTP information including advertised name, bind address, and number of threads that can simultaneously process data source imports. The default is 20 threads.
- Purge setting. The server manages the message purge schedule. You configure the duration of time that the server should “rest” between purging mailboxes from the administration console, Global settings or Server settings, General tabs. By default, message purge is scheduled to run every 1 minute.
- When installing a reverse proxy the communication between the proxy server and the backend mailbox server must be in plain text. Checking **This server is a reverse proxy lookup target** automatically sets the following:
 - zimbralmapCleartextLoginEnabled=TRUE

- `zimbraReverseProxyLookupTarget=TRUE`
- `zimbraPop3CleartextLoginEnabled=TRUE`

The Notes text box can be used to record details you want to save.

Services Settings

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

MTA Server Settings

The MTA tab shows the following settings:

- Authentication enabled. Enables SMTP client authentication, so users can authenticate. Only authenticated users or users from trusted networks are allowed to relay mail. TLS authentication when enabled, forces all SMTP auth to use Transaction Level Security (similar to SSL) to avoid passing passwords in the clear.
- Network settings, including Web mail MTA hostname, Web mail MTA timeout, the relay MTA for external delivery, MTA trusted networks ID, and the ability to enable 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

In the Volume tab you manage storage volumes on the 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.

Note: *If Compress Blobs is enabled (YES), the disk space used is decreased, but memory requirements for the server increases.*

Index Volume

Each Zimbra mailbox server is configured with one current index volume. Each mailbox is assigned to a permanent directory on the current index volume. You cannot change which volume the account is assigned.

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

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

Message Volume

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

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

Scheduling HSM Sessions

Sessions to move messages to the secondary volume are scheduled in your cron table. See “Global HSM” on page 106. From the administration console, when you select a server, you can manually start a HSM session, monitor HSM sessions, and abort HSM sessions that are in progress from the Volumes tab.

When you abort a session and then restart the process, the HSM session looks for entries in the primary store that meet the HSM age criteria. Any entries that were moved in the previous run would be excluded, as they would no longer exist in the primary store.

Backup and Restore - selecting the backup mode

Two distinct backup methods are available on ZCS.

- The **standard backup method** is to run a weekly full backup session and daily incremental backup sessions to back up all mailboxes daily. The standard backup method is appropriate for enterprise deployments where full backups are run during non-working days.
- The **auto-grouped backup method** is recommended for large ZCS environments where running a full backup of all accounts at one time would take too long. The auto-grouped backup method runs a full backup session for a different group of mailboxes at each scheduled backup. The system administrator configures the interval that backups should run and configures the number of groups that backups are made up of. ZCS then automatically backs up mailboxes in groups over the interval specified.

The standard backup method is the default. If you want to use the auto-grouped method, select that from the drop-down. See [Backup and Restore](#) for information about these two methods.

Managing Other Functions

Zimlets

Zimlets are applications that enhance the user experience from the Zimbra Web Client. Some Zimlets are automatically deployed when ZCS is installed and you can add new Zimlets and manage existing Zimlets from the Zimlets Configuration page on the administration console.

To see a list of Zimlets that are deployed, click Zimlets in the Configuration Overview pane. The Content pane lists all the Zimlets that are enabled or disabled. You can upload and deploy new Zimlets. Zimlets are delivered as a zip file that includes all the files necessary to run the Zimlet.

You can manage the Zimlets by domain, and you can configure COSs 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 11 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**
- Create many new accounts at once with the **Bulk Provisioning Wizard**
- View the date when an account was created
- 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
- Set the time zone for an account
- View an account's mailbox
- Change an account's status and delete accounts
- Move a mailbox to another server
- Reindex a mailbox

See the Zimbra 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** command can be used to add, modify, and view accounts, aliases, distribution lists, and Calendar resources. Most of the zmprov functions are available from the administration console.
- 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.

- The CLI **zmaccts** 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.
- The CLI **zmailboxmove** 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.

See [“Zimbra CLI Commands” on page 228](#) for information about how to use these commands.

Setting up and Configuring Accounts

You can configure one account at a time with the New Account Wizard or you can create many accounts at once using the Bulk Provisioning Wizard.

Configuring One Account

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

- General information, including account name, Class of Service (COS) to be assigned, and password
- Contact information, including phone number, company name, and address
- Language preference to display Zimbra Web Client
- Default time zone
- 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
- Themes and Zimlets that the user can access
- Advanced settings including attachment settings, quotas, quota warning flag, and password log in policies

For a description of the features see [Chapter 12, Customizing Accounts, Setting General Preferences and Password Rules](#).

If the COS you assign is configured with the correct functionality for the account, you do not need to configure features, preferences, themes, zimlets, or advanced settings.

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.

Configuring Many Accounts at Once

You can provision up to 500 accounts on once using the Bulk Account Wizard from the administration console. The wizard takes you through the steps to upload a .csv file with the account information and then provisions the user accounts. These accounts are configured with a user name, display name and password (optional). The accounts are automatically assigned the domain default COS.

You create a .csv file with the account information. Each row in the file is an account entry. The account information is configured as

Column 1	Column 2	Column 3
AccountName@example.com	Display Name	Password (optional)

The account name cannot have spaces or use symbols. You can type a period (.) between words. For example: john.smith@example.com.

The password is optional. If you do not provide a password, a random password is generated for the account. When users log in the first time, they are prompted to change the password.

If you do not add the password to the .csv file, the comma after the display name field must be included. For example, **user1@example.com,Jane Brown,**

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.

You can view and edit an account's alias names from the account view.

Class of Service

Class of Service (COS) determines what default attributes an account has and which features are enabled or denied. The COS controls features, mailbox quotas, message lifetime, password restrictions, which Zimlets and Themes are available from ZWC, attachment blocking, and server pools for creation of new accounts.

A default COS is automatically created during the installation of Zimbra Collaboration Suite. A COS is global and does not need to be restricted to a particular domain or set of domains. You can modify the default COS to set the attributes to your email restrictions, and you can create multiple COSs.

Each account is assigned one COS. You can create a domain COS and have all accounts created on that domain automatically assigned this COS. You can create numerous COSs and specify which COS(s) are available for a domain. If the domain does not have a COS defined, the default COS is automatically assigned when an account is created.

Note: *If you delete a COS that accounts are currently assigned, the accounts are 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 from the Zimbra Web Client in the user's Preferences.
- Attachment blocking set as a global setting can override the COS setting.

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

Setting Default Time Zones. The default time zone setting that is displayed in the account's Preferences folder is used to localize the time for received messages and calendar activities in the standard Web client. When using the standard Web client, the time zone on the computer is not used to set the time a message is received or for calendar activities. The time zone setting in the Preferences>General tab is. When using the advanced Web client, the time

zone setting on the computer is used as the time stamp for received messages and for calendar activities, not the time zone setting on the General tab.

Because the advanced Web client and the standard Web client do not use the same time zone source to render messages, you may notice that the same message has a different time when displayed in one or the other client. You can avoid this by having the computer time zone and the Web client time zone set to the same time.

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 Passwords

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.

Directing Users to Your Change Password Page

If your ZWC authentication is configured as external auth, you can configure ZCS to direct users to your password change page when users change their passwords. You can either set this URL as a global setting or a per domain setting.

Set the **zimbraChangePasswordURL** attribute to the URL of your password change page. The **Change Password** link in the Preferences>General tab goes to this URL and when passwords expire, users are sent to this page.

This is changed from the zmprov CLI.

```
zmprov md exampledomain.com zimbraChangePasswordURL http://  
www.mysite.com
```

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. When you are in an account, you can mouse over or right click on a folder to see the number of messages in the folder and the size of the folder. 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.

Reindexing 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.

Text searches on an account might or might not fail with errors when the index is corrupt. You cannot count on a user reporting a failed text search to identify that the index is corrupt. You must monitor the index log for messages about corrupt indexes. If the server detects a corrupt index, a message is logged to the Zimbra mailbox.log at the WARN logging level. The message starts with **Possibly corrupt index**. When this message is displayed, the administrator must correct the problem. In many cases correcting the problem may mean reindexing the mailbox.

Reindexing a mailbox's content can take some time, depending on the number of messages in the mailbox. Users can still access their mailbox while reindexing 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.

- **Pending.** Pending is a status that can be assigned when a new account is created and not yet ready to become active. The login is disabled and messages are bounced.
- **Locked.** When a mailbox status is locked, the user cannot log in, but mail is still delivered to the account. The locked

Global configuration options for moving a mailbox can be set to exclude search indexes, blobs, and HSM blobs when mailboxes are moved. The following configuration options can be set on either the exporting server or the destination server:

- **zimbraMailboxMoveSkipSearchIndex.** If you do not include the search index data, the mailbox will have to be reindexed after the move.
- **zimbraMailboxMoveSkipBlobs.** Blobs associated with the mailbox, including primary and secondary volumes (HSM) are excluded.
- **zimbraMailboxMoveSkipHsmBlobs.** This is useful when HSM blobs for the mailbox being moved already exists. Set this if `zimbraMailboxMoveSkipBlobs` is not set, but you want to skip blobs on HSM volumes.

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.

Moving a Mailbox using the CLI command

To move a mailbox to a new server using the CLI command, 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 the message 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.

The maximum number of members in a distribution list is 1000 recipients. The 1000 recipients include addresses in distribution lists that are nested within a distribution list. Senders do not receive an error when they send a message to a distribution list with more than 1000 members, but the message is not sent to more than 1000 recipients.

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

Instead of creating individual share requests, distribution lists can be created to share items with a group. Users notify the administrator that they have shared an item with the distribution list and the administrator publishes the shared item to the list. This is done in the Shares tab. When a new shared item is published, existing members of the list are automatically notified of the new share.

Everyone in the DL has the same share privileges that the grantee defines for the shared item.

When new members are added to the group distribution list, they are automatically granted the same shared privileges as other members of the group. You can set up the Share tab so that new members are automatically notified about items that are shared with them through the list.

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.

Create Distribution List Aliases

A distribution list can have an alias. This is set up from the administration console, Distribution List Alias tab.

Managing Resources

A resource is a location or equipment that can be scheduled for a meeting. Each meeting room location and other non-location specific resources such as AV equipment is set up as a resource account. The Addresses > Resources section in the administration console shows all resources that are configured for ZCS.

User accounts with the Calendar feature can select these resources for their meetings. The resource accounts automatically accept or reject invitations based on availability.

Administrators do not need to monitor these mailboxes on a regular basis. The contents of the resource mailboxes are purged according to the mail purge policies.

A Resource Wizard on the administration console guides you through the resource configuration. You can configure the account with the following details about the resource:

- Type of resource, either location or equipment

- Scheduling policy
- Forwarding address to receive a copy of the invite
- Description of the resource
- Contact information. This can be a person to contact if there are issues.
- Location information, including room name, specific building location including building and address, and room capacity

When you create a resource account, a directory account is created in the LDAP server.

To schedule a resource, users invite the equipment resource and/or location to a meeting. When they select the resource, they can view the description of the resource, contact information and free/busy status for the resource, if these are set up.

When the meeting invite is sent, an email is sent to the resource account, and, based on the scheduling policy, if the resource is free the meeting is automatically entered in the resource's calendar and the resource is shown as Busy.

Setting up the Scheduling Policy

The scheduling policy establishes how the resource's calendar is maintained. The following resource scheduling values can be set up:

- **Auto decline all recurring appointments.** This value is enabled when the resource can be scheduled for only one meeting at a time. No recurring appointments can be scheduled for this resource.
- **Auto accept if available, auto-decline on conflict.** When this option is selected, the resource account automatically accepts appointments unless the resource is already scheduled. The free/busy times can be viewed. You can modify the auto-decline rule to accept some meetings that conflict
- **Manual accept, auto decline on conflict.** When this option is selected, the resource account automatically declines all appointments that conflict. Appointment requests that do not conflict are marked as tentative in the resource calendar and must be manually accepted. If you set this up, configure the forwarding address so a copy of the invite is sent to the account that can manually accept the invitation. You can modify the auto-decline rule to accept some meetings that conflict.
- **Auto accept always.** The resource account automatically accepts all appointments that are scheduled. In this case, free/busy information is not maintained, thus more than one meeting could schedule the resource at the same time. Because the resource always accepts the invitation, the suggested use for this policy would be for a frequently used location off premises that you want the location address to be included in the invite to attendees.

- **No auto accept or decline.** The resource account is manually managed. A delegated user must log into the resource account and accept or decline all requests.

Conflict Rules. For accounts that include the auto decline on conflict value, you can set up a threshold, either as a number of conflicts or as a percentage of all the recurring appointments to partially accept recurring appointments.

Maximum allowed number of conflicts and/or **Maximum allowed percent of conflicts** are configured to allow a recurring resource to be scheduled even if it is not available for all the requested recurring appointment dates. The resource accepts appointments even if there are conflicts until either the number of conflicts reaches the maximum allowed or the maximum percentage of conflicts allowed. If you set both fields, the resource declines appointments whenever either of the conditions is met.

Managing Resource Accounts

The Resource Accounts Preference>Calendar tab can be configured to let users manage the Resource's Calendar. You can configure the following options to manage the resource.

- An address to forward invites. If the forwarding address was set up when the account was provisioned, you can change the address
- Who can use this resource. In the Permissions section, Invites, select **Allow only the following internal users to invite me to meetings** and add the appropriate users' email addresses to the list.

To fully manage a resource account's calendar, you can share the resource calendar with a user who is given the Manager rights. Users delegated as Manager have full administrative rights for that calendar. They can view, edit, add, remove, accept or decline the invites.

Searching for Addresses

The Search bar offers three search options:

- Search
- Help Search
- Advanced Search



The Search field can be used to quickly find specific accounts, aliases, distribution lists, resources and domains.

Help Search is a powerful unified search to find answers to common questions. When you click Help Search, the Zimbra wiki, forums, and documents are searched. The results are displayed in a new window with links to the information.

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 Advanced Attributes pane can be configured to search for the last login time in a date range or for account that have never logged in.

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 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.

In the Navigation pane, the Searches section includes predefined search queries. Click on the search and the results are immediately displayed in the Content pane. You can search for inactive accounts, locked out accounts, and accounts by status.

You can save the results of your search and download it as a .csv file. The information in the .csv file includes the account name, the user ID number, the type of address, the display name and the status of the account. The COS is listed if it is not the default.

When you create a query in either Search or Advanced Search, you can save the search. Click the small disk icon after Help Search. You give the search a name and it is saved to our Search section in the Navigation pane.

Chapter 12 Customizing Accounts, Setting General Preferences and Password Rules

When an account is provisioned, you create the mailbox, assign the primary account email address, and enable ZCS 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 Web Client Versions

Zimbra offers a standard and an advanced Zimbra Web Client that users can log into. Both Web Clients include mail, calendar, address book and task functionality. Users can select the client to use when they log in.

- Advanced Web Client includes Ajax capability and offers a full set of Web collaboration features, including Documents and Briefcase and the ability to export your account information. This Web client works best with newer browsers and fast internet connections.
- Standard Web Client is a good option when Internet connections are slow or users prefer HTML-based messaging for navigating within their mailbox.

The default ZWC for login is the advanced Zimbra Web Client. When users log in, they view the advanced Zimbra Web Client, unless they use the menu on the login screen to change to the standard version. However, if ZWC detects the screen resolution to be 800 x 600, users are automatically redirected to the standard Web Client. Users can still choose the advanced ZWC but get a warning message suggesting the use of the standard ZWC for better screen view. The default version can be changed in the COS Preferences tab and users can change their preferences.

Zimbra Messaging and Collaboration Applications

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

- Email messaging
- Calendaring
- Address Books
- Tasks
- Documents for Web document authoring
- Briefcase to save files that can be access from the mailbox
- Instant Messenger (Beta)

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

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

Email messaging

ZCS 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 users' account Preferences tab when they log on to the Zimbra Web Client.

The default is to let users manage their preferences. If you do not want users to be able to change their account preferences, you can remove the check from the Major Features Preferences in the Features tab.

Feature Name	Description	COS/ Account Tabs
Mail	Enables the email application. This is enabled by default.	Features

Conversations	<p>Messages can be displayed grouped into conversations or as a message list. Conversations group messages by subject. If this feature is enabled, conversation view is the default, but you can change the default on the COS Preferences tab.</p> <p>Users can change the default from the Mail toolbar, View link.</p>	Feature
HTML compose	<p>Users can compose email messages with an HTML editor. They can specify their default font settings for HTML compose in their account Preferences tab.</p>	Features
Enable attachment indexing	<p>Attachments to email messages are indexed. If attachments are indexed, they can be searched.</p>	Advanced
Allow the user to specify a forwarding address	<p>Users can create a forwarding address for their mail. When this feature is enabled in the COS, in the account configuration, you can specify a default forwarding address that the user can use and enable the function so that a copy of the forwarded message is not saved in the user's mailbox. Users can change the information from their account Preferences tab.</p> <p>In the account configuration, you can also specify forwarding addresses that are hidden from the user. A copy of each message sent to the account is immediately forwarded to the designated forwarding address.</p>	<p>Features tab in COS</p> <p>Forwarding tab in Accounts</p>

Out of office reply	<p>Users can create an email message that automatically replies to incoming messages. This is commonly used as a vacation message. By default message is sent to each recipient only once every seven days, regardless of how many messages that person sends to the address during that week. This can be changed in the COS Preferences tab, Out of office cache lifetime field.</p> <p>Users can also set the start and stop dates for the message. You can change this setting in the COS or Account setup.</p>	Features Preferences
New mail notification	<p>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 Preferences tab.</p> <p>An email with information about the email's subject, sender address and recipient address is sent to the address.</p> <p>Note: See “zmprov (Provisioning)” on page 232 in Appendix A CLI commands, for information about how to change the email template.</p>	Features tab in COS Preferences tab in Accounts
Persona	<p>The name and address configured for the account creates the primary account persona. This is the information that user use as the From address.</p> <p>When Persona is enabled, users can create additional account names to manage different roles. Account aliases can be selected for the From name of messages sent from that persona account and a specific signature can be set for the persona account.</p> <p>The number of personas that can be created is set to 20. You can change this from the CLI zmprov mc zimbraIdentityMaxNumEntries</p>	Features

Maximum length of mail signature	<p>You can set the maximum number of characters that can be in a signature. The default is 1024 characters.</p> <p>Users can create signatures for different roles. The number of signatures users can create is configured in zimbraSignatureMaxNumEntries</p>	Preferences
Advanced Search	Allows users to 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
Initial search preference	The initial search folder is Inbox. When this is enabled, users can set another folder as the default search folder.	Preferences
External POP access	Users can set up to retrieve their POP accounts' email messages directly from their ZWC account. They can add the external account address to their account settings. Users can set these up from their Preferences tab.	Features
External IMAP Access	Users can set up to retrieve their IMAP accounts' email messages directly from their ZWC account. They can add the external account address to their account settings. Users can set these up from their Preferences tab.	Feature
Aliases for this account	You can create an aliases for the account. Users cannot change this.	Alias tab in Accounts

Mail filters	<p>Users can define a set of rules and corresponding actions to apply to incoming mail and calendar appointments. 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 Preferences tab.</p> <p>Note: <i>Spam check on a received message is completed before users' mail filters are run. Messages identified as spam are moved to the Junk folder. To avoid having mail incorrectly marked as junk, users can create a spam white list from the Preferences Mail folder to identify email addresses that should not be marked as spam.</i></p>	Features
Mail filters	<p>Note: <i>To do this, type</i> zmpov ma <account@example.com> +amavisWhiteListSender <name@example.com> +amavisWhiteListSender <name2@example2.com></p>	Features
Tagging	<p>Users can create tags and assign them to messages, contacts, and Documents pages.</p>	Feature
Enable keyboard aliases	<p>Users can use keyboard shortcuts within their mailbox.</p> <p>The shortcut list can be printed from the Preferences Shortcuts folder.</p>	Preferences
GAL access	<p>Users can access the company directory to find names for their email messages.</p>	Features
Autocomplete from GAL	<p>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 Preferences tab.</p>	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 Preferences Mail tab.

- How often, in minutes, that the Web Client checks for new messages, **Check for new mail every...**
- Set or change email message alerts. Alerts can be set up to play a sound, highlight the Mail tab when a message arrives, and flash the browser.
- Set the display language for ZWC. If more than one language locale is installed on ZCS, users can select the locale that is different from the browser language settings.
- 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
- Whether to send a read receipt when it is requested.

Users can set up their own Junk Mail Options of white list and blacklist email addresses that is used to filter incoming message from their Preferences Mail folder. The default maximum number of white list and black list addresses is 100 on each list. This value can be changed using CLI `zmprov` for accounts and COS. The attributes are **zimbraMailWhitelistMaxNumEntries** and **zimbraMailBlacklistMaxNumEntries**.

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

Users can modify the following mail preferences from their Preferences Signatures tab.

- Whether to automatically append a signature to outgoing messages.

- Preferences for how messages that are replied to or forwarded are composed.

Import/Export Folder In the advanced Web Client, the Preference, Import/Export folder can be used to export a user's account data, including email messages and attachments, contacts, calendar, tasks, etc. This data can be saved to their computer or other location as a backup. The account data is saved as a tar-gzipped (tgz) archive file so that it can be imported to restore the user's account. When they run the export command, the data are copied, not removed from the user's account.

You can turn the Import/Export feature off from the COS or Account Features tab, General Features section.

Address Book

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

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

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

Feature Name	Description	COS/ Account Tabs
Address Book	Users can create their own personal contacts lists. By default, two contact lists folders are in the Address Book.	Features
Address book size limit	Maximum number of contacts a user can have in all address books. 0 means unlimited.	Advanced

Users can modify the following Address Book preferences from their account Preferences 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.

Users can import other contact lists into their Address Book and can export their address books as well. The files must be .csv files. This is done from the Preferences Import/Export folder

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. They can also use search for appointments in their calendars.

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

Feature Name	Description	COS/ Account Tabs
Calendar	A calendar and scheduling tool to let users maintain their calendar, schedule meetings, delegate access to their calendar, create multiple personal calendars, and more.	Features
Group Calendar	When Group Calendar is not checked, the only Calendar feature is the ability to create personal appointments and accept invitations to meetings. The Find Attendees, Schedule and Find Resources tabs are not displayed.	Features
Nested Calendars	Calendars can be nested within ZCS folders like Mail, Contact, and Calendar folders. The administrator creates a nested list of calendars using CLI or a nested calendar grouping is imported through migration. The CLI command to define the grouping is zmmailbox -z -m user1 cf -V appointment /<Calendar Name>/ <sub-calendar name>. This creates a calendar nested under the Calendar Name folder.	

Timezone	Sets the timezone that is used for scheduling in the Calendar application. A drop down displays the timezone list. Domain admins set this in the Accounts, General Information tab.	Preferences
Forward calendar invitation to specific addresses	You can specify email addresses to forward a user's calendar invitations. Users can also specify forwarding address from the Preferences Calendar folder. The account the invitation is forwarded to must have been granted admin privileges on the shared calendar to be able to reply to the invitation.	Accounts Forwarding

Troubleshooting Calendar Appointment Issues The CLI **zmcalthk** command is used to check for discrepancy between different users' calendars for the same meeting and send an email notification regarding the discrepancies.

You can also use this command to notify the organizer and/or all attendees when an appointment is out of sync. See Appendix A, "zmcalthk" on page 250.

Setting Remote Calendar Automatic Update Interval

Remote calendars are automatically updated every 12 hours by default. You can change the frequency of these updates with this CLI:

```
zmprov mc zimbraDataSourceCalendarPollingInterval <hr>
```

Filtering Calendar Messages

Users can set up mail filter rules that act on Calendar- related messages. The filter subject is **Calendar Invite**. When they select this subject, messages that are marked as invites are run through the filter.

Other User Calendar Preferences

Users can modify the following Calendar preferences from their account Preferences Calendar folder. 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, List, or Schedule.
- First day of the week to display in the calendar.
- View calendars as a nested group within different folders.

- 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 and select how to be notified, sound, flash the browser title, and popup notification. If popup notification is selected, the user must have Yahoo! BrowserPlus™ installed.
- Set permissions for free/busy and who can invite the user to a meeting.
- Users can import and export their appointments in the standard iCalendar (.ics) format. This is done from the Preferences Import/Export folder.
- Set the preference to use the iCal delegation model for shared calendars for CalDav interface.
- Enable the ability to automatically add invites with PUBLISH method.
- Be notified of changes made to an appointment by a delegated access grantee.

Tasks

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

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

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

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

Documents

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

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

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

You can also create a specific domain Documents account from the administration console. This Documents notebook can be shared with users on the domain, users on all Zimbra domains in your environment, as well as individuals and groups. See Managing ZCS Configurations, [“Documents” on page 112](#).

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

Briefcase

Zimbra Documents lets user upload files from their computer to their Zimbra Web Client account and they can access these files whenever they log into the advanced Zimbra Web Client.

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

Feature Name	Description	COS/ Account Tabs
Briefcase	<p>Users can upload files to their Zimbra Web Client account. They can open the file if the application is available on the computer, send the file in an email, organize files into different briefcase folders.</p> <p>In 6.0.X, Briefcase beta features New Document, New Spreadsheet and New Presentation are enabled by default. You can disable these features in COS or Accounts Feature tabs, Briefcase Features section.</p>	Features

Instant Messaging (Beta)

Zimbra Instant Messaging lets users communicate in real-time with others whom they have identified in their Buddy list.

Feature Name	Description	COS/ Account Tabs
Instant Messaging	Users can create a Buddy list and communicate real-time with member of the list. With IM, users can create instant messages or create a group chat to message between several people for real-time collaboration.	Features
Instant Notification	When this enabled, users immediately receive notification of IM messages, new email messages, and calendar and folder updates. This is disabled by default. Users can change this preference in their IM tab.	Features

Other Configuration Settings for Accounts

Other configuration options include:

- Enabling the Sharing feature that allows users to share items with other users

- Disabling Options (Preferences) for user accounts
- Setting the quota for accounts
- Setting the password policy and failed logon policy
- Setting account session length
- Enabling View Attachments settings
- Selecting ZWC UI theme to display
- Enabling Zimlets for accounts
- Disabling the user preferences for Import/Export.
- Specifying default behavior the appearance of a warning message when navigating from ZWC and the appearance of check boxes for items listed on the Content page for email and contacts

In addition, you can enable Zimbra Mobile for users to access their accounts from their mobile devices. See [“Zimbra Mobile” on page 150](#)

Enabling Sharing

When the Sharing feature is enabled, users can share any of their folders, including their mail folders, calendars, address books, task lists, Document notebooks and Briefcase folders.

Users specify the type of access permissions to give the grantee. They can share with internal users who can be given complete manager access to the folder, external guests that must use a password to view the folder content, and the public access so that anyone who has the URL can view the content of the folder.

When internal users share a mail folder, a copy of the shared folder is put in the grantee's folder list on the Overview pane. Users can manage their shared folders from their ZWC Preferences Sharing folder. In this folder users see a list of folders that have been shared with them and folders that they have shared with others.

Managing Shared Items using Distribution Lists

When distribution lists are used to manage shared items, members of the distribution list are automatically granted rights to the shared item. Administrators manage the shares from the DL's Shares tab. All members of the list have the same share privileges that the grantee defined for the shared folder. When a member is removed from the distribution list, the share privileges associated with the DL are revoked.

Users must notify the administrator that they have shared a folder with the distribution list. When the administrator is notified, the administrator publishes the shared item in the Shares tab to make the shared item available to members of the DL. When a new shared folder is published, existing members of the DL are automatically notified of the new shared item.

New members added to the distribution list can be automatically notified about items that are shared with them. They can accept the shared item from their ZWC Preferences>Sharing tab.

Disabling Preferences

Preferences is enabled by default. Users can modify the default preferences that are configured for their account. You can disable Options and users will not have the Preferences tab in their mailbox. They will not be able to change the default configuration for the features that are set up for their accounts.

Setting Account Quotas

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

Account quota is the amount of space in megabytes that an account can use. The quota includes email messages, Calendar meeting information, task lists, Documents pages and files in Briefcase. When the quota is reached, all email messages are rejected and users cannot add files to their account. If you set the quota to 0, accounts do not have a quota. See “Account Quota and the MTA” on page 48

You can view mailbox quotas from the administration console, Monitoring, Server Statistics.

Users can be notified that their mailboxes are nearing their quota. The percentage threshold for quota notification can be configured. When this threshold is reached, a quota warning message is sent to the user. The quota percentage can be set and the warning message text can be modified in the Advanced tab settings for COS and Accounts.

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 Zimbra.*

The password settings that can be configured are listed below.

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

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
Admin console auth token lifetime	Auth token lifetime sets a browser cookie that contains the auth token. Administrators can open the administration console without having to log on again until the auth token expires. The default is 12 hours.	Advanced
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. When it expires, the log in page is displayed and the user must log in to continue.	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

You can manually expire a user's web client session from the administration console Expire Sessions link. This forces the current session of the account to expire immediately.

Setting Email Retention Policy

The email retention policy for email, trashed and spam messages is set by COS. When the message purge function runs is set by the message purge command.

Feature Name	Description	COS/ Account Tabs
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. The minimum configuration for email message lifetime is 30 days.	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

The server manages the message purge schedule. You configure the duration of time that the server should “rest” between purging mailboxes from the administration console, Global settings or Server settings, General tabs. By default, message purge is scheduled to run every 1 minute.

For example, when the purge interval is set to 1 minute, after mailbox1 is purged of messages that meet the message lifetime setting, the server waits 1 minute before beginning to purge mailbox2.

If the message purge schedule is set to 0, messages are not purged even if the mail, trash and spam message life time is set.

Note: Because users cannot see these message lifetime settings, if you set a purge limit, make the purge policy known to your users.

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 can be viewed in HTML only.	Attachments received in another format are opened in HTML view	Advanced
Attachments can 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 can 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. When this is enabled. The default mobile device policy is also enabled.	Zimbra Mobile
---------------	--	---------------

See the [Zimbra Mobile](#) chapter for information about setting up mobile devices and setting up or changing the mobile device policies that can be enabled.

Configuring Zimlets for Accounts

Zimlets™ is a mechanism for integrating and extending the functionality of the Zimbra Collaboration Suite with third party information systems and content.

Zimlets that are deployed on the ZCS servers are listed in the administration console Configuration>Zimlets section. Zimlets can be deployed and undeployed from here. See [Chapter 14, Working with Zimlets](#) for how to install and deploy Zimlets.

When a Zimlet is deployed, it is immediately available to everyone in the default COS. If a Zimlet is not deployed to another COS directly, the COS displays the Zimlets but they are not enabled.

You can set access privileges to Zimlets by COS, by account, and by domain.

The Zimlet tab displays all Zimlets that are deployed and shows the status of the Zimlet:

- **Enabled.** All Zimlets that are deployed are enabled. Users can disable a Zimlet from their account's Preferences>Zimlet page.
- **Mandatory.** If you want a Zimlet to always be enabled in users' accounts, select **mandatory**. Users do not see these Zimlets on their Zimlet page.
- **Disabled.** If you do not want a Zimlet immediately available to users in this COS, you can disable the Zimlet. Users can enable a Zimlet from their account's Preferences>Zimlet page.

ZCS includes pre configured Zimlets that enhance the user experience while working in the Zimbra Web Client. These Zimlets are already deployed and enabled in the default 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.** This makes a link to the URL mentioned in the message.

- **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.

Other Account Configuration Preferences

The following preferences can be set up:

- **Display a warning when users try to navigate away from Zimbra.** It is easy for users to click the Back and Forward arrows in the browser or close their browser without logging out of their account. If this preference is not checked, users are asked if confirm that they want to navigate away from there account. If this preference is checked, the question is not asked.
- **Show selection checkbox for selecting email and contact items in a list view for batch operation.** If this is enabled, when users view email messages or contacts in the Content pane, a check box displays for each item. Users can select items from the Content pane and then perform an action such as mark as read/unread, move to a specific folder, drag and drop to a folder, delete, and tag for all those selected items. A checkbox in the toolbar

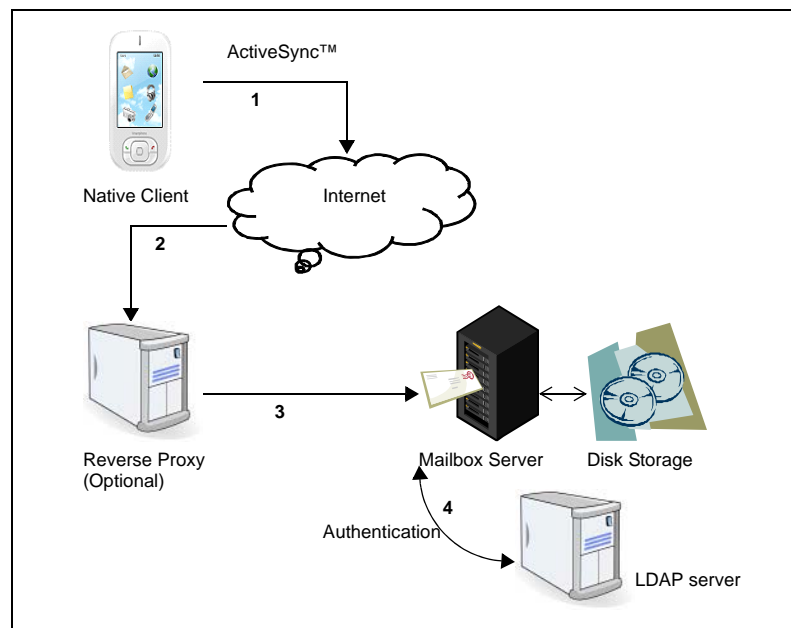
Chapter 13 Zimbra Mobile

Zimbra Mobile is the Zimbra synchronization program enabled on the ZCS mailbox server that provides over-the-air synchronization of mail, contacts, calendar and task data and device security policy enforcement between the mobile device and an account on the ZCS mailbox server.

Devices use the native software and UI that is installed on the device to sync. Zimbra Mobile is compatible with iPhone, iPod Touch, Windows Mobile 5 (WM5), and 6 (WM6) devices, and many other phones that support the Active Sync protocol.

The ActiveSync™ protocol is used to configure and sync the Zimbra mailbox server with the native client that is used on a user's device.

The following diagram shows the flow of data from the server to the mobile.



The diagram shows how the native mobile device application software syncs with the Zimbra mailbox server using ActiveSync™.

7. The user's client connects to the Internet using the ActiveSync™ protocol for syncing with the Zimbra mailbox server. Users configure the following information:
 - a. The Zimbra mailbox server address
 - b. The user's username as configured on the account
 - c. The user's Zimbra mailbox domain name
2. The protocol goes through the reverse proxy if it is present in the path.
3. The client then connects to the user's ZCS account on the mailbox server.
4. The mailbox server accesses the LDAP server to verify and authenticate the user's credentials before allowing a connection.

Setting Up Mobile Devices

ZCS mobile sync is enabled either in the COS for the account or enabled on individual accounts. In most cases, no additional plug-ins are required to be able to use the Zimbra Mobile feature.

The following may need to be configured in the mobile device:

- Server name (address). Enter the fully qualified hostname of the user's ZCS mailbox server.
- User name. Enter the user's primary ZCS account name.
- Domain. Enter the user's ZCS domain name (DNS).
- SSL certificate from the server may have to be added to the device as trusted if SSL is used when the cert is self-signed.

Users can immediately sync their account to their mobile device when this is configured. They can send email, create appointments, and add contacts to their address book.

For details about specific device setup, see the Mobile Device Setup pages on the Zimbra Wiki.

http://wiki.zimbra.com/index.php?title=Mobile_Device_Setup

<http://wiki.zimbra.com/index.php?title=IPhone>

Setting up Mobile Device Security Policies

The administrator can configure mobile security policies that enforce security rules on compliant mobile devices that sync with ZCS accounts. You can enforce general security policies including password rules and set up local wipe capability on compliant devices.

Note: Only WM6 devices and iPhones support security policies set by the server. Older devices do not respond to security policies.

Setting up a mobile policy can be either by COS or for an individual account and is configured from the administration console.

After the mobile policy is set up, the next time a mobile device sends a request to the server, mobile devices that are capable of enforcing security policies automatically set up the rules and immediately enforces them.

This typically means that if a Personal Identification Number (PIN) has not been set up on the device or the PIN is not as strong as required by the mobile policy you set up, the user is required to fix the PIN before they can sync with the server. Once the server confirms that the policy is enforced on the mobile device, the device can sync.

If a mobile device is lost or stolen the device is protected by the following policy rules:

- When the **Idle Time before device is locked** is configured, after the number of minutes configured, the device is locked. To unlock the device, users must enter their PIN.
- When the **Number of consecutive incorrect PIN inputs before device is wiped** is configured, after the PIN is entered incorrectly more than the specified number of times, a locally (generated by the device) initiated wipe of the device is performed. This erases all data on the device.

In addition to the rules, Remote Wipe can be used to erase all data on lost or stolen devices. See the Users' Mobile Device Self Care Features section.

Setting Mobile Device Policies Attributes

The following attributes can be configured to establish rules for PIN and device lockout and local wipe initiation rules.

Allow non-provisionable devices	
Allow partial policy enforcement on device	Devices that are capable of enforcing only parts of the mobile security policy can still be used. For example, the policy requires an alphanumeric PIN, but a device that only supports numbered PIN could still be used.
Force PIN on device	Force the user to create a personal identification number on the mobile device.
Require alpha-numeric password for device	Require that the password include both numeric and alpha characters.

Password Strength Policy Settings

Minimum length of device PIN	This specifies the minimum length of a password.
Number of consecutive incorrect PIN input before device is wiped	The number of failed login attempts to the device before the device automatically initiates a local wipe. The device does not need to contact the server for this to happen.
Idle time before device is locked (Minutes)	How long the device remains active when not in use before the device is locked. To unlock the device, users must enter their PIN.

Users' Mobile Device Self Care Features

The Zimbra Web Client **Preference> Mobile Devices** folder lists users mobile devices that have synced with ZWC. Users can directly manage the following device functions from here:

- Perform a remote wipe of a device. If a mobile device is lost, stolen, or no longer being used, users can initiate a remote wipe from their ZWC account to erase all data from the mobile device. A user selects the device to wipe and clicks **Wipe Device**. The next time the device requests to synchronize to the server, the wipe command is initiated. The device is returned to its original factory settings. Once the wipe is complete, the status of the device in the **Preference> Mobile Devices** folder shows as wipe completed.

Users can cancel a device wipe any time before the device connects with the server.

- Suspend a sync that has been initiated from the mobile device and resume the sync to the device
- Delete a device that from the list. If a device is deleted from the list and attempts to sync after that, the server forces the device to re-fetch the policy on the next sync of the device.

Note: *This list can include devices that do not have the ability to support the mobile policy rules. Wiping a device does not work.*

Changing Mobile Device Password Policy

Once a mobile device is locked by the ZCS server password policy, in order to remove the PIN requirement on the device, the device sync relationship with the server must be deleted and then the PIN requirement for the device must be turned off. After the PIN requirement is turned off, the user re syncs the device to the ZCS account.

ZCS 6.0.5 and later - To disable the password policy

1. In the administration console, open the user account to be modified.
2. Open the Zimbra Mobile tab and uncheck **Force pin on device**.

Once the password policy has been turned off, users must resync their devices to their ZCS account as follows:

- If the device is a WM6 device, the user syncs to the account. After the sync has completed, instruct the user to go to the **Lock** setting on the device and **turn off the device PIN**.
- If the device is an iPhone/iPod Touch 3.0 or above, the user syncs to the account. After the sync, instruct the user to go to the **Settings>General** properties and **turn off Passcode Lock**.

Note: *If the iPhone/iPod Touch is prior to 3.0, an Apple software bug that prevents downloading new device policies to take effect. The user must delete the ZCS account from the iPhone/iPod Touch, turn the PIN off, and then re-setup sync with the ZCS. Because the password requirement was turned off, a PIN is not asked for.*

ZCS 6.0.0 (GA) - to 6.0.4 - To disable the password policy

1. In the administration console, open the user account to be modified.
2. Open the Zimbra Mobile tab and uncheck **Force pin on device**.
3. Click **View Mail** for the account to log into the user's ZWC account, or ask the user to log into his ZWC account.

4. Select **Preferences>Mobile Devices**.
5. Select the mobile device and click **Delete**.
 - If the device is a WM6 device, have the user sync to the account. After the sync has completed, instruct the user to go to the **Lock** setting on the device and **turn off the device PIN**.
 - If the device is an iPhone/iPod Touch 3.0 or above, have the user sync to the account. After the sync, instruct the user to go to the **Settings>General** properties and **turn off Passcode Lock**.

Note: *If the iPhone/iPod Touch is prior to 3.0, an Apple software bug that prevents downloading new device policies to take effect. The user must delete the ZCS account from the iPhone/iPod Touch, turn the PIN off, and then re-setup sync with the ZCS. Because the password requirement was turned off, a PIN is not asked for.*

Chapter 14 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 Zimlets are added to the ZCS, users can look at information and interact with the third-party applications from within their email messages. With Zimlets, arbitrary message content can be made live by linking it with Web content and services on intranets or the Internet.

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

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

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 detailed information about creating Zimlets, see the [Zimlet Development section on the Zimbra Wiki](#).

This chapter describes how to deploy, configure, and manage Zimlets on the Zimbra server. A few of 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 interface (CLI) to deploy the Zimlet to users. You can configure Zimlets only from the command line interface.

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.

Modify COS Before Deploying Zimlets

Before you deploy a Zimlet, the COS attribute, **zimbraProxyAllowedDomains** must be set for the domain address that the Zimlet might call to get information.

To set this attribute, type:

```
zmprov mc <COSname> +zimbraProxyAllowedDomains <*. domain.com>
```

The * must be added before the domain.com.

This must be applied to all COSs that have your Zimlet enabled.

View Status of Zimlets

Type **zmzimletctl listZimlets** to view the status of installed Zimlet files. This displays Zimlets installed on the server, Zimlets installed in LDAP and Zimlets available by COS.

Managing Zimlets from the Administration Console

You can manage the following Zimlet management tasks from the Zimbra 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 it available to the members of the default COS.
- Make a Zimlet available or not available per COS or account.
- Make a Zimlet mandatory.
- 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. You should copy your Zimlets to the **/opt/zimbra/zimlets-extra** directory.

To deploy a Zimlet to the default COS

1. Copy the Zimlet zip file to the `/opt/zimbra/zimlets-extra` directory.
2. To deploy, type the following command

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

The Zimlet is copied to the `/opt/zimbra/zimlets-deployed` directory.

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 enables 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 and grant access to a COS other than the default COS

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 Zimlet zip file to the `/opt/zimbra/zimlets-extra` directory.
2. To deploy, type the following command

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

The Zimlet is copied to the `/opt/zimbra/zimlets-deployed` directory. If your Zimlet included a .jsp file, the .jsp file is copied to the `/opt/zimbra/jetty/webapps/zimlet/<zimletnamefolder>`.

This deployment 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 enables 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

Viewing Zimlet List

To view a list of Zimlets that are on the server and their status type

```
zmzimletctl listZimlets all
```

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.

See the [Zimlet Development section on the Zimbra Wiki](#) for general Zimlet development articles. Review the [ZimletDevSetup](#) article for details about developing and deploying.

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
```

Upgrading a Zimlet

Upgrading your customized Zimlet is the same steps as deploying a new Zimlet.

1. The Zimlet zip files should have the same name. Copy the Zimlet zip file to the /opt/zimbra/zimlets-extra directory, replacing the older version.
2. To deploy, type the following command

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

The Zimlet is copied to the /opt/zimbra/zimlets-deployed directory. If your Zimlet included a .jsp file, the .jsp file is copied to the /opt/zimbra/jetty/webapps/zimlet/<zimletnamefolder>.

3. In order for the newer version to be available, flush the cache. From the administration console, select the server and click **Flush cache**. On the Flush server cache dialog, make sure that there is a check next to **Flush zimlet cache**.

To flush the cache from with command line, **zmprov flushCache zimlet**.

You do not enter the zimlet name.

Disabling or Removing a Zimlet

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

To turn off access from a COS

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

To disable a Zimlet on the Zimbra server

Type **zmzimletctl disable <zimletname>**

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

To uninstall and remove a Zimlet from the Zimbra server

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

Type **zmzimletctl undeploy <zimletname>**

The Zimlet and all associated files are uninstalled.

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

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

Zimlets enabled by default in ZCS

Zimbra Collaboration Suite includes preconfigured Zimlets when ZCS is installed. These Zimlets do not appear in the navigation panel list but come into play by enhancing the user experience when users certain ZWC features.

For email messages, users can 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 in the Address Book.
- **URLs**, to quickly go to the website specified in an email message.

- **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.
- **Emoticons**, to add a textual portrayal of different facial expressions to your messages. The emoticons are available from a link on the compose toolbar.

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.

The Zimlets Gallery

A library of Zimlets are available for deployment when you install or upgrade ZCS. Deploying relevant Zimlets provides users with features to help them efficiently handle routine tasks without leaving the ZWC interface. These Zimlets are found in `/opt/zimbra/zimlets-extra`.

Additional Zimlets can be downloaded from the Zimbra Website, <http://gallery.zimbra.com/gallery.php>

Chapter 15 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, and to create nightly reports
- Mailbox quota monitoring
- MTA mail queue monitoring
- Log files

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

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

Zimbra Logger

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

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. Real-time service status, MTA, spam, virus traffic and performance statistics can be displayed.

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

To enable Server Statistics:

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

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

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

Enabling Remote Syslogging on Mac OS X

To enable remote syslogging on Mac OS X

1. Back up the daemon file to the desktop. Type
`sudo cp /System/Library/LaunchDaemons/com.apple.syslogd.plist ~/Desktop/`
2. Edit the list using the nano Unix editor. Type
`sudo nano /system/Library/LaunchDaemons/com.apple.syslogd.plist`
3. Scroll down to this line
`<string>/usr/sbin/syslogd</string>`
Add the following directly below this line
`<string>-u</string>`
4. Save and exit.
5. Stop and start the daemon. Type
`sudo launchctl unload /System/Library/LaunchDaemons/
com.apple.syslogd.plist`
`sudo launchctl load /System/Library/LaunchDaemons/com.apple.syslogd.plist`

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

If the Zimbra-logger package is installed on a Zimbra mailbox server. Server Statistics 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.

When Server Statistics is selected in the Navigation pane, consolidated statistics for all mailbox servers is displayed. Selecting a specific server in the expanded view shows statistics for that server only. Server specific information also includes disk usage, session information, and mailbox quota details.

The following tabs display system-wide information:

- **Message Count** counts message transactions. A transaction is defined as either the SMTP receipt of a message per person (by Postfix) or a LMTP delivery of it (by mailboxd) per person. For example, if a message is sent to three people, six transactions are displayed. Three for SMTP to Postfix and three for LMTP to mailboxd. The message count is increased by six.
- **Message Volume** displays the aggregate size in bytes of transactions sent and received per hour and per day. Graphs show the total inbound data by volume in bytes.
- **Anti-Spam/Anti-Virus Activity** displays the number of messages that were checked for spam or viruses and the number of messages that were tagged as spam or deemed to contain a virus. The AS/AV count is increased by one per message scanned. One message sent to three people counts as only one message processed by AS/AV.

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.
- Messages 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.
- The Advanced Statistics tab is used to generate

Server-specific statistics also include the following tabs:

- **Disk** for a selected server displays the disk used and the disk space available. The information is displayed for the last hour, day, month, and year.
- **Session** displays information about the active Web client, administrator and IMAP sessions. You can see how many active sessions are opened, who is logged on, when the session was created and the last time the session was accessed.
- **Mailbox Quota** displays information about each account sorted by mailbox size in descending order. See [“Monitoring Mailbox Quotas” on page 171](#).

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 11:30 p.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 25 sender and 25 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 Disk Space

You should regularly review your disks capacity and when disks are getting full you should take preventative measures to maintain service. To alert administrators of low disk space, an email notification is sent to the admin account. The default is to send out warning alerts when the threshold reaches 85% and a critical alert when the threshold reaches 95%.

You can change these values. Use `zmlocalconfig` to configure the disk warning thresholds.

- Warning alerts: **zmdisklog_warn_threshold**
- Critical alert: **zmdisklog_critical_threshold**

When starting services with `zmcontrol`, if the threshold is exceeded, a warning is displayed before the services are started. You should clean up your disk to free up space.

Monitoring Servers

The ZCS server collects many performance-related statistics that can help you diagnose problems and load issues.

The **Server Statistics Advanced Statistics** tab includes advanced graphing options that lets you generate various charts based on statistical information for the CPU, IO, mailboxd, MTA queue, MySQL and other components.

To chart the graphics in the Server Statistics Advanced Statistics tab, select one of these groups and then select from the list of specific counters for the type of information to display.

The information covers a wide array of data:

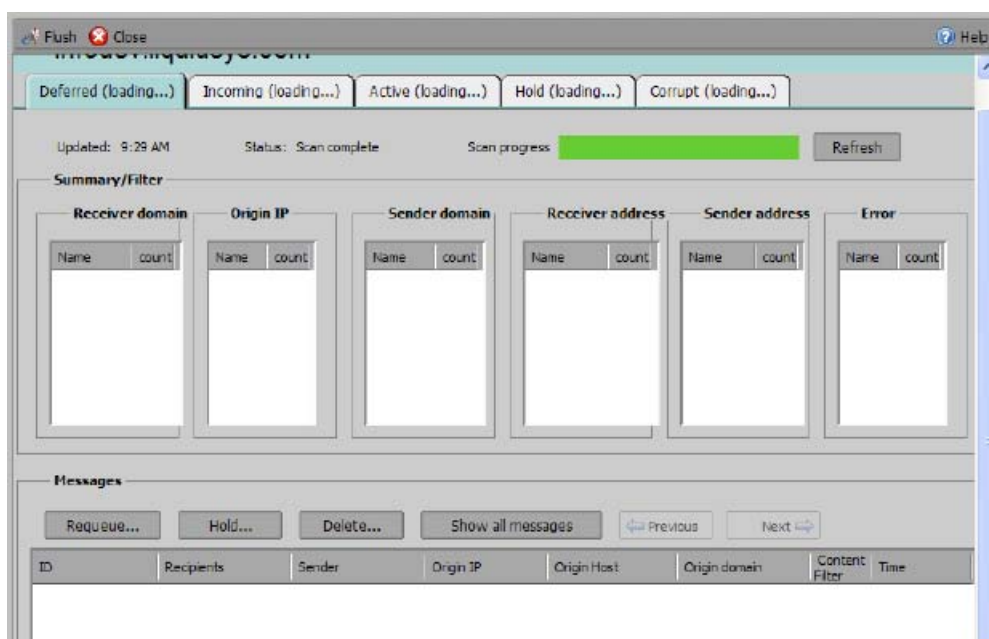
- **cpu.csv**: CPU utilization. This group contains counters to keep track of CPU usage (iowait, idle, system, user, time etc.). CPU information can be tracked both at the server level and the process level.
- **df.csv**: Captures disk usage. Disk utilization is tracked for each disk partition.
- **fd.csv**: file descriptor count. Keeps track of system file descriptor usage over time. This is primarily used to track down “out-of-file descriptor” errors.
- **mailboxd.csv**: ZCS server and JVM statistics. Mailboxd stores almost all of its statistics here. Interesting numbers to keep track of are heap_used, heap_free, imap_conn, soap_sessions, pop_conn, db_conn_count.
- **mtaqueue.csv**: Postfix queue. This measures the mail queue size in number of messages and the size in bytes.
- **proc.csv**: Process statistics for Zimbra processes. For example mailboxd/java, MySQL, OpenLDAP, etc.)
- **soap.csv**: SOAP request processing time.
- **threads.csv**: JVM thread counts. Counts the number of threads with a common name prefix.
- **vm.csv**: Linux VM statistics (from the vmstat command).
- **io-x.csv** and **io.csv** store data from the iostat(1) command (io-x.csv with iostat -x).

You can also use **zmstats** CLI to view performance metrics and statistics. The CLI, **zmstat-chart**, can be used to generate charts from the .csv data. The data is read from the .csv files in **/opt/zimbra/zmstat/<date>**. Files created with **zmstats-chart** are in a standard CSV format that can be loaded into Excel for viewing and charting. See the Zimbra wiki article, [Zmstats](#).

Monitoring Mail 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 52.

Figure 1: Mail 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 following Mailbox Queue functions can be performed for all the messages in a queue:

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

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

Flushing the Queues

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

Monitoring Mailbox Quotas

Mailbox quotas apply to email messages, attachments, calendar appointments, tasks, briefcase files, and document notebooks in a user's account. When an account quota is reached all mail messages are rejected. Users must delete mail from their account to get below their quota limit, or you can increase their quota. This includes emptying their Trash.

You can check mailbox quotas for individual accounts from Server Statistics on the administration console. The Mailbox Quota tab gives you an instant view of the following information for each account:

- Quota column shows the mailbox quota allocated to the account. Quotas are configured either in the COS or by account.
- Mailbox Size column shows the disk space used
- Quota Used column shows what percentage of quota is used

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

Monitoring Authentication Failures

To guard against simple password harvest attacks, a ZCS account authentication password policy can be configured to insure strong passwords and a failed login policy can be set to lockout accounts that fail to log in after the maximum number of attempts. These policies protect against targeted account attacks, but do not provide visibility into dictionary and distributed based attacks.

The `zmauditwatch` script attempts to detect these more advanced attacks by looking at where the authentication failures are coming from and how frequently they are happening for all accounts on a Zimbra mailbox server and sends an email alert to the administrator's mailbox.

The types of authentication failures checked include:

- **IP/Account hash check.** The default is to send an email alert if 10 authenticating failures from an IP/account combination occur within a 60 second window.
- **Account check.** The default is to send an email alert if 15 authentication failures from any IP address occur within a 60 second window. This check attempts to detect a distributed hijack based attack on a single account.

- **IP check.** The default is to send an email alert if 20 authentication failures to any account occur within a 60 second window. This check attempts to detect a single host based attack across multiple accounts.
- **Total authentication failure check.** The default is to send an email alert if 1000 auth failures from any IP address to any account occurs within 60 seconds. The default should be modified to be 1% of the active accounts on the mailbox server.

The default values that trigger an email alert are changed in the following `zmlocalconfig` parameters:

- IP/Account value, change `zimbra_swatch_ipacct_threshold`
- Account check, change `zimbra_swatch_acct_threshold`
- IP check, change `zimbra_swatch_ip_threshold`
- Total authentication failure check, change `zimbra_swatch_total_threshold`

Configure `zimbra_swatch_notice_user` with the email address that should receive the alerts.

Log Files

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

Local logs containing Zimbra activity are in the `/opt/zimbra/log` directory.

- **audit.log.** This log contains authentication activity of users and administrators and login failures. In addition, it logs admin activity to be able to track configuration changes.
- **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 mailboxd log4j server log containing the logs from the mailbox server. This includes the mailbox store, LMTP server, IMAP and POP servers, and Index server. (Note: prior to ZCS 4.5, this log was called `/opt/zimbra/log/zimbra.log`.)
- **myslow.log.** This slow query log consists of all SQL statements from the mailbox server that took more 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 `zmtrainasa` during regularly scheduled executions from the cron.

- **sync.log.** This log contains information about ZCS mobile sync operations.

Other logs include:

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

ZCS activity logged to System syslog

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

Syslog

Zimbra modifies the systems syslog daemon to capture data from the mail and local syslog facility to **/var/log/zimbra.log**. This allows syslogd to capture data from several ZCS components including Postfix, Amavis, ClamAV, mailboxd, zmmtaconfig, and logger. The SNMP module uses the data from the log file to generate traps for critical errors. The zmlogger daemon also collects a subset of the data in this file to provide statistics on the utilization of ZCS via the administration console.

By default, mailboxd is configured to log its output to **/opt/ZCS/log/mailboxd.log**. You can enable mailboxd to take advantage of a centralized syslogd infrastructure by enabling the following either globally or by server

```
zmprov mcf zimbraLogToSysLog True
```

Using log4j to Configure Logging

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

Logging Levels

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

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

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

The following categories are pre-defined in log4j:

zimbra.account	Account operations
zimbra.acl	ACL operations
zimbra.backup	Backup and restore
zimbra.cache	In-memory cache operations
zimbra.calendar	Calendar operations
zimbra.dav	DAV operations
zimbra.dbconn	Database connection tracing
zimbra.extensions	Server extension loading
zimbra.filter	Mail filtering
zimbra.gal	GAL operations
zimbra.im	Instant messaging operations
zimbra.imap	IMAP protocol operations
zimbra.index	Index operations
zimbra.io	File system operations
zimbra.ldap	LDAP operations
zimbra.lmtp	LMTP operations (incoming mail)
zimbra.mailbox	General mailbox operations
zimbra.misc	Miscellaneous
zimbra.op	Changes to the mailbox state
zimbra.pop	POP protocol operations
zimbra.redolog	Redo log operations
zimbra.security	Security events
zimbra.session	User session tracking
zimbra.smtp	SMTP operations (outgoing mail)
zimbra.soap	SOAP protocol
zimbra.sqltrace	SQL tracing
zimbra.store	Mail store disk operations
zimbra.sync	Sync client operations
zimbra.system	Start-up/shutdown and other system messages
zimbra.wiki	Wiki operations
zimbra.zimlet	Zimlet operations
zimbra.mailop	Changes to mailbox state
zimbra.purge	Mailbox purge operations

Changes to the log level take affect immediately.

Table 1 zimbra Logging Levels

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

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

Reviewing mailbox.log Records

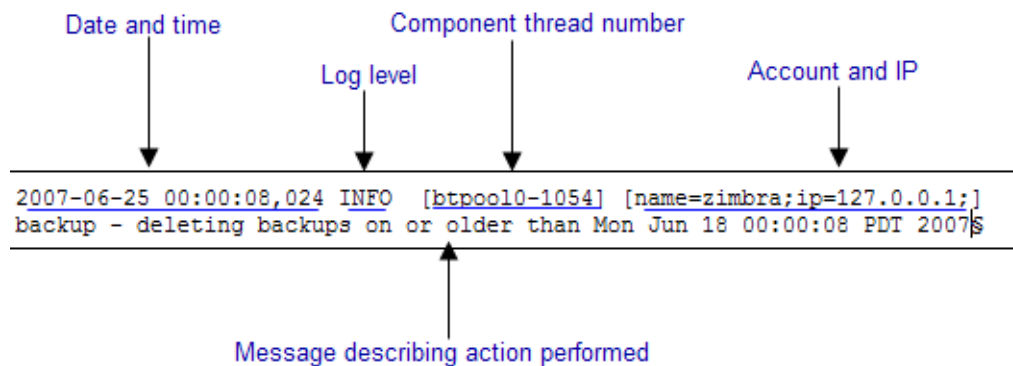
The mailbox.log file logs every action taken on the mailbox server, including authentication sessions, LMTP, POP3, and IMAP servers, and Index server. Review the mailbox.log to find information about the health of your server and to help identify problems.

Mailbox.log records valid and invalid login attempts, account activity such as opening email, deleting items, creating items, indexing of new mail, server activities including start and stop. The progress of an activity on the mail

server is logged as INFO and if the expected results of the activity fails and errors occurs, an exception is written to the log.

Note: You can set up logging options for a single account in order to trace account activity for one user without filling up mailbox.log with log messages for unrelated accounts. See [Appendix A Command-Line Utilities](#), `zmprov miscellaneous`.

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



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

Handler Exceptions and Stack Traces

If an error occurs during the progress of an activity, a handler exception is added to the end of the basic log record to notify you that an event occurred during the execution of the process that disrupted the normal flow. This signals that some type of error was detected.

```
2007-06-25 00:00:10,379 INFO [btpool0-1064] [name=nriers@example.com;
mid=228;ip=72.255.38.207;ua=zimbra Desktop/0.38;] SoapEngine - handler
exception
```

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


```

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

```

Mailbox log files

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

mailbox.log examples

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

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

Service Error - System Crashing

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

```

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

```

Look for errors before the startup message.

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

Mail Error - Mail Delivery problem

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

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

```

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

```

Account Error- Log in error

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

```

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

```

Account Errors - IMAP or POP related

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

```

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

```

Reading a Message Header

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

The following lines are in the message header:

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

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

Checking MySQL

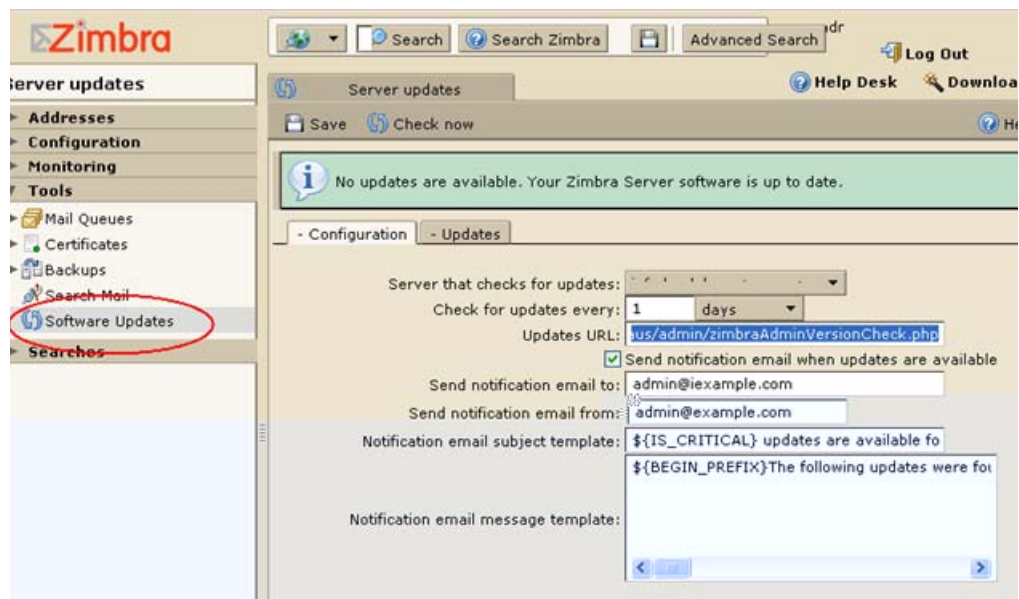
The MySQL database is automatically checked weekly to verify the health of the database. This check takes about an hour. If any errors are found, a report is sent to the administrator's account. The report name that runs the MySQL check is **zmbintegrityreport**, and the crontab is automatically configured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

Note: When the MySQL database is checked, running this report can consume a significant amount of I/O. This should not present a problem, but if you find that running this report does affect your operation, you can change the frequency with which `zmbintegrityreport` is run. See [Appendix B ZCS Crontab Jobs](#).

Checking for Latest ZCS Software Version

ZCS is configured to check for ZCS software updates. The default configuration is to check for updates daily and to automatically send a notification to the admin's mailbox when a new ZCS version is available.

You can change the configuration from the administration console **Overview pane>Tools>Software Updates** link.



The dates and times ZCS checked for updates is saved to the **Updates** tab and an email notification is sent out until you update the ZCS version. If you do not want to receive an email notification of updates, disable **Send notification email when updates are available**.

You can check for updates any time by clicking the **Check now** link.

Chapter 16 Backup and Restore

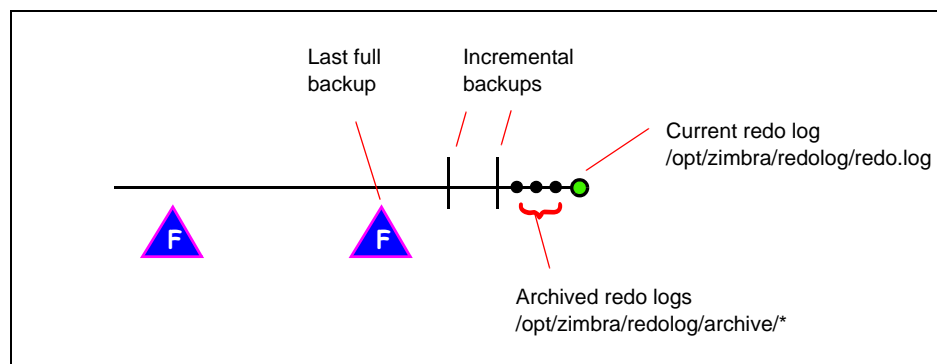
Backing up the ZCS mailbox server on a regular basis can help you quickly restore your mail service, if an unexpected crash occurs. The backup process writes a consistent snapshot of mailboxes to a designated backup directory.

ZCS mailboxes can be restored from the following:

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

Figure 2 shows the sequence of a full 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 2: Sample backup timeline



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

Zimbra Backup Methods

Two distinct backup methods are available on ZCS.

- The **standard backup method** is to run a weekly full backup session and daily incremental backup sessions to back up all mailboxes daily. The standard backup method is appropriate for enterprise deployments where full backups are run during non-working days.
- The **auto-grouped backup method** is recommended for large ZCS environments where running a full backup of all accounts at one time would take too long. The auto-grouped backup method runs a full backup session for a different group of mailboxes at each scheduled backup. The system administrator configures the interval that backups should run and configures the number of groups that backups are made up of. ZCS then automatically backs up mailboxes in groups over the interval specified.

Standard Backup Method

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 file representing a message already exists in the backup. If it does, it flags this object as such and does not copy its content again.

An incremental backup process backs up the LDAP data and gathers all the redo logs written since the last incremental 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 taken place. They contain a full copy of all messages delivered, as well as metadata such as tags, contacts, and conversations.

These backup files can be used to restore the complete mailbox server 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.

Each mailbox 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 reads the current redo log upon startup and re-executes and completes any uncommitted transactions.

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

When 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 mailboxd's server.xml, are not backed up.

Auto-Grouped Backup Method

The auto-grouped backup method is designed for very large ZCS environments where backing up all accounts can take a long time. Auto-grouped backups combine full and incremental backup functions. This eliminates the need for incremental backups. Each auto-grouped session runs a full backup of the targeted group of mailboxes.

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 standard backup process is shown in Figure 3. You can run regularly scheduled backups to the same target area without overwriting previous backup sessions.

The **accounts.xml** file lists all accounts that are in all the backups combined. For each account, this file shows the account ID, the email address, and the label of the latest full backup for that account. If you save your backup sessions to another location, you must also save the latest accounts.xml file to that location. The accounts.xml file is used to look up the latest full Backup for an account during restore. If the accounts.xml file is missing you must specify the backup label to restore from.

All incremental and auto-grouped backup sessions must be saved to the same directory as all the redo logs must be found in the same backup target. Standard full backup sessions can use a different target directory.

Figure 3: Standard Backup directory structure

/opt/zimbra/backup	Default root of backups
accounts.xml/	List of all accounts, each with email file address, Zimbra ID, and latest full backup label. The accounts.xml maintains the mapping of email addresses to their current zimbralds and also the most recent full backup for each account.
sessions/	Root of backup sessions.
full-<timestamp>/	A full backup directory. The timestamp for a session is the backup start time in GMT, including milliseconds. GMT is used rather than local time to preserve visual ordering across daylight savings transitions.
session.xml	Metadata about this backup label for full or incremental session, such as start and stop times.
shared_blobs/	Contains message files that are shared among accounts in this backup.
sys/	Global database tables and localconfig.
db_schema.xml	Database schema information for global tables. Each table dump file has a .csv format.
localconfig.xml	Copy of /opt/zimbra/conf/localconfig.xml at the time of the backup.
<table name>.dat	Database table data dump.
LDAP/ldap.bak	LDAP dumps.
accounts/	Each account's data is saved in a subdirectory of this.
<.../zimbrald>/	Root for each account.
meta.xml	Metadata about this account's backup.
ldap.xml	Account's LDAP information, including aliases, identities, data sources, distribution lists, etc.
ldap_latest.xml	If this is present, this file links to ldap.xml of the most recent incremental backup.
db/	Account-specific database table dumps.
db_schema.xml	Database schema information for this account's tables.
<table name>.dat	Database table data dump.
blobs/	Contains blob files.
index/	Contains Lucene index files.
incr-<timestamp>	An incremental backup directory. This directory is similar to the full backup directory schema and includes these meta files.
session.xml	
sys/db_schema.xml	
accounts/.../<zimbrald>/ldap.xml	
	incr-<timestamp> does not include accounts/.../<zimbrald>/db/db_schema.xml because incremental backup does not dump account tables.

Note: For auto-grouped backups, the directory structure saves the redo log files to the full backup session. There are no incremental backup sessions.

Backup and Restore Using 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.

Standard Backup Method

You can perform the following backup and restore tasks:

- Immediately start a full or incremental backup
- Restore all accounts or specific accounts and restore to a new account or another 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 standard backup schedule is set by default during install, you can change this schedule from the command line. See “Scheduling Backups” on page 189.

Auto-grouped Backup Method

You can only run full backups in the auto-grouped method. It is not recommended to run auto-grouped backups manually since they are scheduled from the CLI and run automatically at the scheduled times. You can perform the following backup and restore tasks:

- Configure the server to run in auto-grouped backup mode
- Find a specific backup
- Abort a backup that is in progress
- Restore all or specific accounts and restore to a new account or another server
- View backup session labels, start and end times, and the status

The auto-grouped backup schedule can only be set from the CLI using the **zmschedulebackup** command. See “Scheduling Backups” on page 194.

Configure Backup from the Admin Console

Backups can be configured from the administration console as a global settings configuration and as a server-specific configuration. Server settings override global settings.

In the global settings, you can configure the email addresses to receive notification about the results of the backup. The default is to sent the notification to the admin account.

For Auto-grouped, you configure the number of groups to divide the backups into.

The screenshot shows the 'Manage Global Settings' web interface. At the top, there are 'Save' and 'Download' buttons. Below them is a yellow note: 'Note: Settings only apply to servers that have the appropriate service(s) installed and enabled. Server settings override.' A horizontal tab bar contains the following tabs: 'General Information', 'Attachments', 'MTA', 'IMAP', 'POP', 'AS/AV', 'Free/Busy Interop', 'Themes', 'License', 'HSM', and 'Backup'. The 'Backup' tab is selected. The main content area shows the following settings:

- Backup mode:** A dropdown menu set to 'Standard'.
- Number of groups:** A text input field containing the number '7'.
- Throttle automatic backups:** An unchecked checkbox.
- Default backup target:** A text input field containing '/opt/zimbra/backup'.
- Notification email sender ("from" address):** A text input field containing 'admin@example.com'.
- Prefix for notification email subject:** A text input field containing 'ZCS Backup Report'.
- Notification email recipients:** A text input field containing 'admin@example.com'.

At the bottom right of the form, there are two buttons: 'Add address' and 'Remove'.

The standard backup is the default and is automatically scheduled. You do not need to make any additional changes. But when running the auto-grouped backup you must manually configure the backup schedule. Access the CLI and follow the steps under “Scheduling Backups” on page 194 to run **zmschedulebackup -D** to set the default schedule for auto-grouped backups.

Throttle automatic backups should be enabled when you are mass migrating new accounts to ZCS and use the auto-grouped backup method.

The auto-grouped backup method automatically backs up mailboxes that have never been backed up when the next backup is scheduled. When migrating a large number of mailboxes, enable **Throttle automatic backups** so that the mailboxes that are migrated to ZCS are not automatically backed up as new mailboxes because the number of new mailboxes could prevent backing up existing mailboxes. Leave the throttle mode on for 7 days (cycle-through) after the mass migration is over. Allow the total mailbox count to reach an equilibrium, then let the auto-group backup cycle through before turning off the throttle mode.

Backup and Restore Using the Command Line Interface

The Zimbra backup and restore procedures can be 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, incremental backups, and deletion of old backups.
- **zmbbackup.** This command executes full or incremental backup of the mail server. This is run on a live server, while the mailboxd process and the mailbox server are running. This command also has an option to manually 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.

- **zmbackupquery.** 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 mailboxd process is stopped.
- **zmrestoreldap.** This command restores the complete LDAP directory server, including accounts, domains, servers, COS and other data.

Refer to “Zimbra CLI Commands” on page 228 for usage and definitions for each of these commands.

Backing up using the Standard Method

When you initiate a backup, you can issue the command from the same server being backed up, run the command remotely and specify the target server on the command line, or use the administration console to start a backup session.

Scheduling Backups

When ZCS was installed, the backup schedule for the standard method of full and incremental backups was added to the crontab. Under the default schedule, the full backup is scheduled for 1:00 a.m., every Saturday. The incremental backups are scheduled for 1:00 a.m., Sunday through Friday.

By default, backups older than a month are deleted every night at 12 a.m.

You can change the backup schedule using the **zmschedulebackup** command.

Specify the fields as follows, separate each field with a blank space:

- 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, or use names)

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

Example of zmschedulebackup options

- Replace the existing full backup, incremental backup and delete backup schedule. When you use -R, the complete backup schedule is replaced. If you use this command, remember to set the delete schedule, if you want backup sessions to be scheduled for automatic deletion. This example replaces the existing schedule to have full backups run on Sunday at 1 a.m., incremental backups to run Monday through Saturday at 1 a.m., and old backups deleted at 12:00 a.m. every day.

```
zmschedulebackup -R f "0 1 * * 7" i "0 1 * * 1-6" d "0 0 * * *
```

- Add an additional full backup time to your current schedule. This example adds a full backup on Thursday at 1 a.m.

```
zmschedulebackup -A f "0 1 * * 4"
```

- Review your backup schedule. The schedule is displayed.

```
zmschedulebackup -q
```

- Save the schedule command to a text file. This would allow you to easily recreate the same schedule after reinstall or upgrade

```
zmschedulebackup -s
```

Note: If you change the default schedule and want to return to it, enter the command `zmschedulebackup -D`.

The default backup schedule looks like this in the cron table:

BACKUP BEGIN :

<pre>0 1 * * 6 /opt/zimbra/bin/zbackup -f - all 0 1 * * 0-5 /opt/zimbra/bin/zbackup -i 0 0 * * * /opt/zimbra/bin/zbackup -del 1m</pre>
--

Read as follows:

- `0 1 * * 6 /opt/zimbra/bin/zbackup -f - all` means that the full backup runs on 1 a.m. on Saturdays.
- `0 1 * * 0-5 /opt/zimbra/bin/zbackup -i` means that an incremental backup runs at 1 a.m. from Sunday through Friday.
- `0 0 * * * /opt/zimbra/bin/zbackup -del 1m` means that backup sessions are deleted at midnight 1 month after they were created.

How to read the crontable

Each crontab entry contains six fields that appear in this order:

Field

1 2 3 4 5 6

0 1 * * 6 /opt/zimbra/bin/zmbbackup -f -all

1 - minute (0-59 allowed)

2 - hour (0-23)

3 - day of month (1-31)

4 - month (1-12 or names)

5 - day of week (0-7 or names allowed, with both 0 and 7 representing Sunday)

6 - string to be executed

The asterisk character works as a wild card, representing every occurrence of the field's value.

Backup Completion Email Notification

A backup report is sent to the admin mailbox when full and incremental backups are performed. This report shows the success or failure of the backup and includes information about when the backup started and ended, the number of accounts backed up and redo log sequence range.

If the backup failed, additional error information is included.

You can add additional recipient addresses or change the notification email address in the administration console Global Settings, Backup/Restore tab.

Full Backup Process

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

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

- c. Creates a backup of the index directory for that mailbox.
5. Returns that account's mailbox to active mode and moves on to the next one.
6. Backs up the LDAP directory.

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.

Backup files are saved as zip files without compression. To change the default zip option, see Appendix A Command Line Interface, "[zmbackup](#)" on page 248.

Incremental Backup Process

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

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

Archived logs that are less than an hour old at the time of incremental backup are copied to the backup and are not deleted. These redologs are deleted one hour after the backup. The interval is set by the localconfig key **backup_archived_redolog_keep_time**. The default is 3600 seconds.

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.

4. Backs up the LDAP directory.

Example Backup Commands

- Perform a full backup of all mailboxes on server1
zmbackup -f -s server1.domain.com -a all
- Perform incremental backup of all mailboxes on **server1** since last full backup
zmbackup -i -s server1.domain.com -a all
- Perform full backup of only **user1**'s mailbox on **server1**
zmbackup -f -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 Backups

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. Each backup session is automatically labeled by date and time. For example, the label **full-20070712.155951.123** says this is a backup from July 12, 2007 at 3:59:51.123.

Note: The times set in the session label are GMT, not the local time. GMT is used rather than local time to preserve visual ordering across daylight savings transitions.

The command can be used to find the following sessions:

- A specific full backup set
zmbbackupquery -lb full-20070712.155951.123
- Full backup sets since a specific date
zmbbackupquery --type full --from "2007/01/01 12:45:45"
- All full backup sets in the backup directory
zmbbackupquery --type full
- Best point in time to restore for an account by specifying a time window
zmbbackupquery -a user1@example.com --type full --from "2007/07/05 12:01:15" --to "2007/07/12 17:01:45"

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. The temporary backup session can be found at <backup target>/sessions_tmp directory. You can use the **rm** command to delete the directory.

Aborting Full Backup In Progress

You can use the CLI command, **zmbbackupabort** to stop a backup that is in progress. The backup is immediately stopped and becomes a partially successful backup.

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

Example

- Stop the backup, if you know the label name
`zmbakupabort -lb full-20070712.155951.123 -s server1`
- Stop the backup, if you do not know the label
 - a. `zmbakupquery`
 - b. `zmbakupabort -s server1 -lb full-20070712.155951.123`

Backing up using the Auto-Grouped Method

The auto-grouped backup method is configured either from the Admin Console User Interface or from the CLI.

Configure Auto-Grouped Backup from the CLI

Set the backup method in the global configuration, and you can override the configuration on a per server basis if you do not want a server to use the auto-grouped backup method.

To set up auto-grouped backup, you modify LDAP attributes using the `zmprov` CLI. Type the command as

```
zmprov mcf <ldap_attribute> <arg>
```

You can also set the attributes at the server level using **zmprov ms**.

The following LDAP attributes are modified:

- **zimbraBackupMode**. Set it to be **Auto-Grouped**. The default is **Standard**.
- **zimbraBackupAutoGroupedInterval**. Set this to the interval in either days or weeks that backup sessions should run for a group. The default is 1d. Backup intervals can be 1 or more days, entered as xd (1d); or 1 or more weeks, entered as xw (1w).
- **zimbraBackupAutoGroupedNumGroups**. This the number of groups to spread mailboxes over. The default is 7 groups.

Scheduling Backups

The standard backup is the default and is automatically scheduled. To run the auto-grouped backup you must manually configure the backup schedule. Run **zmschedulebackup -D** to set the default schedule for auto-grouped backups based on your **zimbraBackupAutoGroupedInterval** setting.

One group is backed up each interval. The auto-grouped backup automatically adjusts for changes in the number of mailboxes on the server. Each backup session backs up the following:

- All mailboxes that have never been backed up before. These are newly provisioned mailboxes.

- All mailboxes that have not been backed within the number of scheduled backup days. For example, if backups are scheduled to run over six days, mailboxes that have not been backed up in the past 5 days are backed up.
- More mailboxes, the oldest backup first. This is done so that the daily auto-grouped backup load is balanced.

Example - if you configured the auto-grouped backup interval to be daily (1d) and the number of groups to be 7, the first time auto-grouped backup runs, all accounts are backed up. After the initial backup, auto-grouped backup runs again the next day. This time accounts that have been newly provisioned and a percentage of accounts close to 1/7 of the total are backed up again, accounts with the oldest backup date are backed up first. This would continue with newly provisioned account and approximately 1/7 of accounts being backed up daily over seven days.

As with the standard backup method, when backing up shared messages, the backup process looks to see whether a file representing a message already exists in the backup. If it does, it flags this object as such and does not copy its content again.

Backup files are saved as zip files without compression. Zipping the backup files saves backup storage space. To change the default zip option, see Appendix A Command Line Interface, [“zmbbackup” on page 248](#).

These backup files can be used to restore the complete ZCS system or individual mailboxes so that account and message data is completely restored. Archived redo logs are moved to the backup session as part of the full backup. When the server is restored from an auto-grouped backup, redo logs are replayed to bring the system to the point before the failure.

Backup Options

The backup process can be configured to selectively back up content. You can configure these backup options so that search indexes, blobs, and HSM blobs are not backed up during a full backup session.

- **zimbraBackupSkipSearchIndex.** Default is FALSE. If set to TRUE, search index is not backed up. The mailbox will have to be reindexed after restoring from a backup without the search index.
- **zimbraBackupSkipBlobs.** The default is FALSE. If this is set to TRUE, blobs are not backed up. This might be useful for getting a quicker backup of just database data when the blobs reside on a fault-tolerant storage. This configuration applies to all blobs, those on the primary volumes as well as secondary (HSM) volumes.
- **zimbraBackupSkipHsmBlobs.** The default is FALSE. If this is set to TRUE, blobs on HSM volumes are not backed up. Set this if zimbraBackupSkipBlobs is FALSE but you want to skip blobs on HSM volumes.

Restoring Data

Three types of restore procedures can be run:

- The **zmrestore** command is used to restore the mailboxes while the ZCS 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.

Restore Process

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

1. Retrieves specified accounts 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 to clear any existing data
 - b. Restores the last full backup of the MySQL data, the index directory, and the message directory for that mailbox
 - c. Replays redo logs in all incremental backups since last full backup
 - 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

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 -a all

- Perform a single account restore on server1

zmrestore -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). 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 restore problems with those accounts.

A restore that is run 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, therefore excluding archived and current redo logs of the system.
 - **-rf** - Restores to the full backup only. This does not include any incremental backups at all.
- 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 -a account@company.com-restoreToTime <arg>

Two common ways to write the <timearg> are

- “YYYY/MM/DD hh:mm:ss”
- YYYYMMDD.hhmmss
- Perform an incremental restore only to last full backup, excluding incremental backups since then, for all accounts

zmrestore -rf --a all

- Restore mailbox and LDAP data for an account

zmrestore -ra -a account@company.com

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

zmrestore -ca -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

- Include **--continueOnError (-c)** to the command so that the restore process continues if an error is encountered.

zmrestore -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 -a account@company.com

- To avoid restoring accounts that were deleted

zmrestore -a account@company.com -skipDeletedAccounts

- To restore a mailbox, but exclude all the delete operations that were in the redo log replay. When the mailbox is restored it will contain messages that were deleted. This is useful if users use POP and remove messages from the server

zmrestore -a account@company.com --skipDeletes

Note: When the latest point in time is requested, do not add a backup label (-lb). Without specifying the label, the most recent full backup before the requested point is automatically used as the starting point.

You can restore mailboxes from the administration console as well.

Stopping a Restore Process

The **zmbackupabort -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 .

To stop the restore type:

zmbackupabort -r

Offline Restore Process

The offline restore process can only be run when the mailboxd server is not running. 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 mailboxd is started before the backup files are restored, the mail server would begin to accept email messages and perform 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 mailboxd is running, it would be too late to restore the pre-disaster data. For this reason, the offline restore must be run before the ZCS mailbox store server is started.

The offline restore process goes through the following steps.

1. Specified accounts to be restored are retrieved. 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 to clear any existing data
 - b. Restores the last full backup of the MySQL data, the index directory, and the message directory for that mailbox
 - c. Replays redo logs in all incremental backups since last full backup
 - 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

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

Example

- Restore all accounts on server1 when mailboxd is stopped
zmrestoreoffline -a all

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. For each account to be restored, put the account into maintenance mode. From the command line, type **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.

```
zmrestore -a (account@abc.com account@abc.com)
```

3. For each account that was restored, put the account back into active mode. From the command line, type
zmprov ma <account> 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.

Selectively Restore Items

When you restore from a full backup, you can select to exclude the following items from being restored

- **Search index.** If you do not restore the search index data, the mailbox will have to be reindexed after the restore.

`zmrestore <all or account> --exclude-search-index`

- **Blobs.** This is a useful option when all blobs for the mailbox being restored already exists.

`zmrestore <all or account>|--exclude-blobs`

- **HSM-blobs.** This is useful when all HSM blobs for the mailbox being restored already exists.

`zmrestore <all or account> --exclude-hsm-blobs`

Restoring the LDAP Server

In a disaster recovery where you need to restore not just one server, but the entire system, 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. You can get more information from this wiki page http://wiki.zimbra.com/index.php?title=Network_Edition_Disaster_Recovery.

General Steps for Disaster Recovery

The sequence of events to restore your mailbox store 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 mailbox store server.
2. Put all mailboxes into maintenance mode, to prevent mail delivery and user login while restoring the mailboxes.

3. Stop the mailbox store server, if it is running.

Recovery

4. Reinstall the ZCS 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.

Restore the Zimbra Collaboration Suite Servers

This direction would be in the case of complete machine failure.

Important: *The ZCS version you install on the new server **must be the same version** as installed on the old server. The server can have a different operating system.*

The new server hardware must meet the requirements described in the Installation Prerequisites section of the ZCS Single Server Installation Guide. Install the new operating system, making any necessary OS configuration modifications as described in the installation guide.

Disaster Recovery Changing Servers

You do the following to restore to a new server:

- Prepare the new server
- Block client access to the old server's IP address with firewall rules
- Mount any volumes that were in use on the older server
- Delete the MySQL data that is set up in the initial installation of ZCS
- Copy the backup files to the new server
- Run **zmrestoreldap** to restore the global LDAP data
- Run **zmrestoreoffline** to restore account data from the backup sessions
- Prepare and run a new backup

Old Server Status

Two scenarios for disaster recovery are the server has died and the ZCS files cannot be accessed, or ZCS is still running, but the server hardware needs to be replaced.

If the server is not running:

1. Block client access to the server IP address with firewall rules.
2. Find the latest full ZCS backup session to use.

If ZCS is still running, to prepare the move to the new server:

1. Block client access to the server's IP address with firewall rules.
2. Run a full backup of the old service, or if the backup is recent, run an incremental backup to get the most current incremental backup session.
3. Run **zmcontrol stop**, to stop ZCS. In order to restore to the most current state, no new mail should be received after the last incremental backup has run.
4. Change the hostname and IP address on the old server to something else. Do not turn off the server.

Preparing the New Server

Before you begin, make sure that the new server is correctly configured with the IP address and hostname and that ZCS is installed and configured with the same domain, hostname, passwords, etc. as the previous server. See the ZCS installation guide for more information about preparing the server. Before you begin to install ZCS, note the information you need from the old server including: admin account name and password, LDAP, Amavis, and Postfix passwords, spam training and non-spam training user account names, exact domain name, and the global document account name.

Installing ZCS on new server

Note: *Make sure the computer time is set to the same time as the old server. Verify that the old hostname and MX DNS records resolve to the new server.*

1. Copy your ZCSLicense.xml file to a directory on the new server. You will not be able to complete the ZCS installation if the license is not on the new server.
2. Run **./install.sh** and follow the directions in the installation guide to install ZCS. Make sure that you configure the same domain, hostname, passwords as on the old server. During ZCS install, the following settings must be changed to match the original server settings:
 - a. **Zimbra LDAP Server.** For **Domain to create**, identify the same default domain as on the old server.

- b. **Zimbra Mailbox Server.** An administrator's account is automatically created.
 - Make sure that the account name for **Admin user to create** is the same name as on the original server.
 - Set the admin password to be the same as on the old server.
 - Set the LDAP password to be the same as on the old server.
 - Set the Postfix user and Amavis user passwords to be the same as on the old server
 - Change the **Spam training user** and the **Non-spam (HAM) training user** account names to be the same as the spam account names on the old server.
 - **Global Document Account** – This account name is automatically generated and is usually named wiki. If you changed this, change the Global Document Account name to be the same account name as on the original server.
- c. Change any other settings on the new server to match the configuration on the original server.
- d. In the main menu, set the default backup schedule and the automatic starting of servers after the configuration is complete to **NO**.

Restoring to the new server:

1. Stop the new server, type **zmcontrol stop**.
2. If the old server had additional storage volumes configured, mount any additional volumes now.
3. Delete the mysql data and re initialize an empty data directory. If you do not do this, **zmrestoreoffline** will have errors. As zimbra, type
 - a. **rm -rf /opt/zimbra/db/data/***
 - b. **/opt/zimbra/libexec/zmmyinit**
 The mySQL service is now running.
4. Copy all the files in the **/backup** directory from the old server or from an archive location to **/opt/zimbra/backup**.
5. To restore the LDAP, type **zmrestoreldap -lb <latest_label>**.
 If you are restoring large number of accounts, you may want to run a command such as the UNIX command, **nohup**, so that the session does not terminate before the restore is complete.

Note: To find the LDAP session label to restore, type **zmrestoreldap -lbs**.
6. Because some ZCS services are running at this point, type **zmconvertctl start**. This is required before running **zmrestoreoffline**.

7. Sync your LDAP password from backup directory to the new production servers LDAP config. type
`zmlocalconfig -f -e zimbra_ldap_password=<password>.`
8. To start the offline restore, type
`zmrestoreoffline -sys -a all -c -br.` You may want to run a command such as `nohup` here also. To watch the progress, tail `/opt/zimbra/log/mailbox.log`.

***Note:** Use `-c` on the command line so that accounts will be restored even if some accounts encounter errors during the offline restore process.*
9. Because some ZCS services are running at this point, type `zmcontrol stop` to stop all services.
10. Remove any old backup sessions because these sessions are no longer valid. Type `rm -rf /opt/zimbra/redolog/* /opt/zimbra/backup/*`
11. To start ZCS, type `zmcontrol start`.
12. Now run a full backup, type `zmbbackup -f -a all`.
13. Remove the firewall rules and allow client access to the new server.

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, type `zmprov ma zimbraAccountStatus active`

Partitions become corrupted

If any partition becomes corrupted, replace the failed disk(s), then 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 mailboxd 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 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.

Important: *The mailboxd 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, type **zmprov md <domain> zimbraDomainStatus maintenance**

2. With the mailboxd service not running, type **zmrestoreoffline**.

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 mailboxd, 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**.

Using snapshots to backup and restore

You can also backup and restore your server using the snapshot feature provided by the storage layer, rather than using Zimbra's backup and restore feature. Using snapshots, you can maintain a standby site to use if your primary site fails at some point of time and reroute users to the standby site to keep operations running.

Snapshots are taken for all volumes of data and are transferred to the standby site periodically. Data volumes that are backed up using snapshots include mysql, blobs, lucene index, and redologs.

When the primary site is down, the **zmplayredo** command is used

- to bring consistency to the snapshots
- to reapply any changes in data to minimize data loss across volumes

Example

There are four volumes of data:

- Mysql
- Blob
- Lucene index
- Redologs

Sets of snapshots are taken every hour and transferred to the remote standby site. However, all snapshots are not taken at one instant and could be a second to a minute apart from each other. Also, snapshots of redologs may be taken more frequently. The sequence of events could look like:

8:00:00 - snapshot mysql

8:00:01 - snapshot blob

8:00:02 - snapshot index

8:00:03 - snapshot redolog

8:05:00 - transfer the snapshot set to remote site completed

8:15:00 - snapshot redolog

8:15:05 - transfer of redolog snapshot to remote site completed

8:30:00 - snapshot redolog

8:30:05 - transfer of redolog snapshot to remote site completed

8:35:00 - primary site fails

On the remote site, there are snapshots from the 8:00 set of data as well as subsequent snapshots of the redologs. They all have to be brought together so that the most recent information is available on the standby site once users are rerouted to it.

You can now run the **zmpplayredo** command to replay changes from 8:00:00.

zmpplayredo --fromTime '2008/10/17 08:00:00:000'

All data is brought forward to the current time and the standby site is set up and running. Data from 8:30:00 to 8:35:00 is lost but that is expected when the restore process is being carried out.

Chapter 17 Zimbra Archiving and Discovery

Zimbra Archiving and Discovery is an optional feature for the Zimbra Collaboration Suite (ZCS) Network Edition that offers

- Archiving, the ability to archive messages that were delivered to or sent by ZCS
- Discovery, the ability to search across mailboxes

The prerequisite to enabling archiving is the installation and configuration of the Zimbra Archiving package on at least one mailbox server. The installation of this package provides the ZCS discovery (also known as cross mailbox) search tool and sets the attributes that allow archiving to be enabled on the Zimbra MTAs.

This chapter covers the following:

- Installing and configuring archiving and discovery in single-server and in a multi-server deployment, as a dedicated archive server.
- Creating archive mailboxes
- Performing discovery searches

Archiving is configured on a per account basis. When archiving is enabled for an account, any email from or to that account is forked at the MTA, and a copy of the message is delivered to a predefined archive mailbox. The archiving process is transparent to account users.

Discovery allows you to conduct a search for email messages across live and archived mailboxes and copy the results to a target specified mailbox.

How Archiving Works

When a message is sent or received by a user, the message is always routed through the Postfix MTA. The Postfix MTA allows integrating software that can perform actions on messages that are in flight. When archiving is enabled for the sender or the recipient of messages, Zimbra Archiving integrates with an MTA hook and the Amavisd-New utility to fork a copy of the message.

The “**does recipient or sender have archiving enabled**” check is performed on the SMTP standard envelope and not on the From or To/Cc headers. Since

checks are performed on the envelope, Bcc copies and messages sent to distribution lists are captured.

For example, if User A sends a message to User B, and if User B has archiving enabled, the MTA delivers two messages — one to User B's mailbox and one to User B's archive mailbox. The message received in User B's mailbox looks normal, as shown in the following example:

```
Received: from localhost (localhost.localdomain
[127.0.0.1])...
From: userA@example.com
To:userB@example.com
Subject: New License Key
Message-ID: <015f01c717fe$70f042d1$b1d6f61d@thom>
Date: Mon, 04 Nov 2008 23:48:18 -0000

Hi B,
Can you send me the license key for the software
again?
Thanks, A
```

The message received in User B's archive mailbox contains additional **X-Envelope-From** and **X-Envelope-To** headers. These headers show the real email address the message was sent from and each of the email addresses that the message was sent to.

```
Received: from localhost (localhost.localdomain
[127.0.0.1])...
From: userA@example.com
To:userB@example.com
Subject: New License Key
Message-ID: <015f01c717fe$70f042d1$b1d6f61d@thom>
X-Envelope-From: userA@example.com
X-Envelope-To: userB@example.com
Date: Mon, 04 Nov 2008 23:48:18 -0000

Hi B,
Can you send me the license key for the software again?
Thanks, A
```

Zimbra archiving can be set up to create archiving accounts that are maintained within ZCS or can be set up to work with third-party archiving systems using SMTP forwarding to forward messages to a third-party archive server. For third-party archiving, ZCS is configured to act as the forwarding agent.

How Discovery Works

The discovery feature of Archiving and Discovery is used to search across live* and archive mailboxes for email messages and attachments. The discovery tool can be run from the administration console and the results are copied to a target mailbox that you specify.

* A live mailbox is an account on the system other than archive accounts and system accounts.

Note: *Discovery is also referred to as cross mailbox search.*

You can search outgoing and incoming email by date, from, to, cc, subject, keywords, and attachments. The advanced search feature can be used to quickly create a query to search by name, dates and time ranges, distribution list, aliases.

Target mailboxes are created to receive discovery search results. You can organize your search results by creating different target mailboxes or by creating individual folders within a target mailbox for each search you run. **X-zimbra-Source** header information is added to each message header that is copied to the targeted mailbox. This header label includes the account ID, the account name, and the server that the account resides on.

You can see the results of the search by logging on to the target mailbox address.

Installing Archiving Package as an Update to ZCS

The Zimbra-archiving package can be installed and configured on an existing single-server deployment or on a multi-server deployment as an upgrade to ZCS, and archiving is enabled on each MTA in your ZCS deployment.

If the mailbox server and the MTA server reside on the same node, you configure and enable archiving as a single upgrade process. If your mailbox and MTA servers are on separate nodes, the zimbra-archive package is installed first on at least one mailbox server and then the archiving component is enabled on each MTA in the deployment.

Installing zimbra-archiving in a Single-Server Environment

In this upgrade process, it is assumed that the LDAP, MTA, mailstore and archiving servers are on the same node. To install archiving in a single-server deployment, you have to:

- Upgrade the server installation and install the zimbra-archiving package.
- Enable archiving on the MTA server using the CLI commands.

Follow these steps to install and enable archiving on a single-server:

1. Refer to the Single-server Quick Start guide to open an SSH connection to the ZCS server. Log on to the server as **root** and run the **.install.sh** command to begin the upgrade process.
2. Accept the license agreement. The server then checks for existing packages and asks if you wish to upgrade. Type **Yes** to run the upgrade.
3. Type **Yes** for zimbra-archiving when presented with the packages to be installed.

The upgrade process begins and the archiving package is installed. At this point the Discovery feature is installed and can be used.

4. To enable archiving, switch user to **zimbra** and enable archiving on the MTA server.

- a. To enable archiving type:

```
zmprov ms <zmhostname> +zimbraServiceEnabled archiving
```

- b. The server must be restarted. Type:

```
zmcontrol stop
```

```
zmcontrol start
```

Installing zimbra-archiving in a Multi-Server Environment

The following upgrade scenario assumes that the LDAP server, MTA server(s), and mailstore server(s) have ZCS installed correctly. You are now adding a new server that will be dedicated as a archiving server to this environment.

When you add archiving and discovery to an existing ZCS multi-server environment as a dedicated archiving server, you install the zimbra-archiving package and the zimbra-store package on the dedicated server, and you enable archiving on each MTA server in your deployment.

Before beginning the install process, note down the following information. You need this when you install the archiving server. Run the **zmlocalconfig -s** command to find the information.

LDAP Admin Password _____

LDAP Hostname _____

LDAP Port _____

Refer to the Multiple-Server Installation chapter in the Multi-Server Install Guide for detailed steps on installing the packages.

1. Open an SSH connection to the mailbox server that is being configured for archiving. Log on to the server as **root** and unpack the Zimbra software. Run the **.install.sh** command to begin the install process.
2. Type **y** and press **Enter** to install the following packages:
 - zimbra-store

- zimbra-archiving

The zimbra-core package is installed by default.

```
Select the packages to install

Install zimbra-ldap [Y] N
Install zimbra-logger [Y] N
Install zimbra-mta [Y] N
Install zimbra-snmp [Y] N
Install zimbra-store [Y] Y
Install zimbra-apache [Y] N
Install zimbra-spell [Y] N
Install zimbra-proxy [N] N
Install zimbra-archiving [N] Y
Install zimbra-convertd [N] N

Installing:
  zimbra-core
  zimbra-store
  zimbra-archiving

This system will be modified. Continue [N] Y
```

3. Type **y** and press **Enter** to modify the system.
4. The Main menu displays the default entries for the Zimbra component you are installing. To expand the menu, type **x** and press **Enter**.
5. Select the **Common Configuration** menu and configure the LDAP Hostname, LDAP password, and LDAP port.
6. Select the **zimbra-store** menu and configure the Admin password and the License file location.

Complete the installation process following the steps under Installing Zimbra Mailbox Server. At this point the Discovery feature is installed and can be used.

Enable archiving on each MTA

After the archiving package has been installed on the archiving server, you must enable archiving on each MTA server in the deployment. Complete the following on each MTA server. This is run as zimbra.

1. Modify the MTA server to enable archiving, type


```
zmprov ms <zmhostname> zimbraServiceInstalled archiving +zimbraServiceEnabled archiving
```
2. Stop and restart the server. Type


```
zmcontrol stop
zmcontrol start
```

Repeat for MTA server.

Creating Dedicated Archive COS in a Multi-Server Environment

In a multi server deployment with a dedicated archive server, you create a dedicated archive COS for the server. This COS is set up on the archive server as a dedicated host. The server is removed from the COS server pool so that the archive server is not randomly assigned to new accounts.

You can create the COS from the administration console or from the CLI. Attributes can be configured in the COS to set mailbox features, quotas, and password, turn off spam and virus checks and to hide the archive accounts from GAL. In addition to setting these attributes, you remove the archive server from the COS server pool.

Note: These steps to remove the server from the server pool are not done in a single-server deployment. Creating a dedicated archiving COS is a good idea as this makes it easy to create archive mailboxes that are configured the same.

Using the Administration Console

Create a new dedicated COS configured correctly for your archive accounts. To remove the server from the server pool, in the Server Pool tab deselect the archive server.

Using CLI

To obtaining the zimbra-store server ID of the archive server and the server pool, zimbraMailHostPool ID.

1. Look up the server ID for the archive server, type

```
zmprov gs -e <archivestoreservername> zimbraID
```

The archive store server ID is returned.

```
zmprov gs -e local host.com zimbraID
# name example. com
zimbraId: 6515ef25-2d56-4cd7-951c-c922g23d6e8e
```

2. Look up the zimbraMailHostPool ID for the default COS on this server, type

```
zmprov gc default zimbraMailHostPool
```

In this example, the default COS lists three servers, including the archive server.

```
zmprov gc default zimbraMailHostPool
# name default
zimbraMailHostPool: 6515ef25-2d56-4cd7-951c-c922g23d6e8e d6b9a0 266e-46ac-ala5-7391d4763616 d6b9a0 266e-25ca-ala5-7451d4951616
```

3. Removing the archive zimbra-store server ID from the server pool..

```
zmprov mc <cos> zimbraMailHostPool <archiveserver ID>
```

```
zmprov mc default zimbraMailHostPool 6515ef25-2d56-4cd7-951c-  
c922g23d6e8e
```

Repeat this process to remove the archive store server ID from the **zimbraMailHostPool** in all existing COS

- Now create an COS for the archive server. Set the **zimbraMailHostPool** on a single Zimbra server to only be the archive server ID.

```
zmprov cc <archivingCOSName> zimbraMailHostPool <archive server ID>
```

```
zmprov cc archiving zimbraMailHostPool 6515ef25-2d56-4cd7-951c-c922g23d6e8e
```

Now when you create an archive account and use the archive COS, the account is automatically created on the archive server.

Administering the archive server

*The **amavisd-new** server process controls account archiving as well as antivirus and antispam processes. The **zmarchivectl** command can be used to start, stop, restart or obtain the status of the **amavisd-new** server process that controls account archiving. Caution should be taken when starting or stopping the archiving process as it is a shared server process between archiving, antivirus, and antispam processes. Performing actions on any of them affect any of the other services that may be enabled in your deployment.*

If you want to disable archiving and not antivirus, or antispam services, disable the respective service either through the CLI or through the administration console.

To disable archiving using CLI, type

```
zmprov ms <zmhostname> -zimbraServiceEnabled archiving
```

Archiving Attribute

Four attributes are related to the archive feature. Two that configure a mailbox and two template attributes to construct the archive account names.

Attributes configured on users' account

To set up archiving for a mailbox two attributes are configured on the primary user's mailbox. One attributed enables archiving and the second shows where messages are being archived.

- **amavisArchiveQuarantineTo** — The current archives address. If this is unset, archiving is not enabled.

- **zimbraArchiveAccount** — Any previous and current archive addresses that this mailbox was archived to.

Archive Account Name Templates

In order to construct archive account names, Zimbra supports two attributes that establish the archive naming conventions. These attributes are used to create and manage archive accounts naming scheme. You can set up these attributes either by COS or by account. For COS, these attributes can be changed using **zmprov mc**. For accounts, use **zmprov ma**.

- **zimbraArchiveAccountDateTemplate**. This attribute sets the date format used in the name template. The default is yyyyMMdd. Adding the date to the account name makes it easier to roll off older data from the system to backups.
- **zimbraArchiveAccountNameTemplate**. This attribute sets up how the archive mailbox name is created. The default value is **\${user}-\${date}@\${domain}.archive**. The archive account address would be like this example: **user-20070510@example.com.archive**. If you change the default value, you must use syntax that creates a valid email address. We recommend that you add **.archive** to all archive accounts to create archive mailboxes in a non-routable domain to prevent spoofing of the archives.

Creating Archive Mailboxes

Archive mailboxes are created using the CLI, **zmarchiveconfig**. The following archiving scenarios enable archiving for an account:

- Create an archive mailboxes with an assigned COS
- Create an archive mailboxes with no COS assigned
- Archive forwarding to a third-party archiving server

Note: *Archive accounts you create are counted against the number of accounts you can create based on your Zimbra license. Archive mailboxes are listed in the administration console along with the live accounts. Archive forwarding does not count against the Zimbra license.*

Create an archive mailbox and assign a COS

1. Log on as ZCS.
2. Type **zmarchiveconfig enable <account@example.com> archive-cos <cosname>**

Archive accounts are created based on the Zimbra Archive name templates.

- The attribute **zimbralsSystemResource** is added to the archive account and set to TRUE.
- The archive account is displayed in the administration console.
- When a message is received in a mailbox with archiving enabled, a copy of the message is sent to the archive mailbox..

Create an archive mailbox with no COS or password

If the archive account is not assigned a COS, the following settings are set by default.

- Mailbox quota is set to 0, unlimited quota.
- Spam and virus checks are disabled.
- Hide in GAL is enabled, so the archive account does not display in the GAL

To create an account:

1. Log on as ZCS
2. Type `zmarchiveconfig enable user@example.com` .

Enable archive forwarding to a third-party archiving server

If the archive account is not maintained within ZCS, you do not need to set a password, COS or other attributes as no archive account is created in ZCS.

1. Log on as zimbra.
2. Type `zmarchiveconfig enable <account@example.com> archive-address account-archive@offsiteserver.com archive-create false` .

Searching Across Mailboxes

When the archiving and discovery feature is installed, you can search across mailboxes using the discovery tool either from the administration console or through the command line interface.

Note: *You do not need to have any archive mailboxes configured to search across mailboxes, the package just needs to be installed.*

You can assign a user to run the mailbox searches from the administration console by creating a delegated administrator with rights to access the mailbox search tool. See Chapter 9, Delegated Administration.

Cross Mailbox Search from the Administration Console

The discovery tool, **Search Mail**, is added to **Tools** on the administration console Navigation pane when the archiving package is added. When you click **Search Mail**, a search page opens, allowing you to configure the following information:

- **Server name.** The server name of the to be searched.
- **Target mailbox and folders.** One target mailbox and folder is created automatically. You can use this mailbox for all your search results and create new folders for each search, or you can create a new target mailbox for each separate search.

Note: A target mailbox is like any other mailbox and can have any features or preferences that are defined by the COS or by account. Target mailboxes are listed in the administration console Accounts list. You may want to give the target mailboxes account names that identifies them as target mailboxes for cross-mailbox searches and configure a COS specific for target mailboxes to be able to manage access. For example: `CMS_user1.example.com`. CMS is a prefix that means **cross mailbox search**. With this practice, all target mailboxes are listed together

- Limit the number of messages returned by the search.
- You can select to send an email notification when the search is completed. The email notification includes the search task ID and status on the subject line and you can specify the type of to include in the message, such as the number of messages found, the list of addresses resulting from the search and the search query used.
- Select which mailboxes to search: all archive mailboxes, all live mailboxes or selected mailboxes. When you check **Select accounts to search**, you select which account addresses to search.
- **Create the search query.** You can search outgoing and incoming email by date, from, to, cc, subject, keywords, and attachments. Advanced Search can be used to quickly create a query to search by name, dates and time ranges, distribution list, aliases. For a list of the search grammar that can be used see the [Zimbra Wiki](#), [Search Tips](#) article.

When searching archive messages, you can search by the envelope address using the **envfrom** and **envto** query language extensions.

As the search is being run, the Search Mailbox Content pane lists the search and the status. You can click **Refresh** to update this page.

You should delete the search task when it is completed as it occupies server memory. **Note:** When the server is restarted the searches listed in the Search Mailbox Content pane are deleted.

When you use the discovery feature in the administration console, the tool makes copies of messages in the target mailbox you create. The messages occupy server space, increasing the size of your server. You may want to delete these messages from the target mailbox when they are no longer needed.

Search using the Command Line Interface

Use the CLI command, **zmarchivesearch** to run the cross mailbox search from the command line.

For more information about **zmarchivesearch**, refer Appendix A, Command-Line Utilities.

Chapter 18 Changing ZWC Theme Colors and Logo

You can change the logo and base colors of the Zimbra Web Client themes without having to customize individual ZCS themes. This can be done either from the CLI or from the administration console.

Changing the base colors for themes and adding a custom logo can be configured as a global setting or as a domain setting. When the global settings are changed, the changes apply to themes on all servers. When the domain settings are changed, the base color and logos for themes on the domain are changed.

If global settings and domain-level settings for theme base colors or logos are not the same, the domain values are displayed for the domain.

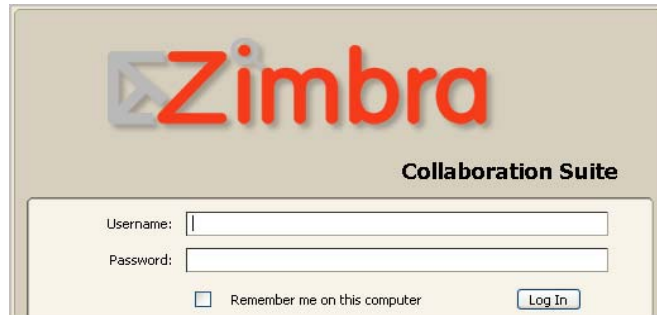
Important: *If the logo and base colors are customized in multi-domain ZCS environments, you must set a virtual host as the base color and logo attributes are displayed based on the Host header sent by the browser. See “Virtual Hosts” on page 111.*

Note: *A number of Zimbra themes are included with ZCS. Some of these themes, such as lemongrass, Hot Rod, Waves and Yahoo, have been designed with graphics or color codes that are not changed, when you change the base color. You may want to disable those themes from user’s Theme preferences selection.*

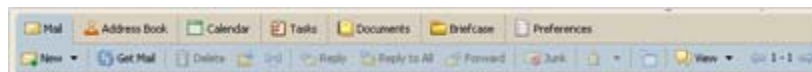
Customizing Base Theme Colors

The following base colors in ZWC themes can be changed:

- The primary background color displayed in the client. This color is the background of the page. Variants of the color are used for buttons, background color of the Content and Navigation panes, tabs, and selection highlight. In the following image, the background color displays with the logo, the variant of the background color displays in the login area.



- The secondary color is the color used for the toolbar, selection headers in the Navigation pane, and for a selected tab. In the following image, The selected tab, **Mail**, and the toolbar are displayed in the secondary color.



- The selection color is the color displayed for a selected item such as a message, the clicked item from a right-click or other drop-down menu selection.



- The foreground color is the text color displayed. The default text color is black. The text color usually does not need to be changed.

Replacing the ZWC Logo

You can replace the Zimbra log with your company's logo globally or per domain.

Note: License Policy for Logo Replacement

The Zimbra Public License does not allow removing the Zimbra logo in the Zimbra Web Client. Only Network Edition customers can replace Zimbra logos that display in the Zimbra Web Client. Therefore, only customers of the Network Edition should use these instructions. Additional information about the license usage can be found at <http://www.zimbra.com/license/index.html>.

Graphics to Replace

The following Zimbra logo files can be changed. Your logos must be the same size as the specified here or the image may not display correctly. These graphic files can be saved on another server or in a directory that is not overwritten when ZCS is upgraded.

- Company logo that displays on the login and splash screens for ZWC and the ZCS administration console. The dimension of the graphic must be exactly 450 x 100
- Small company logo in the upper-left of the ZWC application and the administration console. The dimension of the graphic must be exactly 120 x 35.
- Company Web address that links from the company logos

Graphics not replaced

The Zimbra icon that displays in the Advanced search toolbar and the favicon.ico that displays in the URL browser address field cannot be changed at this time.

Using Command Line Interface to

Changing the ZWC theme base colors and logos is performed from the command line using the **zmprov** command.

Change Theme Colors

The color code is entered as a six-digit hexadecimal code.

Attributes

The following attributes are configured either as a global config setting or as a domain setting:

- **zimbraSkinBackgroundColor.** Enter the hex color number for the primary background color displayed in the client.
- **zimbraSkinSecondaryColor.** Enter the hex color number for the toolbar and selected tabs.
- **zimbraSkinSelectionColor.** Enter the hex color number for the color of the selected item.
- **zimbraSkinForegroundColor.** Enter the hex color number for the text. This usually does not need to be changed as the default is black.

How to change base colors for themes

Before you begin, identify the six-digit hexadecimal base color values for the various elements you are changing. The commands are entered as:

- For Global:
zmprov modifyConfig <attribute-name> ["#HEX_6digit_colorcode"]
- For Domain:
zmprov modifyDomain <domain> <attribute-name> ["#HEX_6digit_colorcode"]

To modify a domain

In this example, the following base colors are being changed:

- Background color to Coral, #ff7F50
- Secondary color to turquoise, #ADEAEA
- Selection color to yellow, #FFFF00.

1. As the Zimbra user, type the following

```
zmprov modifyDomain domainexample.com zimbraSkinBackgroundColor  
"#FF7F50" zimbraSkinSecondaryColor "#ADEAEA" zimbraSkinSelectionColor  
"#FFFF00"
```

The quote marks, "", are required so the use of the # sign does not comment out the text that follows.

2. To apply the changes, type

```
zmmailboxctl
```

ZCS themes for that domain now display these colors.

Add Your Logos

Attributes

You add the company logo information and URL by modifying these attributes:

- **zimbraSkinLogoURL.** Enter the company Web address that you want linked from the logo.
- **zimbraSkinLogoLoginBanner.** Enter the company logo file name that is displayed on the login and splash screens for the ZWC and the ZCS administration console.
- **zimbraSkinLogoAppBanner.** Enter the logo graphic file name for the graphic in the upper-left of the ZWC application and the administration console.

To add logos for a domain

1. As the Zimbra user, type the following

```
zmprov modifyDomain domainexample.com zimbraSkinLogoURL http://  
example.com
```

```
zmprov modifyDomain domainexample.com zimbraSkinLogoLoginBanner  
http://imageserverexample.com/directory/logo_banner_name.png
```

```
zmprov modifyDomain domainexample.com zimbraSkinLogoAppBanner
http://imageserverexample.com/directory/banner_app_logo.png
```

- To apply the changes, type
`zmmailboxdctl`

Examples

Figure 4: Web Client before changing the base colors



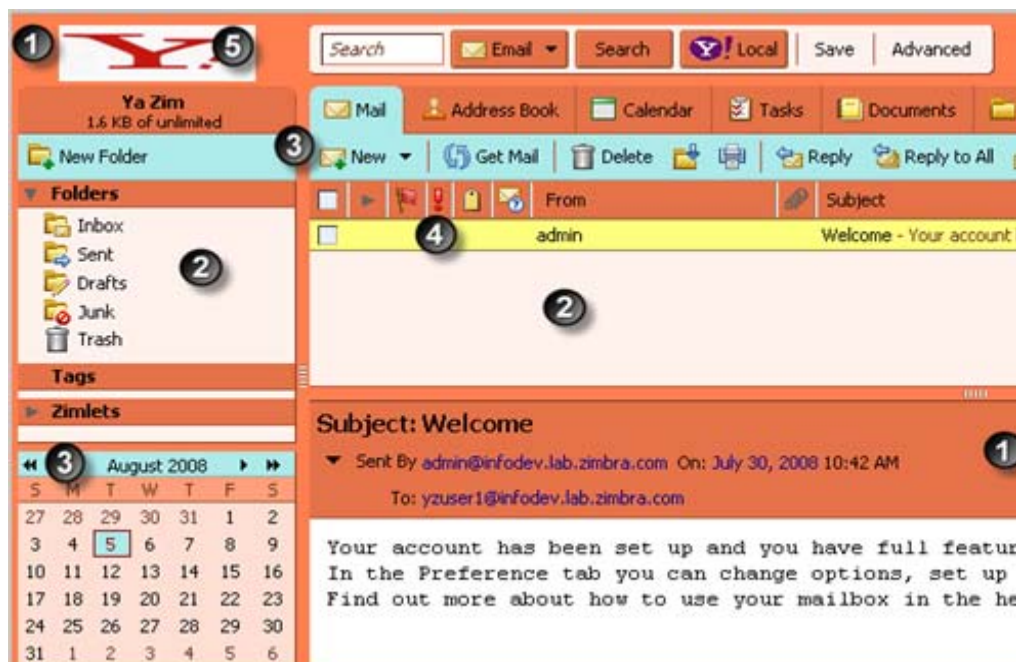
Figure 5: Web Client Login Page after changing base colors



The base color and variations of the base color are displayed.

The Company logo displayed here and on the splash screen is 450 x 100.

Figure 6: Web Client after changing the base colors



- 1 Background color. You select this color. Background for all pages and log in page. This hex code is #FF7F50
- 2 This is the variant color that is automatically set from the background color. This is used for buttons, tabs, and selection highlights. You cannot chose this color.
- 3 Secondary color. You select this color. Displays on toolbar, selection headers, and selected tabs. This hex code is ADEAEA
- 4 Selection color. You select this color. Displays for a selected item such as a message or a drop-down list selection.
- 5 Small company banner logo. The small logo size is 120 x 35. For the Yahoo! theme, the dimension of the logo is 170 x 28. Only one can be set.

Changing Theme Colors and Logo from Administration Console

On the administration console, the Global Settings and the Domains settings include a Themes tabs that can be configured to customize the color scheme and to add a company logo and logo URL. You upload your company logo to be used on the Zimbra Web Client and administration console pages.

Changing Base Theme Colors

You can change the same areas as changed from the CLI. You can either select colors from a color pallet table of defined colors or enter the six-digit hexadecimal color value for an exact color match.

On the Themes tabs, you can select a color from the pallet for each of the following areas.

- Foreground, which is the text color.
- Background, which is the primary background color displayed in the client.
- Secondary, which is the color used for the toolbar, selection headers in the Navigation pane and for selected tabs.
- Selection, which is the color displayed for a selected item such as a message, right-click, or drop down menu selection.

Adding Your Logo

You can replace the Zimbra logo with your company's logo globally or per domain from the Themes tabs. Your logos must be the same size as specified here or the image may not display correctly. The graphic files are saved on another server or in a directory that is not overwritten when ZCS is upgraded.

The Zimlet icon that displays in the Advanced search toolbar and the favicon.ico that displays in the URL browser address field are not changed.

More Documentation

If you are interested in learning more about customizing ZWC colors and

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
- Starting and stopping a service
- Move mailboxes
- Cross mailbox searches
- Installing self-signed certificates
- Local configuration

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

General Tool Information

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

Follow these guidelines when using the commands

- CLI commands are run as the zimbra user, that is **su - zimbra**.
- The actual CLI commands are case-sensitive. You must type them in lower case.
- Press **ENTER** after you type a command.
- Typing the CLI command and then **-h** displays the usage options for the command. Example: **zmprov -h** lists all the options available for the zmprov utility.

- Each operation is invoked through command-line options. Many have a long name and a short name. For example, these two commands are equivalent:

```
zmprov createAccount joe@domain.com test123
```

```
zmprov ca joe@domain.com test123
```

Syntax Conventions

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

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

Location of Command-Line Utilities

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

Zimbra CLI Commands

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

Table 1 zimbra CLI Commands

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

Table 1 zimbra CLI Commands

CLI	Description
zmaccts	Lists the accounts and gives the status of accounts on the domain
zmamavisdctl	Start, stop, restart, or find the status of the Amavis-D New
zmantispamctl	Start, stop, reload, status for anti-spam service
zmantivirusctl	Start, stop, reload, status for the anti-virus service
zmapachectl	Start, stop, reload, or check status of Apache service (for spell check)
zmarchive config	Command to view, modify, or configure archiving
zmarchivectl	Start, stop, reload, status for archiving
zmarchivesearch	Search archives on the account
zmauditswatchctl	Start, stop, restart, reload, status of the auditwatch
zmbbackup	Performs full backups and incremental backups for a designated mail host.
zmbbackupabort	Stops a backup that is in process.
zmbbackupquery	Find a specific full backup set
zmblobchk	Check consistency of the Zimbra blob store
zmcalthk	Check consistency of appointments and attendees in the Zimbra calendar
zmcertmgr	Manage self-signed and commercial certificates
zmclamdctl	Start, stop, or find the status of Clam AV
zmcleaniplanetics	Clean iPlanet ICS calendar files
zmcontrol (Start/Stop Service)	Start, stop, status of the Zimbra servers. Also can use to find the Zimbra version installed.
zmconvertctl	Start, stop, the conversion server or find the status of the converted attachments conversion/indexing
zmdumpenv	General information about the server environment is displayed
zmgsautil	Create, delete the GAL sync account and initiate manual syncs.
zmhostname	Find the hostname of the Zimbra server
zmhsm	Start, stop and status of a HSM session.
zmitemdatafile	Extracts and packs tgz files that ZCS uses for REST import/export
zmjava	Execute Java with Zimbra-specific environment settings
zmldappasswd	Changes the LDAP password

Table 1 zimbra CLI Commands

CLI	Description
zmlicense	View and install your Zimbra license
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
zmloggerhostmap	Used to manually map a DNS hostname to a zmhostname.
zmlogswatchctl	Start, stop, status of the swatch that is monitoring logging
zmmailbox	Performs mailbox management tasks
zmmailboxdctl	Start, stop, reload, or find the status of the mailbox components (mailboxd, MySQL, convert)
zmmailboxmove (Move Mailbox)	Used to move selected mailboxes from one Zimbra server to another.
zmmboxsearch (Cross Mailbox Search)	Search across mailboxes to find messages and attachments
zmmetadump	Support tool that dumps an item's metadata in a human-readable form
zmmtaconfigctl	Start, stop, or find the status of the MTA configuration daemon
zmmtactl	Start, stop, or find the status of the MTA
zmmypasswd	Trace messages
zmmypasswd	Change MySQL passwords
zmmysqlstatus	Status of mailbox SQL instance
zmperditionctl	Start, stop, or find the status of the perdition IMAP proxy
zmplayredo	Performs data restore using backed up snapshots taken periodically. Users who use snapshots to backup and restore their information from a standby site use this command.
zmprov (Provisioning)	Performs all provisioning tasks in Zimbra LDAP, including creating accounts, domains, distribution lists and aliases
zmproxyconfgen	Generates configuration for the nginx proxy
zmproxycctl	Start, stop, restart, and find the status of the IMAP proxy service
zmproxypurge	Purges POP/IMAP routing information from one or more memcached servers

Table 1 zimbra CLI Commands

CLI	Description
zmpython	Ability to write Python scripts that access Zimbra Java libraries. It sets the ZCS class path and starts the Jython interpreter.
zmredodump	Support tool for dumping contents of a redolog file for debugging purposes
zmrestore	Performs full restores and incremental restores for a designated mail host
zmrestoreldap	Restore accounts from the LDAP backup
zmrestoreoffline (Offline Restore)	Performs full restore when the Zimbra server (i.e., the mailboxd process) is down
zmsaslauthdctl	Start, stop, or find the status of saslauthd (authentication)
zmschedulebackup	Schedule backups and add the command to your cron table
zmshutil	Used for other zm scripts, do not use
zmskindeploy	Deploy skins for accounts from the command line
zmsoap	Print mail, account, and admin information in the SOAP format
zmspellctl	Start, stop, or find the status of the spell check server
zmsshkeygen	Generate Zimbra's SSH encryption keys
zmstat-chart	Generate charts from zmstat data collected in a directory
zmstat-chart-config	Generate an .xml file with data included from the account setup
zmstat-chart-config	Outputs an XML configuration that describes the current state of the data gathered from zmstat-chart to generate charts on the administration console.
zmstatctl	Start, stop, check status, or rotate logs of zmstat data collectors
zmstorectl	Start, stop, or find the status of Zimbra store services
zmwatchctl	Start, stop, or find the status of the Swatch process, which is used in monitoring
zmsyslogsetup	Used to setup system log config file
zmthrdump	Initiate a thread dump and save the data to a file with a timestamp
zmtlctl	Set the Web server mode to the communication protocol options: HTTP, HTTPS or mixed

Table 1 zimbra CLI Commands

CLI	Description
zmtrainsa	Used to train the anti-spam filter to recognize what is spam or ham
zmtzupdate	Provides mechanism to process timezone changes from the command line
zmupdateauthkeys	Used to fetch the ssh encryption keys created by zmsshkeygen
zmvolume	Manage storage volumes on your Zimbra Mailbox server
zmzimletctl	Deploy and configure Zimlets

Using non-ASCII Characters in CLIs

If you use non-ASCII characters in the CLI, in order for the characters to display correctly, you must change this setting to the desired UTF-8 before running the CLI command. To change this, type

```
export LC_All=<UTF_locale>
```

Important: The default locale on the zimbra user system account is **LANG=C**. This setting is necessary for starting ZCS services. Changing the default LANG=C setting may cause performance issues with amavisd-new and the IM services may fail to start.

zmprov (Provisioning)

The **zmprov** tool performs all provisioning tasks in Zimbra LDAP, including creating accounts, aliases, domains, COS, 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 "blue" to user 1 and would not change the value of any other instances of that attribute.

```
zmprov ma user1 +zimbraZimletUserProperties
"com_company_testing:favoriteColor:blue"
```

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
-L	--log property file	log 4j property file, valid only with -l
-a	--account {name}	account name to auth as
-p	--password {pass}	password for account
-P	--passfile {file}	read password from file
-z	--zadmin	use Zimbra admin name/password from localconfig for admin/password
-y	--authtoken (authtoken)	use auth token string (has to be in JSON format) from command line
-Y	--authtoken (authtoken file)	use auth token string (has to be in JSON format) from command line
-v	--verbose	verbose mode (dumps full exception stack trace)
-d/	--debug	debug mode (dumps SOAP messages)
-m	--master	use LDAP master. This only valid with -l

The commands in the following table are divided into the 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		
addAccountAlias	aaa	{name@domain id adminName} {alias@domain} zmprov aaa joe@domain.com joe.smith@engr.domain.com
checkPasswordStrength	cps	Syntax: {name@domain id} {password} Note: This command does not check the password age or history. zmprov cps joe@domain.com test123
createAccount	ca	Syntax: {name@domain} {password} [attribute1 value1 etc] Type on one line. zmprov ca joe@domain.com test123 displayName JSmith
createDataSource	cds	{name@domain} {ds-type} {ds-name} [attr1 value1 [attr2 value2...]]
createIdentity	cid	{name@domain} {identity-name} [attr1 value1 [attr2 value2...]]
createSignature	csig	{name@domain} {signature-name} [attr1 value1 [attr2 value2...]]
deleteAccount	da	Syntax: {name@domain id adminName} zmprov da joe@domain.com
deleteDataSource	dds	{name@domain id} {ds-name ds-id}
deleteIdentity	did	{name@domain id} {identity-name}
deleteSignature	dsig	{name@domain id} {signature-name}
getAccount	ga	Syntax: {name@domain id adminName} zmprov ga joe@domain.com
getAccountMembership	gam	{name@domain id}
getAllAccounts	gaa	Syntax: [-v] [{domain}] zmprov -l gaa zmprov gaa -v domain.com

Long Name	Short Name	Syntax, Example, and Notes
getAllAdminAccounts	gaaa	Syntax: gaaa zmprov gaaa
getDataSources	gds	{name@domain id} [arg 1 [arg 2...]]
getIdentities	gid	{name@domain id} [arg 1 [arg 2...]]
getSignatures	gsig	{name@domain id} [arg 1 [arg 2...]]
modifyAccount	ma	{name@domain id adminName} [attribute1 value1 etc] zmprov ma joe@domain.com zimbraAccountStatus maintenance
modifyDataSource	mds	{name@domain id} {ds-name ds-id} [attr 1 value 1 [attr2 value 2...]]
modifyIdentity	mid	{name@domain id} {identity-name} [attr 1 value 1 [attr 2 value 2...]]
modifySignature	msig	{name@domain id} {signature-name signature-id} [attr 1 value 1 [attr 2 value 2...]]
removeAccountAlias	raa	{name@domain id adminName} {alias@domain} zmprov raa joe@domain.com joe.smith@engr.domain.com
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>
setAccountCOS	sac	{name@domain id adminName} {cos- name cos-id} zmprov sac joe@domain.com FieldTechnician

Long Name	Short Name	Syntax, Example, and Notes
setPassword	sp	{name@domain id adminName} {password} Note: Passwords cannot include accented characters in the string. Example of accented characters that cannot be used: ã, é, í, ú, ü, ñ. zmprov sp joe@domain.com test321
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}
searchCalendarResources	scr	[-v] domain attr op value {attr op value...}
Free Busy Commands		
getAllFbp	gafbp	[-v]
getFreebusyQueueInfo	gfbqi	[{provider-name}]
pushFreebusy	pfb	{domain account-id} [account-id...]
Domain Provisioning Commands		
countAccount	cta	{domain id} This lists each COS, the COS ID and the number of accounts assigned to each COS
createAliasDomain	cad	{alias-domain-name} {local-domain-name id} [attr1 value1 [attr2 value2...]]
createDomain	cd	{domain} [attribute1 value1 etc] zmprov cd mktng.domain.com zimbraAuthMech zimbra

Long Name	Short Name	Syntax, Example, and Notes
deleteDomain	dd	{domain id} zmprov dd mktng.domain.com
getDomain	gd	{domain id} zmprov gd mktng.domain.com
getDomainInfo	gdi	name id virtualHostname {value} [attr1 [attr2...]]
getAllDomains	gad	[-v]
modifyDomain	md	{domain id} [attribute1 value1 etc] zmprov md domain.com zimbraGalMaxResults 500 Note: Do not modify zimbraDomainRenameInfo manually. This is automatically updated when a domain is renamed.
renameDomain	rd	{domain id} {newDomain} Note: renameDomain can only be used with “zmprov -l/--ldap”
COS Provisioning Commands		
copyCos	cpc	{src-cos-name id} {dest-cos-name}
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

Long Name	Short Name	Syntax, Example, and Notes
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
getServer	gs	{name id} zmprov gs domain.com
getAllServers	gas	[-v] zmprov gas
getAllReverseProxyBackends	garpb	
modifyServer	ms	{name id} [attribute1 value1 etc] zmprov ms domain.com zimbraVirusDefinitionsUpdateFrequency 2h
getAllReverseProxyURLs	garpu	Used to publish into nginx.conf what servers should be used for reverse proxy lookup.
getAllMtaAuthURLs	gamau	Used to publish into saslauthd.conf what servers should be used for saslauthd.conf MTA auth
getAllMemcachedServers	gamcs	Used to list memcached servers (for nginx use).
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

Long Name	Short Name	Syntax, Example, and Notes
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]
getDistributionListmembership	gdlm	{name@domain id}
getDistributionList	gdl	{list@domain id} zmprov gdl list@domain.com
modifyDistributionList	mdl	{list@domain id} attr1 value1 {attr2 value2...} zmprov md list@domain.com
deleteDistributionList	ddl	(list@domain id)
addDistributionListAlias	adla	{list@domain id} {alias@domain}
removeDistributionListAlias	rdla	{list@domain id} {alias@domain}
renameDistributionList	rdl	{list@domain id} {newName@domain}
zimbra Documents Provisioning Commands (Notebook)		
importNotebook	imprn	{name@domain} {directory} {folder} Before importing files, any file that will become a Documents page (wiki-style page), must be renamed to include the extension ".wiki". If not it is imported as a file, accessed either as an attachment or an image. imprn joe@domain.com /opt/zimbra/wiki/ template template
initNotebook	in	[{name@domain}] in joe@domain.com

Long Name	Short Name	Syntax, Example, and Notes
initDomainNotebook	idn	{domain} [{name@domain}] Creates the domain Documents account idn domain.com domainwiki@domain.com
UpdateTemplates	ut	[-h host] {template-directory}
Mailbox Commands		
getMailboxInfo---	gmi	{account}
getQuotaUsage---	gqu	{server}
reIndexMailbox	rim	{name@domain id} {action} [{reindex-by} {value1} [value2...]]
RecalculateMailboxCounts	rmc	{name@domain id} When unread message count and quota usage are out of sync with the data in the mailbox, use this command to immediately recalculate the mailbox quota usage and unread messages count. <i>Important: Recalculating mailbox quota usage and message count should be schedule to run in off peak hours and used on one mailbox at a time.</i>
selectMailbox	sm	{account-name} [{zmmailbox commands}]
Logs		
addAccount Logger	aal	{name@domain id} {logging-category} {debug info warn error} Creates custom logging for a single account
getAccountLoggers	gal	[-s/--server hostname] {name@domain id} {logging-category} {debug info warn error}
getAllAccountLoggers	gaal	[-s/--server hostname] Shows all individual custom logger account

Long Name	Short Name	Syntax, Example, and Notes
removeAccountLogger	ral	<p><code>[-s/ --server hostname]</code> <code>{name@domain id} {logging-category}</code></p> <p>When <code>name@domain</code> is specified, removes the custom logger created for the account otherwise removes all accounts all account loggers from the system.</p>

See the [zmprov Log Categories on page 245](#) for a list of logging categories.

Search

searchGAL	sg	<p><code>{domain} {name}</code> <code>zmprov sg joe</code></p>
autoCompleteGal	acg	<code>{domain} {name}</code>
searchAccounts	sa	<p><code>[-v] {ldap-query} [limit] [offset] [sortBy {attribute} [sortAscending 0 1] [domain {domain}]</code></p>

Share Provisioning Commands

For a GUI view of results, see Distribution List Shares tab on the administration console

getPublishedDistributionListShareInfo	gpdlsi	<code>{dl-name dl-id} [{owner-name owner-id}]</code>
getShareInfo	gsi	<code>{owner-name owner-id}</code>
publishDistributionListShareInfo	pdlsi	<code>{+ -} {dl-name@domain id} {owner-name owner-id} [{folder-path folder-id}]</code>

Miscellaneous Provisioning Commands

describe	desc	<p><code>[[-v] [-ni] [{entry-type}]] [-a {attribute-name}]</code></p> <p>Prints all attribute names (account, domain, COS, servers, etc.).</p>
generateDomainPreAuthKey	gdpak	<p><code>{domain id}</code></p> <p>Generates a pre-authentication key to enable a trusted third party to authenticate to allow for single-sign on. Used in conjunction with <code>GenerateDomainPreAuth</code>.</p>

Long Name	Short Name	Syntax, Example, and Notes
generateDomainPreAuth	gdpa	{domain id} {name} {name id foreignPrincipal} {timestamp 0} {expires 0} Generates preAuth values for comparison.
syncGal	syg	{domain} [{token}]
flushCache	fc	[skin local account config cos domain server zimlet] [name1 id] Flush cached LDAP entries for a type. See Zimbra Directory Service chapter. Flushing LDAP Cache
getAccountLogger	gal	[-s /--server hostname] {name@domain id}

The following are **zmprov** commands that are specific to Zimbra IMAP/POP proxy.

--getAllReverseProxyURLs	-garpu	Used to publish into nginx.conf the servers that should be used for reverse proxy lookup
--getAllMtaAuthURLs	-gamau	Used to publish into saslauthd.conf the servers that should be used for saslauthd.conf MTA auth
--getAllMemcachedServers	-games	Used to list memcached servers (for Zimbra Proxy use)

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 **zmprov 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.
- To modify the purge interval, set **zimbraMailPurgeSleepInterval** to the duration of time that the server should “sleep” between every two mailboxes. Type:
`zmprov ModifyServer <server-name> zimbraMailPurgeSleepInterval <Xm>`
X is the duration of time between mailbox purges; **m** represents minutes. You could also set **<xh>** for hours.
- Modify **zimbraNewMailNotification** to customize the notification email template. A default email is sent from Postmaster notifying users that they have received mail in another mailbox. To change the template, you modify the receiving mailbox account. The variables are
 - `${SENDER_ADDRESS}`
 - `${RECIPIENT_ADDRESS}`

- `${RECIPIENT_DOMAIN}`
- `${NOTIFICATION_ADDRESSS}`
- `${SUBJECT}`
- `${NEWLINE}`

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

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

zmprov Log Categories

zimbra.account	Account operations
zimbra.acl	ACL operations
zimbra.backup	Backup and restore
zimbra.cache	Inmemory cache operations
zimbra.calendar	Calendar operations
zimbra.dav	DAV operations
zimbra.dbconn	Database connection tracing
zimbra.extensions	Server extension loading
zimbra.filter	Mail filtering
zimbra.gal	GAL operations
zimbra.im	Instant messaging operations
zimbra.imap	IMAP protocol operations
zimbra.index	Index operations
zimbra.io	Filesystem operations
zimbra.ldap	LDAP operations
zimbra.lmtp	LMTP operations (incoming mail)
zimbra.mailbox	General mailbox operations
zimbra.misc	Miscellaneous
zimbra.op	Changes to mailbox state
zimbra.pop	POP protocol operations
zimbra.redolog	Redo log operations
zimbra.security	Security events
zimbra.session	User session tracking
zimbra.smtp	SMTP operations (outgoing mail)
zimbra.soap	SOAP protocol
zimbra.sqltrace	SQL tracing
zimbra.store	Mail store disk operations
zimbra.sync	Sync client operations
zimbra.system	Startup/shutdown and other system messages
zimbra.wiki	Wiki operations
zimbra.zimlet	Zimlet operations

zmaccts

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

Syntax

zmaccts

zmarchive config

This command is used for configuring the archiving mailbox. It has the option of using short commands or full names for commands that lead to the same function being carried out.

Syntax

zmarchiveconfig [args] [cmd] [cmd-args...]

Description

Long Name	Short Name	Description
--help	-h	Displays the usage options for this command
--server	-s	(host)[::(port)] Displays the server hostname and optional port
--account	-a	(name) Returns the value of the account name to be authorized
--ldap	-l	Allows archiving to be provisioned via LDAP
--password	-p	(pass) Returns the password for auth account
--passfile	-P	(file) Allows password to be read from file
--zadmin	-z	Allows use of Zimbra admin/password from local
--debug	-d	Activates debug mode (dumps SOAP messages)
Command in...		

Long Name	Short Name	Description
enable <account>		[archive-address <aaddr> [archive-cos <cos>] [archive-create <TRUE/FALSE>] [archive-password <pa [zimbraAccountAttrName <archive-attr-value>]+
disable <account>		

zmarchivectl

This command is used to start, stop, reload, or check the status of the Zimbra account archive.

Syntax

```
/opt/zimbra/bin/zmarchivectl start|stop|reload|status
```

zmarchivesearch

This command is used to search across account archives. You can search for archives that match specific criteria and save copies to a directory.

Syntax

```
zmarchivesearch {-m <user@domain.com>} {-q <query_string>} [-o <offset>] [-l <limit>] [-d <output_directory>]
```

Description

Long Name	Short Name	Description
--dir	-d	<arg> Directory to write messages to. If none is specified, then only the headers are fetched. Filenames are generated in the form RESULTNUM_ACCOUNT-ID_MAILITEMID
--help	-h	Displays help messages
--limit	-l	<arg> Sets the limit for the number of results returned. The default is 25
--mbox	-m	<arg> Name of archive account to search
--offset	-o	<arg> Specifies where the hit list should begin. The default is 0

Long Name	Short Name	Description
--query	-q	<arg> The query string for archive search
--server	-s	<arg> Mail server hostname. Default is localhost
--verbose	-v	Allows printing of status messages while the search is being executed

Example

This example is to search archives on a specified server and put a copy of the archive in a specified directory.

```
zmarchivesearch -m user1@yourdomain.com -q "in:sent" -o 0 -l 30 -d /var/tmp
```

zmbakup

This tool performs full backups and incremental backups for a designated mail host.

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

Syntax

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

```
zmbakup {-f | -i | del} {-a <arg>} [options]
```

Description

Long Name	Short Name	Description
--account	-a	<arg> Account email addresses separated by white space or all for all accounts. This option is not specified for auto-grouped backups since the system knows which accounts to backup every night.
--debug	-d	Display diagnostics for debugging purposes.
--delete	-del	<arg> Deletes the backups including and prior to the specified label, date (YYYY/MM/DD[-hh:mm:ss]) or period (nn(d m y)).

Long Name	Short Name	Description
--fullBackup	-f	Starts a full backup. In auto-grouped backup mode, this option also copies the redologs since the last backup (which is the main function of an incremental backup).
--help	-h	Displays the usage options for this command.
--incrementalBackup	-i	Starts an incremental backup. This option is not available in the auto-grouped backup mode
--server	-s	<arg> Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name.
--sync	-sync	Runs full backup synchronously.
--target	-t	<arg> Specifies the target backup location. The default is <zimbra_home>/backup.
--zip	-z	Zips email blobs in backup
--zipstore		Stores blobs uncompressed when --zip option is used.

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 -a user1@domain.com -s server1`
- Perform incremental backup of **user1**'s mailbox on **server1**
`zmbbackup -i -a user1@domain.com -s server1`

zmblobchk

Checks the consistency of the Zimbra blob store (/opt/zimbra/store). This command checks and records notes of files without matching database metadata. It also checks to make sure that size information is correct for the files.

Syntax

zmblobchk [options] start

The start command is required to avoid unintentionally running a blob check. The ID values are separated by commas.

Description

Long Name	Short Name	Description
--export-dir		<path> Target directory for database export files.
--help	-h	Displays help messages
--mailboxes	-m	<mailbox-ids> Specify which mailboxes to check. If not specified, check all mailboxes.
--missing-blob-delete-item		Delete any items that have a missing blob.
--no-export		Delete items without exporting
--skip-size-check		Skip blob size check
--unexpected-blob-list		<path> Write the paths of any unexpected blobs to a file
--verbose	-v	Display verbose output; display stack trace on error
--volumes		<volume-ids> Specify which volumes to check. If not specified, check all volumes

zmcalkchk

This command checks the consistency of appointments on the Zimbra calendar and sends an email notification regarding inconsistencies. For example, it checks if all attendees and organizers of an event on the calendar agree on start/stop times and occurrences of a meeting.

See the output of **zmmailbox help appointment** for details on time-specs.

Syntax

```
zmcalchk [-d] [-n <type>] <user> <start-time-spec> <end-time-spec>
```

Description

Short Name	Description
-d	Debugs verbose details
-m	Allows the user to specify the maximum number of attendees to check. The default value is 50.
-n	-n none user organizer attendee all Send email notifications to selected users if they are out of sync for an appointment

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 Saturday at 1:00 a.m. (0 1 * * 6)
- Incremental backup, Sunday through Friday at 1:00 a.m. (0 1 * * 0-5)

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, or use names)

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}[f|i|d] ["schedule"]
```

Description

Name	Command Name	Description
help	-h	Displays the usage options for this command.
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.
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.
compress	-z	Compress email blobs with zip
target	-t	Can be used only to designate a full back target location. The default is /opt/zimbra/backup. <i>Note: You cannot designate a target for incremental backups. If a target (-t) location is added for incremental scheduled backups, it is ignored.</i>
account	-a	Account specific. The default is all accounts.
Incremental Backup	i	<time specifier> Incremental backup. Incremental backup is not used with the auto-grouped backup mode.
Full Backup	f	Full backup
Delete	d <arg>	Delete backups

Examples

- To schedule the default full and incremental backup
`zmschedulebackup -D`
- To replace the existing schedule with a new schedule
`zmschedulebackup -R f ["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

This command can be used to stop a backup process. Before you can abort an account you must know its backup label. This label is displayed after you start the backup procedure. If you do not know the label, use **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 [options]`

Description

Long Name	Short Name	Description
<code>--debug</code>	<code>-d</code>	Display diagnostics for debugging purposes
<code>--help</code>	<code>-h</code>	Displays the usage options for this command
<code>--label</code>	<code>-lb</code>	<arg> Label of the full backup to be aborted. Use the zmbakupquery , to find the label name.
<code>--restore</code>	<code>-r</code>	Abort the restore in process
<code>--server</code>	<code>-s</code>	<arg> 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>	<arg> Specifies the target backup location. The default is <zimbra_home>/backup.

zmbackupquery

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

To find out the best full backup to use as the basis for point-in-time restore of an account, run a command like this:

```
$ zmbackupquery -a <account email> --type full --to <restore-to time>
```

Syntax

zmbackupquery [options]

Description

Long Name	Short Name	Description
--account	-a	<arg> Account email addresses separated by white space or all for all accounts
--debug	-d	Display diagnostics for debugging purposes
--help	-h	Displays the usage options for this command
--fromt		<arg> List backups whose start date/time is at or after the date/time specified here.
--label	-lb	<arg> The label of the full backup session to query. An example of a label is backup200507121559510 .
--server	-s	<arg> 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	<arg> Specifies the backup target location (The default is <zimbra_home>/backup.)
--to		<arg> List backups whose start date/time is at or before the date/time specified here.
--type		<arg> Backup set type to query. "full" or "incremental", both are queried if one is not specified.
--verbose	-v	Returns detailed status information

Specify date/time in one of these formats:

```
2008/12/16 12:19:23
2008/12/16 12:19:23 257
2008/12/16 12:19:23.257
2008/12/16-12:19:23-257
2008/12/16-12:19:23
20081216.121923.257
20081216.121923
20081216121923257
20081216121923
```

Specify year, month, date, hour, minute, second, and optionally millisecond.

Month/date/hour/minute/second are 0-padded to 2 digits, millisecond to 3 digits.

Hour must be specified in 24-hour format, and time is in local time zone.

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, **-rf** is the same as **--restorefullBackupOnly**.

Syntax

zmrestore [options]

Description

Long Name	Short Name	Description
--account	-a	<arg> Specifies the account email addresses. Separate accounts with a blank space or type all to restore all accounts.
--backedupRedologs 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

Long Name	Short Name	Description
--createAccount	-ca	Restores accounts to target accounts whose names are prepended with prefix. (Can only be used in commands that use the -pre option.)
--debug	-d	Display diagnostics for debugging purposes
--help	-h	Displays the usage options for this command
--ignoreRedoErrors		If true, ignore all errors during redo log replay
--label	-lb	<arg> The label of the full backup to restore. Restores to the latest full backup if this is omitted.
--prefix	-pre	<arg> The prefix to pre-pend to the original account names
--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
--restorefullBackup Only	-rf	Restores to the full backup only, not any incremental backups since that backup.
--server	-s	<arg> Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name.
--skipDeletes		If true, do not execute delete operation during redo log replay
--skipDeletedAccounts		Do not restore if named accounts were deleted or did not exist at backup time. (This option is always enabled with -a all)
--systemData	-sys	Restores global tables and local config
--target	-t	<arg> Specifies the backup target location. The default is <zimbra_home>/backup.

Examples

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

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

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

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

- Create a new account from a backup of the target account. The name of the new account will be new_user1@domain.com.

```
zmrestore -a user1@domain.com -ca -pre new_
```

zmrestoreoffline (Offline Restore)

This tool is run when the Zimbra server (i.e., the mailbox 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]

Description

Long Name	Short Name	Description
--account	-a	<arg> Specifies the account email addresses. Separate accounts with a blank space or state all for restoring all accounts. Required.
--backedupRedologsOnly	-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
--createAccount	-ca	Restores accounts to new target accounts whose names are pre-pended with prefix
--debug	-d	Display diagnostics for debugging purposes
--help	-h	Displays the usage options for this command
--ignoreRedoErrors		If true, ignore all errors during redo log replay

Long Name	Short Name	Description
--label	-lb	<arg> The label of the full backup to restore. Type this label to specify a backup file other than the latest.
--prefix	-pre	<prefix> The prefix to pre-pend to the original account names.
--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
-- restoreFullBackup Only	-rf	Restores to the full backup only, not any incremental backups since that backup.
--server	-s	<arg> 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.
-- 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)
--systemData	-sys	Restores global tables and local config.
--target	-t	<arg> Specifies the backup target location. The default is <zimbra_home>/backup.

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 <arg>} {-t <arg>} [options]
```

Description

Short Name	Description
-lb	<arg> Session label to restore from. For example, full200612291821113.
-t	<arg> Specifies the backup target location. The default is /opt/zimbra/backup.
-lbs	Lists all session labels in backup
-l	Lists accounts in file.
-a	<arg> 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 ZCS 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.

Long Name	Short Name	Description
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

```
zmmailboxmove {-a <arg>} {-t <arg>|-po} [options]
```

Description

Long Name	Short Name	Description
--account	-a	<arg> 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	-s	<arg> Mail server hostname. The default is the localhost. Server where the --account mailbox is located.
--targetServer	-t	<arg> Server where mailbox is moved to Use -t option to move a mailbox from the current server to the new server specified by the option. .

Long Name	Short Name	Description
<code>--authtokenfile</code>	<code>-Y</code>	Use auth token string (has to be in JSON format) from command line
<code>--authtoken</code>	<code>-y</code>	Use auth token string (has to be in JSON format from command line

Example

In these examples, two separate command lines are used to move the mailbox and to purge the old mailbox. This is because `-t` and `-po` are mutually exclusive.

To move a mailbox from the default server to the target server:

```
zmmailboxmove -a user1@domain.com -t server2.domain.com
```

To move a mailbox from the default server to the target server, while overwriting any existing mailbox for the account on the target server:

```
zmmailboxmove -a user1@domain.com -t server2.domain.com -ow
```

To purge an old mailbox from the default server, after checking that the contents of the mailbox were successfully moved to the target server:

```
zmmailboxmove -a user1@domain.com -po
```

zmmailboxsearch (Cross Mailbox Search)

The CLI command **zmmailboxsearch** is 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 {-m <arg>} {-q <arg>} [-o <arg>] [-l <arg>] [-d <arg>] [options]
```

Description

Long Name	Short Name	Description
<code>--dir</code>	<code>-d</code>	<code><arg></code> 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 .
<code>--help</code>	<code>-h</code>	Displays help information
<code>--limit</code>	<code>-l</code>	Sets the limit for the number of results returned. The default is 25.

Long Name	Short Name	Description
<code>--mbox</code>	<code>-m</code>	<arg> Comma-separated list of mailboxes to search. UIDs or email-address or /SERVER/MAILBOXID or *.
<code>--offset</code>	<code>-o</code>	<arg> Specify where the hit list should start. The default is 0
<code>--query</code>	<code>-q</code>	<arg> The query string for the search
<code>--server</code>	<code>-s</code>	<arg> Mail server hostname. default is the localhost
<code>--verbose</code>	<code>-v</code>	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 -m user1@yourdomain.com,user2@yourdomain.com -q "in:inbox" -d /var/tmp
```

zmcertmgr

The CLI command **zmcertmgr** is used to manage your certificates from the command line. You can use the administration console to easily view, update and install self-signed and commercial certificates. See the administration console help for more information about using this tool.

Syntax

```
zmcertmgr {attribute} [arg]
```

Description

Name	Syntax, Example, Notes
<code>viewdeployedcert</code>	[all ldap mta proxy mailboxd] View the deployed certificate.
<code>viewstagedcert</code>	<self comm> [certfile]
<code>gensr</code>	<self comm> [-new] [subject] [-subjectAltNames "host1,host2"] Generate the certificate signing request.

Name	Syntax, Example, Notes
install	<self comm> [-new] [validation_days-] Install either a self signed or commercial signed certificate
viewcsr	<self comm> [csr_file] View the certificate signing request information
verifycert	<self comm> [priv_key] [certfile]

zmgsutil

The CLI command **zmgsutil** can be used to create or delete the GAL sync account and to force syncing of the LDAP data to the GAL sync account.

A GAL sync account is created when the GAL is configured on a domain. This account is created and the polling interval for performing a full sync is managed from the administration console.

To see attributes and settings for a GAL sync account, run **zmprov gds** against the account.

Long Name	Description
createAccount	Creates the GAL sync account. This should be done from the administration console.
deleteAccount	Deletes the GAL sync account and the references to the LDAP server. The account can also be deleted from the administration console. deleteAccount [-a {galsynceaccountname}]-i {account-id}]
trickleSync	This syncs new and updated contact data only. trickleSync [-a {galsynceaccountname}]-i {account-id}] [-d {datasource-id}] [-n {datasource-name}] The datasource ID the LDAP datasource ID. The datasource name is the name of the address book (folder) in the GAL account created to sync LDAP to. A cron job can be set up to run trickleSync.

zmldappasswd

The CLI command **zmldappasswd** changes the LDAP password on the local server. In multi node environments, this command must be run on the LDAP master server only.

This CLI command use0 - atn o0 hish5(angeothuse0 rAP p)-6.3 ssse0 rds.()JTJ0 -1.858 TD.

Name	Syntax, Example, Notes
-p	Changes ldap_postfix_password
-r	Changes ldap_root_passwd

Only one of a, l, p, or r can be specified. If options are not included, the zimbra_ldap_password is changed.

zmlocalconfig

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

Syntax

zmlocalconfig [options]

To see the local config type **zmlocalconfig**

Description

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

Long Name	Short Name	Description
--show	-s	Forces the display of the password strings
--unset	-u	Remove a configuration key. If this is a key with compiled-in defaults, set its value to the empty string.
--expand	-x	Expand values

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
-y	--authtoken (authtoken)	use authtoken string (has to be in JSON format) from command line
-Y	--authtoken (authtoken file)	use authtoken string (has be in JSON format) from command line
-m	--mailbox	mailbox to open
-p	--password {pass}	password for admin account and or mailbox
-P	--passfile {file}	read password from file
-r	--protocol	(proto req-proto/response-proto) specify request/response protocol [soap1, soap12, json]
-t	--timeout	timeout (in seconds)
-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 appointment	help on appointment-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

<code>zmmailbox help filter</code>	help on filter-related commands
<code>zmmailbox help folder</code>	help on folder-related commands
<code>zmmailbox help item</code>	help on item-related commands
<code>zmmailbox help message</code>	help on message-related commands
<code>zmmailbox help misc</code>	help on miscellaneous commands
<code>zmmailbox help permission</code>	help on permission 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>
```

- To find the mailbox size for an account

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

zmtlsctl

This command is used to set the Web server `zimbraMailMode` to the communication protocol options: HTTP, HTTPS, Mixed, Both and Redirect.

- HTTP.** HTTP only, the user would browse to `http://zimbra.domain.com`.
- HTTPS.** HTTPS only, the user would browse to `https://zimbra.domain.com`. `http://` is denied.
- Mixed** If the user goes to `http://` it will switch to `https://` for the login only, then will revert to `http://` for normal session traffic. If the user browses to `https://`, then the user will stay `https://`
- Both** A user can go to `http://` or `https://` and will keep that mode for the entire session.

- **Redirect** Like mixed if the user goes to http:// it will switch to https:// but they will stay https:// for their entire session.

All modes use SSL encryption for back-end administrative traffic.

Important: Only zimbraMailMode HTTPS can ensure that no listener will be available on HTTP/port 80, that no client application will try to auth over HTTP, and that all data exchanged with the client application will be encrypted.

Mailboxd 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 ZCS installation, in /opt/zimbra/ssl/zimbra/server/server.crt.

Syntax

zmctlctl [mode]

mode = http, https, mixed, both, redirect

Steps to run

1. Type **zmctlctl [mode]** and press **ENTER**.
2. Type **zmmailboxdctl stop** and press **ENTER**.
3. When mailboxd is stopped, type **zmmailboxdctl start** and press **ENTER**.

Limitations When Using Redirect

- Many client applications send an auth request in the initial HTTP request to the Server ("blind auth"). The implications of this are that this auth request is sent in the clear/unencrypted prior to any possible opportunity to redirect the client application to HTTPS.
- Redirect mode allows for the possibility of a man-in-the-middle attack, international/unintentional redirection to a non-valid server, or the possibility that a user will mis type the server name and not have certificate-based validity of the server.
- In many client applications, it is impossible for users to tell if they have been redirected (for example, ActiveSync), and therefore the users continue to use HTTP even if the auth request is being sent unencrypted.

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	-s	<arg> 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.

Syntax

zmlicense [options]

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	--i	<arg> Installs the specified license file.[arg] This is the Zimbra license file that you received.
-l	--ldap	Install on LDAP only
--print	-p	Displays the license information.

zmmetadump

This command is a support tool that dumps the contents of an item's metadata in a human readable form.

Syntax

zmmetadump -m <mailbox id/email> -i <item id>

or **zmmetadump -f <file containing encoded metadata>**

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. This requires a restart for the change to take effect.

Syntax

zmmypasswd [--root] <new_password>.

zmplayredo

Users who maintain a backup and restore mechanism using the snapshot facility of the storage layer use this command to restore backed up data. This command brings all backed up data to the current state so that there is no loss of information during the restore process.

Syntax

zmplayredo <option>

Time is specified in the local time zone. The year, month, date, hour, minute, second, and optionally millisecond should be specified. Month/date/hour/minute/second are 0-padded to 2 digits, millisecond to 3 digits. The hour must be specified in a 24- hour format.

Description

Long Name	Short Name	Description
--fromSeq		<arg> Replays snapshots from the specified redolog sequence
--fromTime		<arg> Replays snapshots from the specified time

Long Name	Short Name	Description
--help	-h	Shows the help information for this command
--logfiles		<arg> Replays the specified logfiles in order
--mailboxId		<arg> Replays snapshots for the specified mailbox
--queueCapacity		<arg> Used for specifying the queue capacity per player thread. The default value is 100
--stopOnError		Stops the replay on occurrence of any error
--threads		<arg> Specifies the number of parallel redo threads. The default value is 50
--toSeq		<arg> Replays snapshots to the specified redolog sequence
--toTime		<arg> Replays snapshots to the specified time

zmpoxyconfgen

This command generates the nginx proxy configuration files. It reads LDAP settings to replace template variables and generates the final nginx configuration.

Syntax

ProxyConfGen [options]

Description

Long Name	Short Name	Description
--config	-c	<arg> Overrides a config variable. The <arg> format should be name=value. To see a list of names, use -d or -D
--defaults	-d	Prints the default variable map
--definitions	-D	Prints the Definitions variable map after loading LDAP configuration and processing overrides
--help	-h	Displays help information
--include-dir	-i	<arg> Displays the directory path (relative to \$workdir/conf), where included configuration files are written

Long Name	Short Name	Description
--dry-run	-n	Specifies not to write configuration and only display the files that would be written
--prefix	-p	<arg> Displays the config file prefix. The default value is nginx.conf
--template-prefix	-P	<arg> Displays the template file prefix. The default value is \$prefix
--server	-s	<arg> Specifies a valid server object. Configuration is generated based on the specified server's attributes. The default is to generate configuration based on global configuration values
--templatedir	-t	<arg> Specifies the proxy template directory. The default value is \$workdir/conf/nginx/templates
--verbose	-v	Displays verbose data
--workdir	-w	<arg> Specifies the proxy working directory. The default value is /opt/zimbra

zmproxypurge

This command purges POP/IMAP proxy routing information from one or more memcached servers. Available memcached servers are discovered by the **zmprov gamcs** function. Others can be specified if necessary using the server port.

Syntax

ProxyPurgeUtil [-v] [-i] -a account [-L accountlist] [cache1 [cache2...]]

Description

Long Name	Short Name	Description
--help	-h	Shows the help for the usage options for this tool.
--verbose	-v	Displays verbose data
--info	-i	Displays account routing information
--account	-a	Displays account name
--list	-L	Displays file containing list of accounts, one per line

Long Name	Short Name	Description
--output	-o	Specifies the format to be used for printing routing information with information. The fields that display by default are <ul style="list-style-type: none">• cache server• account name• route information
cacheN		(optional command) Specifies additional memcache server in the form of server:port

zmredodump

This command is mainly used for debugging purposes and dumps the contents of a redolog file. When users are debugging a problem, Zimbra support might ask them to run **zmredodump** with specific options.

Multiple log files/directories can be specified with all redolog files under each directory being sorted in ascending order and processed.

Syntax

zmredodump [options] <redolog file/directory> [...]

Description

Long Name	Short Name	Description
--help	-h	Displays help messages
	-m	Specifies the mailbox ids separated by a comma or a space. The entire list of mailbox ids must be quoted if using space as a separator. To dump contents of all the redolog files, omit this option.
--no-offset		Specifies if file offsets and size for each redolog dump should not be shown

Long Name	Short Name	Description
--quiet	-q	Activates the quiet mode. Used to only print the log filename and errors, if any. Useful for verifying integrity of redologs with minimal output
--show-blob		Shows blob content. The specified item's blob is printed with <START OF BLOB> and <END OF BLOB> marking the start and end of the blob

zmskindeploy

This command simplifies the process of deploying skins in ZWC. This tool processes the skin deployment, enables the skin for all users of the ZWC deployment, and restarts the web server so that it recognizes the new skin.

For more information about this tool, see http://wiki.zimbra.com/index.php?title=About_Creating_ZCS_Themes

Syntax

zmskindeploy <path/to/skin/dir/or/zipfile>

zmsoap

Prints mail, account, and admin information in the SOAP format.

Syntax

zmsoap [options] <path1 [<path2>...]

Description

Long Name	Short Name	Description
--help	-h	Prints usage information
--mailbox	-m	<name> Displays mailbox account name. Mail and account requests are sent to this account. This attribute is also used for authentication if -a and -z are not specified
--target		<name> Displays the target account name to which the requests are sent. Used only for non-admin sessions

Long Name	Short Name	Description
--admin name	-a	<name>Displays the admin account name to authenticate as
--zadmin	-z	Displays the Zimbra admin name and password to authenticate as
--password	-p	<pass>Displays account password
--passfile	-P	<path> Reads password from a file
--element	-e	<path> Displays the root element path. If specified, all path arguments that do not start with a slash (/) are relative to this element
--type	-t	<type> Displays the SOAP request type. Can either be mail, account, or admin
--url	-u	<http[s]://...> Displays the server hostname and optional port value
--verbose	-v	Prints the SOAP request and other status information
path		<[path...]> Displays the element or attribute path and value. Roughly follows the XPath syntax as: [/element1[/element2][/@attr][=value]

zmstat-chart

This command is used to collect statistical information for the CPU, IO, mailboxd, MTQueue, MySQL, and other components and to run a script on the csv files to display the usage details in various charts. These csv files are saved to **/opt/zimbra/zmstat/**.

You must enable zmstat to collect the performance charts data.

To enable zmstat for charting on each server

1. Enter **zmprov ms {hostname} zimbraServerEnable : stats.**
2. Restart the server, enter

```
zmcontrol stop
```

```
zmcontrol start
```

Syntax

```
zmstat-chart -s <arg> -d <arg> [options]
```

Description

Long Name	Short Name	Description
--aggregate-end-at		<arg> If this is specified, the aggregate computation ends at this timestamp. Usage is MM/dd/yyyy HH:mm:ss.
--aggregate-start-at		<arg> If this is specified, the aggregate computation starts at this timestamp. Usage is MM/dd/yyyy HH:mm:ss.
--end-at		<arg> If this is specified, all samples after the specified timestamp are ignored. Usage is MM/dd/yyyy HH:mm:ss.
--start-at		<arg> If this is specified, all samples before this timestamp are ignored.
--title		<arg> This gives the chart a title that displays. Defaults to the last directory name of srcdir.
--no-summary		Summary data generation is not included.
--conf	-c	<arg> Chart the configuration xml files.
--destdir	-d	<arg> The directory where the generated chart files are saved.
--srcdir		One or more directories where the csv files are located. The csv files are moved to directories listed by date under zmstat/.

zmstat-chart-config

This command generates an xml file **/opt/zimbra/conf/zmstat-chart.xml** from a template, taking into account the server setup including the LDAP node and the processes run, among other specifications.

zmstatctl

This is a control script for checking zmstat data collectors. It starts or stops monitoring processes, checks status or rotates logs.

Syntax

```
zmstatctl start|stop|status|rotate
```

zmthrdump

This command invokes a thread dump in the ZCS server process and prints the output file. It also gives the option of saving the thread dump to a file and inserts a timestamp on the logfile.

Syntax

zmthrdump [-h] [-i] [-t <timeout seconds>] [-p <pid file>] [-f <file>] [-o <out-file>]

Description

Short Name	Description
-h	Displays help messages
-i	Appends the timestamp to the LOGFILE before invoking SIGQUIT
-p	Returns the PID to send SIGQUIT. The default value can be found in zmmailboxd_java.pid
-f	Specifies the LOGFILE to save the thread dump output in. The default value is zmmailbox.out
-o	Specifies the output file of the thread dump. The default value is stdout
-t	Specifies the timeout value (in seconds) to exit if the process becomes unresponsive. The default value is 30 seconds.

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 49.

The zmtrainsa command can be run manually to forward any folder from any mailbox to the spam training mailboxes. If you do not enter a folder name when you manually run zmtrainsa for an account, for spam, the default folder is Junk. For ham, the default folder is Inbox.

Syntax

zmtrainsa <user> spam|ham [folder]

zmtzupdate

This command is used to update time zone changes in existing appointments for specific users or all users. A .ics rule file should first be created to run with this command. A rule file lists a series of rules to match a time zone and the replacement time zone definitions. More information about this command can be found at http://wiki.zimbra.com/index.php?title=Changing_ZCS_Time_Zones

Syntax

zmtzupdate --rulefile <rule file> -a <“all” or list of specific email addresses> [--sync] [--after <date/time stamp>]

Description

Long Name	Short Name	Description
--account	-a	<arg> account email addresses separated by a white space. Use “all” for all accounts to be updated
--after		<arg> Appointments occurring after the specified date/time in this field are updated. The default cut off time is January 1 st , 2008
--help	-h	Displays help information
--rulefile		Specifies the .ics XML file that should be used to update time zone definitions
--server	-s	<arg> Specifies the mail server hostname. The default value is localhost
--sync		If specified, this option causes the zmtzupdate command to block till the server processes all requested accounts. The default value is no.

zmvolume

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

Syntax

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

Description

Long Name	Short Name	Description
--add	-a	Adds a volume
--compress	-c	<arg> Compress BLOBs; "true" or "false"
--compressionThreshold	-ct	Compression threshold; default 4KB
--delete	-d	Deletes a volume
--displayCurrent	-dc	Displays the current volume
--edit	-e	Edits a volume

zmzimletctl

This command is used to manage Zimlets and to list all zimlets on the server. See Chapter 14, Working with Zimlets. Most Zimlet deployment can be completed from the zimbra administration console.

Syntax

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

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

zmproxyconfig

This command is used to manage Zimbra proxy and should only be used when you have to make changes to Zimbra proxy after it has been installed. See Chapter 6, Working with Zimbra Proxy.

Note: Previous to ZCS 6.0, this command was called *zmproxyinit*.

Syntax

```
./zmpoxyconfig [-h] [-o] [-m] [-w] [-d [-r] [-s] [-a w1:w2:w3:w4] [-i p1:p2:p3:p4] [-p p1:p2:p3:p4] [-x mailmode]] [-e [-a w1:w2:w3:w4] [-i p1:p2:p3:p4] [-p p1:p2:p3:p4] [-x mailmode]] [-f] -H hostname
```

Description

Short Name	Description
-h	Displays help messages
-H	Hostname of the server on which enable/disable proxy functionality
-a	Colon separated list of Web ports to use. Format: HTTP-STORE:HTTP-PROXY:HTTPS-STORE:HTTPS-PROXY (Ex: 8080:80:8443:443)
-d	Disable proxy
-e	Enable proxy
-f	Full reset on memcached port and search queries and POP/IMAP throttling
-i	Colon separated list of IMAP ports to use. Format: IMAP-STORE:IMAP-PROXY:IMAPS-STORE:IMAPS-PROXY (Ex: 7143:143:7993:993)
-m	Toggle mail proxy portions
-o	Override enabled checks
-p	Colon separated list of POP ports to use. Format: POP-STORE:POP-PROXY:POPS-STORE:POPS-PROXY (Ex: 7110:110:7995:995)
-r	Run against a remote host. Note that this requires the server to be properly configured in the LDAP master
-s	Set Cleartext to FALSE (secure mode) on disable
-t	Disable reverse proxy lookup target for the store server. Only valid with -d. Make sure that you intend for all proxy functions for the server to be disabled.
-w	Toggle Web proxy portions

Short Name	Description
-x	zimbraMailMode to use on disable (Default is HTTP)

hostname is the value of the **zimbra_server_hostname** LC key for the server being modified.

Required options are -f by itself, or -f with -d or -e

Note that

- -d or -e require one or both of -m and -w.
- -i or -p require -m.
- -a requires -w.
- -x requires -w and -d for store.
- -x requires -w for proxy.

The following are the defaults for -a, -i, -p, and -x if they are not supplied as options.

-a default on enable: 8080:80:8443:443
 -a default on disable: 80:0:443:0
 -i default on enable: 7143:143:7993:993
 -i default on disable: 143:7143:993:7993
 -p default on enable: 7110:110:7995:995
 -p default on disable: 110:7110:995:7995
 -x default on store disable: http
 -x default on proxy enable/disable: http

Appendix B ZCS Crontab Jobs

The crontab is used to schedule commands to be executed periodically on the Zimbra servers.

How to read the crontab

Each entry in a crontab file consists of six fields, specified in the following order

minute hour day month weekday command

The fields are separated by blank spaces or tabs.

Field	Description
• 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, 1 is Monday, etc., or use names)
• command	This is the complete sequence of commands to be executed for the job

When an asterisk (*) is displayed, it means all possible values for the field. For example, an asterisk in the hour time field would be equivalent to “every hour”

ZCS Cron Jobs

You can view the ZCS crontab by logging on as `zimbra` and typing **`crontab -l`**.

The following cron jobs are scheduled to run for ZCS

Log pruning

The log pruning deletes logs from **`/opt/zimbra/log`** that are over eight days old. The job runs at 2:30 a.m.

Status logging

`zmstatuslog` calls `zmcontrol status` and outputs its data into `syslog`. This is primarily so that the logger can read the data and keep the administration console status up-to-date. Status logging job runs every 2 minutes.

Backups

Full and incremental backups are scheduled to run according to the schedule defined by **`zmschedulebackup`** command. By default the full backup is scheduled for 1:00 a.m., every Saturday. The incremental backups are scheduled for 1:00 a.m., Sunday through Friday. By default, backups older than a month are deleted on the first of each month at 12 a.m.

Jobs for `crontab.store`

Log pruning

The log pruning deletes logs from **`/opt/zimbra/mailboxd/logs`** that are over eight days old. The job runs at 2:30 a.m.

Clean up the quarantine dir

Mail identified with a virus or spam are not dropped immediately, but are put in quarantine. Messages older than seven days are deleted at 1:00 a.m. daily.

Table maintenance

The `ANALYZE TABLE` statement is run on all tables in the database to update the statistics for all indexes. This is done to make sure that the MySQL query optimizer picks the correct ones when executing SQL statements. This script is run 1:30 a.m. on Sunday.

Report on any database inconsistencies

`zmbdbintegrityreport` is run weekly to check the MySQL database for corruption and will notify the administrator if any corruption is found. When this is run, it may consume a significant amount of I/O. If you find that it is an issue, you may want to change the frequency with which **`zmbdbintegrityreport`** is run by editing the ZCS crontab entry. This report runs at 11:00 p.m. Sundays.

Large sites may opt to disable this by setting **`zmlocalconfig -e zmbdbintegrityreport_disabled=TRUE`**.

If you choose to disable this, it is recommended that the integrity report be run by hand during the normal maintenance windows and prior to running any ZCS upgrades.

Monitor for multiple mysqld tp prevent corruption

A script is executed to see if mysqld process is running to detect cases where corruption is likely to be caused. An email is generated if it finds more than 1 mysqld process running. The script runs every 5 minutes.

Jobs for crontab.logger

process logs

zmlogprocess runs every 10 minutes to parse logs and produce MTA metrics (as/av, volume, count, etc).

Daily reports

When the logger package is installed, a daily mail report is automatically scheduled in the crontab. The report runs every morning at 11:30 and is sent to the administrator's email address.

Jobs for crontab.mta

Queue logging

The **zmqueue** report status via the syslog is reviewed. This is logger data. The status is updated every 10 minutes.

Spam training

The **zmtrainsa** script is enabled to feed mail that has been classified as spam or a non-spam to the SpamAssassin application. SpamAssassin learns what signs are likely to mean spam or ham. This job should run only on one Zimbra MTA. The job runs at 11:00 p.m.

Spam training cleanup

zmtrainsa empties the spam and ham mailboxes each day. The job runs at 11:45 p.m.

DSPAM cleanup

This job does not run at this time.

Spam Bayes auto-expiry

Spam bayes auto-expiry maintains the spam-assassin Bayes database. This keeps the database to manageable size ensuring spam processing remains as quick as possible. This runs every day at 11:20 p.m.

Clean up amavisd/tmp

This job is used to clean up the amavisd temp files. It runs at 5:15 a.m. and at 8:15 p.m.

Single Server Crontab -I Example

```
[zimbra@example ~]$ crontab -l
# ZIMBRASTART -- DO NOT EDIT ANYTHING BETWEEN THIS LINE AND ZIMBRAEND
#
# Log pruning
#
30 2 * * * find /opt/zimbra/log/ -type f -name \*.log\* -mtime +8 -exec rm {} \;      >
/dev/null 2>&1
35 2 * * * find /opt/zimbra/log/ -type f -name \*.out.???????????? -mtime +8 -ex    ec
rm {} \; > /dev/null 2>&1
#
# Status logging
#
*/2 * * * * /opt/zimbra/libexec/zmstatuslog
#
# Backups
#
# BACKUP BEGIN
0 1 * * 6 /opt/zimbra/bin/zmbbackup -f -a all
0 1 * * 0-5 /opt/zimbra/bin/zmbbackup -i
0 0 * * * /opt/zimbra/bin/zmbbackup -del 1m
# BACKUP END
#
# crontab.ldap
#
#
# crontab.store
#
# Log pruning
#
30 2 * * * find /opt/zimbra/mailboxd/logs/ -type f -name \*log\* -mtime +8 -exec      rm
{} \; > /dev/null 2>&1
30 2 * * * find /opt/zimbra/log/ -type f -name stacktrace.\* -mtime +8 -exec rm      {}
\; > /dev/null 2>&1
#
# Table maintenance
#
30 1 * * 7 /opt/zimbra/libexec/zmmaintaintables >> /dev/null 2>&1
#
# Report on any database inconsistencies
#
0 23 * * 7 /opt/zimbra/libexec/zmdbintegrityreport -m
#
# Monitor for multiple mysqld to prevent corruption
#
*/5 * * * * /opt/zimbra/libexec/zmcheckduplicatemysqld -e > /dev/null 2>&1
#
# crontab.logger
#
# process logs
#
00,10,20,30,40,50 * * * * /opt/zimbra/libexec/zmlogprocess > /tmp/logprocess.out
2>&1
#
# Graph generation
#
10 * * * * /opt/zimbra/libexec/zmgengraphs >> /tmp/gengraphs.out 2>&1
```



```

#
# Daily reports
#
10 1 * * * /opt/zimbra/libexec/zmdailyreport -m
#
#
crontab.mta
#
#
# Queue logging
#
0,10,20,30,40,50 * * * * /opt/zimbra/libexec/zmqueueelog
#
# Spam training
#
0 23 * * * /opt/zimbra/bin/zmtrainsa >> /opt/zimbra/log/spamtrain.log 2>&1
#
# Spam training cleanup
#
45 23 * * * /opt/zimbra/bin/zmtrainsa --cleanup >> /opt/zimbra/log/spamtrain.log
2>&1
#
# Dspam cleanup
#
0 1 * * * [ -d /opt/zimbra/data/dspam/data/z/i/zimbra/zimbra.sig ] && find /opt/
zimbra/dspam/var/dspam/data/z/i/zimbra/zimbra.sig/ -type f -name \*sig -mtime +7
exec rm {} \; > /dev/null 2>&1 -
8 4 * * * [ -f /opt/zimbra/data/dspam/system.log ] && /opt/zimbra/dspam/bin/dspa
m_logrotate -a 60 -l /opt/zimbra/data/dspam/system.log
8 8 * * * [ -f /opt/zimbra/data/dspam/data/z/i/zimbra/zimbra.log ] && /opt/zimbra
dspam/bin/dspam_logrotate -a 60 -l /opt/zimbra/data/dspam/data/z/i/zimbra/zimb
ra.log a/
#
# Spam Bayes auto-expiry
#
20 23 * * * /opt/zimbra/libexec/sa-learn -p /opt/zimbra/conf/salocal.cf --dbpath
/opt/zimbra/data/amavisd/.spamassassin --siteconfigpath /opt/zimbra/conf/spamas
sassin --force-expire --sync > /dev/null 2>&1 /
#
# Clean up amavisd/tmp
#
15 5,20 * * * find /opt/zimbra/data/amavisd/tmp -maxdepth 1 -type d -name 'amavi
*' -mtime +1 -exec rm -rf {} \; > /dev/null 2>&1 s-
#
# Clean up the quarantine dir
#
0 1 * * * find /opt/zimbra/data/amavisd/quarantine -type f -mtime +7 -exec rm -f
\; > /dev/null 2>&1 {}
#
# ZIMBRAEND -- DO NOT EDIT ANYTHING BETWEEN THIS LINE AND ZIMBRASTART
[zimbra@example ~]$

```

Appendix C The zmlocalconfig Settings

This table outlines the zmlocalconfig settings that commonly need to be configured by an administrator.

zmlocalconfig setting	Description
LDAP	
ldap_master_url	URL to the LDAP master server For example, ldap://master.example.com:389
ldap_url	List of LDAP server URLs for use by this server. For example, ldap://replica.example.com:389 ldap://master.example.com:389 . <i>Note: ldap_url is used for read access only</i>
ldap_postfix_password	Password used by the postfix user to identify itself to the LDAP server. It is configured on the MTA server to be the same as the password on the LDAP master server. To change this password, use <code>opt/zimbra/bin/zmldappasswd[-p] new password</code>
ldap_replication_password	Password used by the LDAP replication user to identify itself to the LDAP master. It must be the same as the password on the LDAP master server. To change this password, use <code>opt/zimbra/bin/zmldappasswd[-l] new password</code>

zmlocalconfig setting	Description
ldap_nginx_password	<p>Password used by the Nginx server to identify itself to the LDAP server. It is configured to be the same as the replication/Amavis/Postfix passwords on the LDAP master server.</p> <p>To change this password, use opt/zimbra/bin/zmldappasswd[-n] new password</p>
ldap_amavis_password	<p>Password used by the Amavis user to identify itself to the LDAP server. It is configured on the MTA server to be the same as the Postfix/Nginx/replication passwords on the LDAP master server.</p>
ldap_starttls_supported	<p>Enables/disables the LDAP client in the mailbox server, Postfix, and Amavis servers to communicate with the LDAP server. To disable use of starttls, set this command to 0. To enable use, change the setting to 1.</p>
Java	
mailboxd_java_heap_memory_percent	<p>Percentage of system memory that is used as the maximum Java heap size of the JVM running mailboxd server. The value is usually set to 40 percent.</p>
mailboxd_java_options	<p>JVM options that are used when launching the mailboxd server. The ZCS installer enables all the recommended options by default, including the client, NewRatio, MaxPermSize, Djava.awt.headless, and SoftRefLRUPolicy</p>
MySQL	

zmlocalconfig setting	Description
mysql_memory_percent	Percentage of system memory that MySQL should use. This value is stored here for use by zmmyconf program. Changing this setting does not immediately reflect in the MySQL server. Using precaution, you should regenerate my.cnf and restart the MySQL server for the change to take effect
mysql_port	Port number on which the MySQL server should listen. The default Zimbra MySQL port is 7306.
mysql_root_password (use zmmypasswd)	Password for MySQL's built-in 'root' user, not to be confused with the Unix root login. As a convenience, during database initialization, a random password is generated and saved in the local config file and in MySQL. To change this password, use the zmmypasswd program. This changes the password saved in both the local config file and in MySQL
zimbra_mysql_password (use zmmypasswd)	This is the password for zimbra_mysql_user. It is stored in the local config file for use by the store application for authentication. To change this password, use the zmmypasswd program which changes the password saved in both the local config file and in MySQL
zimbra_mysql_user	This is the MySQL user name to create or access Zimbra databases and tables. This value is also used in the -u option of the MySQL command line program
Postfix	
postfix_	More details about Postfix configuration can be found at http://www.postfix.org/postconf.5.html

Appendix D 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 zimbra, 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.

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 253
- aborting backup 193
- account
 - assign to mailbox server 123
 - deleting 125
 - other configuration settings 143
 - restoring 196
- account authentication 33
- account distribution by COS 123
- account limits by domain 113
- account provisioning, zmprov 234
- account quota 145
- account quota and MTA 48
- account status 124
- account types by COS, setting 113
- account types, tracking number assigned 113
- account, creation date 119
- account, password restriction 123
- account, provision with zmprov 242
- accounts
 - batch provisioning 121
- accounts object 37
- accounts, list all 243
- accounts, number used 107
- accounts, setting up and configuring 120
- accounts, user 71
- active status 124
- add logos for a domain 222
- address book size limit, configuring 138
- address book, features 138
- addresses, search for 129
- admin console, tasks 72
- admin extensions 118
- admin password, change 243
- administration console 16, 69
- administration tasks 119
- administrator message of the day 73, 74
- administrator password, change 70
- advanced ZWC 131
- alias, add with zmprov CLI 243
- anti-spam component 17
- anti-spam protection 48
- anti-spam settings 103
- anti-spam statistics 167
- anti-spam training filter 49
- anti-virus component 17
- anti-virus protection 48
- anti-virus settings 104
- anti-virus statistics 167
- anti-virus updates 48, 104
- application packages, Zimbra 18
- appointment reminder 141
- appointment reminder popup,
Yahoo!BrowserPlus 141
- archive mailboxes, creating 216
- archive templates 216
- Archiving 209
- archiving attribute 215
- archiving package, installing as an update to
ZCS 211
- archiving, administering archive server 215
- Archiving, creating dedicated COS 214
- archiving, how it works 209
- attachment settings
 - global settings 100
- attachment viewing options, setting 149
- attachment viewing, setting account
options 148
- attachments
 - blocking 100
- audit log 172
- auth token, immediate session end 148
- authentication 33
- authentication modes 111
- authentication, custom 35
- autho token lifetime 148
- autoCompleteGal, zmprov 241
- auto-grouped backup method 117, 184
- automatic purge of messages, setting up 148

B

- backup 30
 - aborting 193
 - auto-grouped 194
 - full 191
 - incremental 192
 - interrupted 193
 - scheduling 189

- backup administration console 186
- backup CLI commands 188
- backup directory structure 185
- backup method, auto-grouped 185
- backup method, standard 184
- backup options 195
- backup process, overview 21
- backup timeline 183
- backup ZCS 183
- backup, CLI commands 248
- backup, skip backup of blobs 195
- backup, skip HSM blob backup 195
- backup, standard method, auto-grouped method 117, 184
- backup, skip backup of search index 195
- backups cron job 286
- batch provisioning new accounts 121
- blocking attachments 100
- bounced delivery report 168
- Briefcase feature 142

C

- calendar preferences 140
- calendar resource provisioning, zmprov 236
- calendar sync, zmcalkchk 140
- calendar, enabling personal appointments only 139
- calendar, import or export .ics 141
- calendar, nested 139
- calendar, features 139
- change administrator password 70
- change password page, configure 123
- changing account status 124
- changing password 123
- checking for latest ZCS software updates 181
- Clam AntiVirus software 48
- clamd.log 172
- class of service 122
 - about 38, 122
- class of service object 38
- class of service, COS 71
- clean up amavisd/tmp cron job 287
- clean up the quarantine dir cron job 286
- CLI auto-grouped backup 194
- CLI command to move
 - mailbox, zmmailboxmove 120
- CLI commands, provisioning 232
- CLI commands, start/stop service 259
- CLI for account management
 - zmmailbox 119
 - zmmboxsearch 120
 - zmprov 119
- CLI utilities 227

- closed status 125
- company directory 40
- component thread number 176
- components, Zimbra 17
- config provisioning, zmprov 238
- configuration, typical example 23
- contact 12
- contact lists 138
- core functionality 15
- COS account types, setting 113
- COS provisioning, zmprov 237
- COS, denying access from a zimlet 163
- COS, list all 243
- COS, password restriction 123
- creating accounts 121
- crontab jobs 285
- crontab store jobs 286
- crontab, how to read 285
- crontab.logger cron jobs 287
- crontab.mta jobs 287
- cross mailbox search 120
- cross mailbox search, CLI 261
- cross mailbox search 217
- custom authentication 35

D

- daily reports 167
- data store 20, 29
 - about 29
 - file location 22
- dates, Zimlet 163
- deleting accounts 125
- directory structure 21
- disable 151
- disaster recovery
 - basic steps 200
 - overview 200
 - restoring offline 201
 - restoring to new server 203
- discovery, how it works 211
- disk full alerts 168
- disk layout 28
- disk space monitoring 168
- distribution list provisioning, zmprov 238
- distribution list used for sharing 127
- distribution list, create with zmprov CLI 243
- distribution list, maximum members 126
- distribution list, sharing items 144
- distribution lists object 38
- distribution lists, group sharing 127
- distribution lists, managing 126
- documentation 12
- Documents application 112

- Documents provisioning, zmprov 239
- Documents, features 141
- domain admin console view 90
- domain admin link to admin console 90
- domain provisioning, zmprov 236
- domain rename process 114
- domain renaming 114
- domain, account limits 113
- domain, after domain is renamed 114
- domain, create with zmprov CLI 243
- domain, set default with zmprov CLI 243
- domains
 - authentication modes 111
 - virtual hosts 111
- domains object 38
- domains, global address list mode 110
- domains, managing 108
- domains, Documents account 112

E

- edge MTA 46
- email addresses zimlet 163
- email messaging, features 132
- equipment resources 127
- error report, daily 168
- exclude items in mailbox move 126
- export calendar appointments in .ics 141
- export preferences on ZWC 138
- external AD account authentication 34
- external LDAP account authentication 34

F

- failed logging policy, setting 147
- features, core 15
- features, web client 16
- find backup 193
- flushCache, zmprov 242
- forwarding address, hidden 133
- free/busy interoperability 104
- free/busy, zmprov 236
- full backup 191

G

- GAL 40
 - LDAP search filter used 40
 - search options 40
 - search parameter settings 41
- GAL access for COS 136
- GAL attributes 40
- GAL mode 110
- GAL sync account 110

- generateDomainPreAuth, zmprov 241
- global configuration 99
- global configuration object 39
- global Documents account 112
- global settings 71
 - anti-spam 103
 - anti-virus 104
 - HSM 106
 - license 107
 - MTA 102
 - POP and IMAP 103
- group calendar, enabling 139
- group sharing, using distribution lists for 127

H

- ham mailbox 49
- handler exceptions in mailbox log 176
- hidden forwarding address 133
- high availability support 15
- horizontal scalability 15
- HSM
 - scheduling 117
- HSM, CLI 269
- HSM, global setting 106
- HTTP proxy 59
- http proxy 59
- http proxy, setting up 60

I

- IMAP access 137
- IMAP global settings 103
- IMAP proxy, setting up 57
- IMAP, class of service 122
- import calendar appointments in .ics 141
- import preferences on ZWC 138
- incoming mail routing 28
- incremental backup 192
- index messages 19
- index store 20, 29
 - file location 22
- index volume 116
- index/search
 - back-end technologies used 29
- indexing 30
- install certificate, CLI 262
- Instant Messaging feature 143
- instant notification 143
- internal account authentication 34
- internal authentication mechanism 34
- interop 104

K

Kerberos proxy set up 62
keyboard shortcuts, enable 136

L

LDAP

- directory traffic 32
- hierarchy 32
- implementation 32
- overview 31
- schema include files for Zimbra 33

LDAP Amavis password 292
LDAP NGINX password 292
LDAP Postfix password 291
LDAP replication password 291
LDAP schema 33
LDAP server, restoring 200
legal discovery 67
legal intercept 65
legal intercept attributes 65
license 11
license ID 107
license information 107
license policy for replacing logo 220
license, extended trial 11
license, number of accounts used 107
license, renew within 107
license, updating 107
linking to admin console log in page 90
local configuration, CLI 265
location resources 127
lockout status 125
log files 30
log files, description of 172
log pruning cron job 286
log, how to read mailbox.log records 176
log4j pre-defined zimbra categories 173
log4j, used to configure logging 173
logger 165
logger_myslow.log 172
logging levels 173
logging on to admin console 69
Lucene 29

M

mail filters 136
mail filters, working with spam check 136
mail identities 134
mail notification 134
mail report, change 168
mail reports 167

mailbox full notification 145
mailbox log examples 177
mailbox log records 175
mailbox log, how to read 176
mailbox management tool 119
mailbox move, CLI 260
mailbox quota, enforcing 125
mailbox quotas
 specifying 145
mailbox quotas, monitoring 171
mailbox search 120
mailbox server
 overview 27
mailbox snapshot for legal discovery 67
mailbox, move 120, 125
mailbox, reindexing 124
mailbox, view from admin console 124
mailbox, zmpov 240
mailbox.log 172
mailboxes, cross mailbox search 217
main.cf file 46
management tasks 71
management tasks from CLI 73
managing resource accounts 129
managing resources 127
mandatory 151
mandatory zimlets 151
master.cf file 46
maximum number in distribution lists 126
message header information 179
message lifetime 149
message of the day for administrators 73, 74
message search 120
message store 19, 20, 28
 file location 22
 single-copy 28
message store, MIME format 20
message volume 117, 167
messages received and sent report 168
messages, purging 148
modes, set with zmtlsctl CLI 268
modify base colors 222
modify ZWC theme, attributes 222
modify ZWC theme, graphics to replace 221
Monitor for multiple mysqld tp prevent corruption
 cron job 287
monitoring quotas 171
monitoring server status 166
monitoring tool 165
move mailbox 120, 260
moving a mailbox 125
MTA 19
MTA functionality 46
MTA package, Zimbra 19

- MTA queues 52
- MTA settings, how to configure 102
- MySQL 20
- MySQL, database check 180

N

- nested calendars 139
- nginx 55

O

- offline restore 198
- offline restore CLI 189
- offline restore, CLI 257
- open source components 17
- out of office reply 134

P

- password policy, setting 145
- password restriction 123
- password, admin change 243
- password, change password page 123
- password, changing admin 70
- password, failed login policy 147
- password, LDAP Amavis 292
- password, LDAP NGINX 292
- password, LDAP Postfix 291
- password, LDAP replication 291
- performance charts 276
- performance statistics 166
- persona 134
- phone number Zimlet 164
- polling interval for GAL sync 110
- POP 103
- POP proxy, setting up 57
- POP3, external access 135
- ports, proxy 56
- Postfix 45
- Postfix configuration files 46
- postfix error report 168
- process logs cron job 287
- product overview 15
- protocol, set with CLI 268
- provisioning, CLI commands 232
- proxy architecture 55
- proxy components 55
- proxy ports 56
- proxy, http 59
- proxy, Kerberos 62
- proxy,http 59
- public service host name 108
- public service host name, setting up 109

- publishing shares 127
- purge messages 149
- purge, setting up 148

Q

- query backup, CLI 254
- queue logging cron job 287
- queues 52
- quota out of sync 240
- quota, address book 145
- quota, setting up notification 145
- quotas and message delivery 48
- quotas, monitoring 171
- quotas, setting 145

R

- recalculate mailbox count command 240
- recipient object 38
- recipients, most active report 168
- redo log 30
- reindexing a mailbox 124
- relay host settings 47
- removing zimlets 163
- rename a domain 114
- renew license 107
- replace ZWC logo 220
- report on any database inconsistencies cron job 286
- report, daily mail 167
- report, database inconsistencies 286
- reports, MySQL 180
- resource accounts, managing 129
- resource calendar, sharing 129
- resource conflict rules 129
- resources, maintaining calendars 128
- resources, managing 127
- resources, scheduling policy 128
- REST URL 108
- restore backup, CLI 255
- restore CLI commands 188
- restore live system 199
- restore mailbox and exclude delete operation 198
- restore process 196
- restore, selection items to exclude 199
- restoring an account 196
- restoring LDAP server 200
- restoring to new server 203

S

- schedule backups, CLI 251
- scheduling backups 189

- scheduling policy for resources 128
- schema, LDAP 33
- screen resolution, standard web client 131
- search 129
- search across mailboxes 120, 211
- searchGAL, zmprov 241
- senders, most active report 168
- server
 - admin extensions 118
 - managing zimlets 118
 - volume settings 116
- server mode, changing 268
- server pool by COS 123
- server provisioning, zmprov 238
- server settings
 - services 116
- server statistics 166
 - message count 167
 - message volume 167
- server statistics, enable on admin console 165
- server status 166
- server, Zimbra
 - managing 115
- service, start/stop 259
- session idle lifetime 148
- session time out policy, 148
- sessions, expire 148
- setting up legal intercept 66
- setting up zimlets 159
- shared items, managing 144
- shares tab, distribution list 144
- sharing, notifying distribution list 127
- signatures, maximum length 135
- single-copy message storage 28
- single-copy store 28
- skins 150, 219
- skype 164
- smart host 47
- SMTP authentication 47
- SMTP restrictions 47
- SNMP monitoring 180
- SNMP package, Zimbra 20
- SNMP traps, error 180
- software version checking 181
- spam bayes auto-expiry cron job 287
- spam mailbox 49
- spam message lifetime 149
- spam training cleanup cron job 287
- spam training cron tab 287
- spam training filter 49
- spam training, CLI 278
- spam white list, for mail filters 136
- spam, turning on/off training attributes 49
- SpamAssassin 48

- spamtrain .log 172
- stack traces in mailbox log 176
- standard web client, setting as default 131
- standard ZWC 131
- start service 259
- statistics 72
 - anti-spam 167
- status 72
- status logging cron job 286
- stop restore 198
- stop service 259
- store package 19
- support 12
- sync.log 173
- syncGAL, zmprov 242
- system architecture 17
- system architecture graphic 18

T

- Table maintenance cron job 286
- tasks feature 141
- tasks from admin console 72
- theme colors 219
- themes 150
- themes, setting account options 150
- third-party software bundled with 17
- timezone, enabling for Calendar 140
- training filter for spam 49
- transaction log 30
- trashed message lifetime 149
- trial license 11

U

- unread message count out of sync 240
- updating a license 107
- updating anti-virus software 48, 104
- upgrading zimlets 162
- URL zimlet 163
- user auth token lifetime, expire 148
- user warning message, navigation from ZCS 152

V

- vacation message 134
- view mailbox from admin console 124
- view quota 145
- virtual host 111
- volume settings 116
- volumes, managing with CLI 279

W

Web client features 16
wiki 112

X

x-envelope headers 210

Z

Zimbra applications 131
zimbra cron jobs 286
Zimbra logger 165
Zimbra mobile 150
Zimbra monitor host 165
Zimbra MTA 45
Zimbra objects
 ldap 37
Zimbra Schema 33
Zimbra web client, import/export account data 138
zimbraMailReferMode, use with proxy 62
zimbraProxyAllowedDomains, zimlets 160
zimlet gallery 164
zimlet status view 160
zimlet, enable 151
zimlets 159
zimlets included with ZCS 163
zimlets, configure 162
Zimlets, configuring for accounts 151
zimlets, disabling 163
zimlets, listing 161
zimlets, listing all 281
zimlets, managing 118
Zimlets, managing from the administration
 console 160
zimlets, managing from command line 160
zimlets, modify COS 160
zimlets, remove 163
zimlets, specify COS to use 161
zimlets, upgrading 162
zmbbackup 248, 255
zmbintegrityreport 286
zmbintegrityreport disable 286
zmlocalconfig settings 291
zmlocalconfig,Java 292
zmlocalconfig,LDAP 291
zmlocalconfig,MySQL 292
zmlocalconfig,Postfix 293
zmprov CLI 232
zmstat-chart 276
zmtrainsa CLI command for spam training 49
zmtrainsa spam training tool 49
ZWC versions 131

