

# Zimbra Collaboration Server Administrator's Guide

**Release 7.2**

**Network Edition**

**April 2012**

## Legal Notices

Copyright ©2005-2014 Telligent Systems, Inc.  All rights reserved.  This product is protected by U.S. and international copyright and intellectual property laws.

“Telligent” and “Zimbra” are registered trademarks or trademarks of Telligent Systems, Inc. in the United States and other jurisdictions.  All other marks and names mentioned herein may be trademarks of their respective companies.

Telligent Systems, Inc. d/b/a Zimbra Software, LLC

www.zimbra.com

Zimbra Collaboration Server 7.2.3

Rev 4 - March 2014

GA. April 2012

# Table of Contents


**1 Introduction . . . . . 11**

Intended Audience . . . . . 11
Zimbra Collaboration Server License . . . . . 11
Obtaining a License . . . . . 12
Available Documentation . . . . . 12
Support for Recommended Third-Party Components . . . . . 13
Support and Contact Information . . . . . 13

**2 Product Overview . . . . . 15**

Core Functionality . . . . . 16
Zimbra Components . . . . . 17
System Architecture . . . . . 18
Zimbra Packages . . . . . 19
Backup Process Overview . . . . . 22
Zimbra System Directory Tree . . . . . 22
Example of a Typical Multi-Server Configuration . . . . . 24

**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 . . . . . 31
Log . . . . . 31

**4 Zimbra LDAP Service . . . . . 33**

Directory Services Overview . . . . . 33
LDAP Hierarchy . . . . . 34
Zimbra Schema . . . . . 35
Account Authentication . . . . . 36
Internal Authentication Mechanism . . . . . 36
External LDAP and External Active Directory Auth Mechanism. . . . 37
Custom Authentication - zimbraCustomAuth . . . . . 38
Kerberos5 Authentication Mechanism . . . . . 39
Zimbra Objects . . . . . 39
Company Directory/GAL . . . . . 42
Converting OpenLDAP back-hdb to OpenLDAP back-mdb . . . . . 45
Flushing LDAP Cache . . . . . 46
Themes and Locales . . . . . 46
Accounts, COS, Domains, and Servers . . . . . 46
Global Configuration. . . . . 47

**5 Zimbra MTA . . . . . 49**
Zimbra MTA Deployment . . . . . 49
Postfix Configuration Files . . . . . 50
MTA Functionality . . . . . 51
SMTP Authentication . . . . . 51
SMTP Restrictions . . . . . 51
Relay Host Settings . . . . . 51
MTA-LDAP Integration . . . . . 52
Account Quota and the MTA . . . . . 52
MTA and Amavisd-New Integration . . . . . 52
Anti-Virus Protection. . . . . 53
Anti-Spam Protection . . . . . 53
Receiving and Sending Mail through Zimbra MTA . . . . . 56
Zimbra MTA Message Queues . . . . . 57

**6 Working with Zimbra Proxy . . . . . 59**
Zimbra Proxy Components . . . . . 59
Zimbra Proxy Architecture and Flow . . . . . 59
Customizing Zimbra Proxy Configuration . . . . . 60
Zimbra IMAP/POP Proxy . . . . . 60
Zimbra Proxy Ports for POP/IMAP . . . . . 61
Setting up IMAP/POP Proxy after HTTP Proxy . . . . . 61
Configuring ZCS HTTP Proxy . . . . . 63
Setting up HTTP Proxy after IMAP/POP Proxy is set up . . . . . 64
Setting Proxy Trusted IP Addresses . . . . . 66
Configuring Zimbra Proxy for Kerberos Authentication . . . . . 67

**7 Managing Legal Requests for Information . . . . . 69**
Legal Intercept for Law Enforcement . . . . . 69
Configuration . . . . . 70
Create Mailbox Snapshots for Legal Discovery . . . . . 71

**8 Using the Administration Console . . . . . 73**
Logging In . . . . . 73
Changing Administrator Passwords . . . . . 74
About the Administration Console . . . . . 74
Managing Tasks from the Administration Console. . . . . 77
Tasks Not Available from Administration UI. . . . . 77
Creating Message of the Day for Administrators . . . . . 78
Checking for ZCS Software Updates . . . . . 79
Searching from the Administration Console . . . . . 80

**9 Delegated Administration . . . . . 83**
Delegated Administration Terminology . . . . . 83
How Delegated Administration Rights are Granted . . . . . 84
Selecting Target Types . . . . . 85
Rights . . . . . 86
Implementing Delegated Administration . . . . . 91
Creating Administrator Groups and Administrators . . . . . 91
Configure Grants on Administrator Accounts or Admin Groups. . . . 95
Granting ACLs to a Target . . . . . 95

Revoking Rights . . . . . 95
Viewing Rights Granted to Administrators . . . . . 96
Predefined Delegated Administrator Role . . . . . 96
Domain Administration Group . . . . . 96
Distribution List Administration Group. . . . . 98
Specific Access Rights . . . . . 98

**10 Managing ZCS Configuration . . . . . 105**

Managing Global Configurations . . . . . 105
General Global Settings . . . . . 106
Global Settings to Block Mail Attachments. . . . . 107
Global MTA Settings . . . . . 107
Global IMAP and POP Settings . . . . . 109
Anti-spam Settings . . . . . 109
Anti-virus Settings . . . . . 110
Zimbra Free/Busy Interoperability . . . . . 110
Customizing Themes . . . . . 113
Global HSM . . . . . 113
License Information . . . . . 114
Backup/Restore . . . . . 115
Setting Up S/MIME. . . . . 116
Managing Domains . . . . . 117
General Information . . . . . 118
Global Address List (GAL) Mode . . . . . 119
Authentication Modes. . . . . 121
Virtual Hosts. . . . . 121
Domain Advanced Tab. . . . . 122
Free/Busy Interoperability . . . . . 123
Zimlets on the Domain . . . . . 123
Customizing Themes for Domains . . . . . 123
Setting Account Limits . . . . . 124
Renaming a Domain. . . . . 124
Adding a Domain Alias . . . . . 125
Installing a SSL Certificate for a Domain . . . . . 125
Managing Servers . . . . . 126
General Server Settings . . . . . 127
Services Settings . . . . . 127
MTA Server Settings . . . . . 127
IMAP and POP Server Settings . . . . . 128
Volume Settings . . . . . 128
Backup and Restore - selecting the backup mode. . . . . 129
Managing Other Functions . . . . . 129
Zimlets . . . . . 129
Admin Extensions. . . . . 130
Adding Words to ZCS Spell Dictionary. . . . . 130
Setting System-wide Signatures . . . . . 130

**11 Managing User Accounts . . . . . 133**

Setting up Accounts . . . . . 134
Configuring One Account . . . . . 134
Configuring Many Accounts at Once . . . . . 135
Examples of XML Files. . . . . 141
Managing Aliases . . . . . 143

Managing Class of Services . . . . . 143
COS Calendar Preference to Set Default Time Zones. . . . . 144
Distributing Accounts Across Servers . . . . . 144
Changing Passwords . . . . . 145
Directing Users to Change Password Page External Authentication 145
Setting Polling Intervals . . . . . 145
View an Account Mailbox . . . . . 146
Reindexing a Mailbox . . . . . 146
Changing Account Status . . . . . 146
Deleting an Account . . . . . 147
Moving a Mailbox to a New Server . . . . . 147
Set Global Options to Exclude Items from the Mailbox Move . . . . 148
Move A Mailbox from the Administration Console . . . . . 148
Move Mailboxes Using CLI zmmboxmove . . . . . 148
View Progress of Mailbox Moves . . . . . 149
Managing Distribution Lists . . . . . 149
Manage Access to Distribution Lists . . . . . 149
Enable View of Dist List Members for Active Directory Accounts . 151
Using Distribution Lists for Group Sharing . . . . . 151
Managing Resources . . . . . 152

**12 Customizing Accounts, Setting General Pref and Password Rules . . 155**

Zimbra Web Client Versions . . . . . 155
Zimbra Messaging and Collaboration Applications . . . . . 156
Email Messaging . . . . . 156
How Autocomplete Ranks Names . . . . . 163
Email Preferences Users Manage . . . . . 163
Using Import/Export Page . . . . . 164
Setting Up Trusted Addresses Preferences. . . . . 164
Subscribing to RSS Feeds . . . . . 164
Address Book . . . . . 165
Calendar . . . . . 165
Setting Remote Calendar Automatic Update Interval. . . . . 167
Filtering Calendar Messages . . . . . 167
Disable Attendee Edits to Appointments . . . . . 167
Other User Calendar Preferences . . . . . 168
Tasks . . . . . 169
Briefcase . . . . . 170
Enabling Sharing . . . . . 170
Managing Shared Items using Distribution Lists . . . . . 171
Enable SMS Notification . . . . . 171
Disabling Preferences . . . . . 171
Setting Account Quotas . . . . . 172
Setting Email Policies . . . . . 172
Setting Password Policy. . . . . 172
Setting Failed Login Policy . . . . . 174
Setting Session Timeout Policy . . . . . 175
Setting Email Retention Policy . . . . . 176
Recovering Deleted Items From the Dumpster . . . . . 177
Letting Users Select Setting Attachment Viewing Options. . . . . 178
Zimbra Web Client UI Themes . . . . . 178
Zimbra Mobile. . . . . 179
Configuring Zimlets for Accounts . . . . . 179

Other Account Configuration Preferences . . . . . 180

**13 Managing Zimbra Mobile . . . . . 181**

Setting Up Mobile Devices . . . . . 182
Setting up Mobile Device Security Policies . . . . . 183
Setting Mobile Device Policies Attributes . . . . . 184
Users' Mobile Device Self Care Features . . . . . 184
Changing Mobile Device Password Policy . . . . . 185

**14 Managing Zimlets . . . . . 187**

Accessing Zimlets . . . . . 188
Default Zimlets included in ZCS . . . . . 188
Zimlets from the Zimbra Gallery . . . . . 189
Developing Customized Zimlets . . . . . 189
Deploying Zimlets . . . . . 189
Deploying a Zimlet from the Admin Console . . . . . 189
Deploying a Zimlet from the CLI . . . . . 190
Adding Proxy Allowed Domains to a Zimlet . . . . . 191
Adding Proxy Allowed Domains to a Zimlet using the CLI . . . . . 191
Deploying a Zimlet and Granting Access to a COS . . . . . 192
Enabling, Disabling, or Making Zimlets Mandatory . . . . . 192
Default Zimlets . . . . . 192
Toggling a Zimlet between Enabling and Disabling . . . . . 193
Disabling a Zimlet using the CLI . . . . . 194
Undeploying Zimlets . . . . . 195
Undeploying a Zimlet from the Admin Console . . . . . 195
Undeploying a Zimlet using the CLI . . . . . 196
Configuring Zimlets . . . . . 196
Changing Zimlet Configurations . . . . . 196
Viewing Zimlet Status . . . . . 197
Viewing Zimlet status using the Admin Console . . . . . 197
Viewing Zimlet Status using the CLI . . . . . 197
Upgrading a Zimlet . . . . . 197
Upgrading a Zimlet . . . . . 197

**15 Monitoring ZCS Servers . . . . . 199**

Zimbra Logger . . . . . 200
Reviewing Server Status . . . . . 201
Server Performance Statistics . . . . . 201
Generating Daily Mail Reports . . . . . 202
Monitoring Disk Space . . . . . 203
Monitoring Servers . . . . . 203
Monitoring Mail Queues . . . . . 204
Flushing the Queues . . . . . 205
Monitoring Mailbox Quotas . . . . . 205
Monitoring Authentication Failures . . . . . 206
Log Files . . . . . 206
Syslog . . . . . 207
Using log4j to Configure Logging . . . . . 208
Logging Levels . . . . . 208
Protocol Trace . . . . . 210
Reviewing mailbox.log Records . . . . . 210

Reading a Message Header . . . . . 215
SNMP . . . . . 216
SNMP Monitoring Tools . . . . . 216
SNMP Configuration. . . . . 216
Errors Generating SNMP Traps . . . . . 216
Checking MySQL . . . . . 216
Checking for Latest ZCS Software Version . . . . . 216
Updating ZCO Connector msi on ZCS Downloads Page . . . . . 217

**16 Backup and Restore . . . . . 219**

Zimbra Backup Methods . . . . . 220
Standard Backup Method. . . . . 220
Auto-Grouped Backup Method. . . . . 221
Directory Structure for Backup Files . . . . . 221
Backup and Restore Using the Administration Console . . . . . 223
Standard Backup Method. . . . . 223
Auto-grouped Backup Method . . . . . 223
Configure Backup from the Admin Console. . . . . 224
Backup and Restore Using the Command Line Interface . . . . . 225
Backing up using the Standard Method . . . . . 225
Scheduling Backups. . . . . 225
Full Backup Process. . . . . 227
Incremental Backup Process . . . . . 228
Finding Specific Backups. . . . . 229
Aborting Full Backup In Progress . . . . . 229
Backing up using the Auto-Grouped Method . . . . . 230
Configure Auto-Grouped Backup from the CLI . . . . . 230
Scheduling Backups. . . . . 230
Backup Options . . . . . 231
Backup Up content Options . . . . . 231
Backing up MySQL Database . . . . . 232
Managing Disk Space for Backups . . . . . 232
Restoring Data . . . . . 233
Restore Process. . . . . 233
Stopping a Restore Process. . . . . 235
Offline Restore Process . . . . . 235
Restoring Individual Accounts on a Live System . . . . . 236
Selectively Restore Items. . . . . 237
Restoring the LDAP Server . . . . . 237
Disaster Recovery for Specific Situations . . . . . 238
General Steps for Disaster Recovery. . . . . 238
Crash Recovery Server Startup . . . . . 238
Restore the Zimbra Collaboration Server. . . . . 238
Preparing the New Server . . . . . 239
Restoring from Different Failure Scenarios . . . . . 242
Changing Local Configuration Files after Restoring Zimbra. . . . . 243
Using snapshots to backup and restore . . . . . 243

**17 Zimbra Archiving and Discovery . . . . . 245**

How Archiving Works . . . . . 246
How Discovery Works . . . . . 247
Installing Archiving Package as an Update to ZCS . . . . . 248
Installing zimbra-archiving in a Single-Server Environment. . . . . 248

Installing zimbra-archiving in a Multi-Server Environment . . . . . 248
Enable archiving on each MTA . . . . . 250
Creating Dedicated Archive COS in a Multi-Server Environment . . . . 250
Using the Administration Console . . . . . 250
Using CLI . . . . . 251
Archiving Attribute . . . . . 252
Attributes configured on users' account . . . . . 252
Archive Account Name Templates . . . . . 252
Creating Archive Mailboxes . . . . . 253
Create an archive mailbox and assign a COS . . . . . 253
Create an archive mailbox with no COS or password . . . . . 253
Enable archive forwarding to a third-party archiving server . . . . . 254
Searching Across Mailboxes . . . . . 254
Cross Mailbox Search from the Administration Console . . . . . 254
Search using the Command Line Interface . . . . . 255

**18 Changing ZWC Theme Colors and Logo . . . . . 257**

Customizing Base Theme Colors . . . . . 257
Replacing the ZWC Logo . . . . . 258
Using Command Line Interface . . . . . 259
Add Your Logos . . . . . 260
Changing Theme Colors and Logo from the Admin Console . . . . . 261
Changing Base Theme Colors . . . . . 261
Adding Your Logo. . . . . 261

Appendix A Command-Line Utilities . . . . . 263

General Tool Information . . . . . 263
Zimbra CLI Commands . . . . . 264
Using non-ASCII Characters in CLIs . . . . . 269
zmprov (Provisioning) . . . . . 269
zmaccts . . . . . 283
zmarchiveconfig . . . . . 283
zmarchivectl . . . . . 284
zmarchivesearch . . . . . 284
zmbackup . . . . . 285
zmblobchk . . . . . 288
zmcalchk . . . . . 289
zmschedulebackup . . . . . 290
zmbackupabort . . . . . 293
zmbackupquery . . . . . 293
zmrestore . . . . . 295
zmrestoreoffline (Offline Restore) . . . . . 297
zmrestoreldap . . . . . 299
zmcontrol (Start/Stop/Restart Service) . . . . . 300
zmmailboxmove (Move Mailbox 7.1.2 or earlier) . . . . . 301
zmmboxmove (7.1.3 or later) . . . . . 303
zmmboxmovequery . . . . . 303
zmpurgeoldmbox . . . . . 303
zmmboxsearch (Cross Mailbox Search) . . . . . 304
zmcertmgr . . . . . 305
zmgsautil . . . . . 306
zmldappasswd . . . . . 307

zmlocalconfig . . . . . 308
zmmailbox . . . . . 309
zmtlsctl . . . . . 312
zmhsm . . . . . 313
zmlicense . . . . . 313
zmmetadump . . . . . 314
zmmypasswd . . . . . 314
zmplayredo . . . . . 314
zmproxyconfgen . . . . . 315
zmproxypurge . . . . . 316
zmredodump . . . . . 317
zmskindeploy . . . . . 318
zmsoap . . . . . 318
zmstat-chart . . . . . 319
zmstat-chart-config . . . . . 321
zmstatctl . . . . . 321
zmthrdump . . . . . 322
zmtrainsa . . . . . 322
zmtzupdate . . . . . 323
zmvolume . . . . . 323
zmzimletctl . . . . . 324
zmproxyconfig . . . . . 325
zmsyncreverseproxy . . . . . 328

Appendix B Configuring SPNEGO Single Sign-On for ZCS . . . . . 331

Configuration Process . . . . . 331
Create the Kerberos Keytab File . . . . . 332
Configure ZCS . . . . . 334
Configure Your Browser . . . . . 337
Test your setup . . . . . 337
Troubleshooting setup . . . . . 338

Appendix C ZCS Crontab Jobs . . . . . 341

How to read the crontab . . . . . 341
ZCS Cron Jobs . . . . . 341
Jobs for crontab.store . . . . . 342
Jobs for crontab.logger . . . . . 343
Jobs for crontab.mta . . . . . 343
Single Server Crontab -l Example . . . . . 344

Appendix D Glossary . . . . . 347

Index . . . . . 353

# 1 Introduction

Zimbra Collaboration Server (ZCS) is a full-featured messaging and collaboration solution that includes email, address book, calendaring, tasks, and Web document authoring.

Topics in this chapter include:


- Intended Audience
- Zimbra Collaboration Server License
- Available Documentation
- Support for Recommended Third-Party Components
- Support and Contact Information


## Intended Audience

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

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

## Zimbra Collaboration Server License

- **Trial Extended**. You can obtain the Trial Extended license from the Zimbra license portal for free, similar to a trial license. This license allows you to create up to 50 users and is valid for an extended period of time.
- **Regular**. You must purchase the Zimbra Regular license. This license is valid for a specific Zimbra Collaboration Server and is encrypted with the number of Zimbra accounts (seats) you have purchased, the effective date, and expiration date of the regular license.

- **Perpetual**. You must purchase the Zimbra Perpetual license. This license is similar to a subscription license and is valid for a specific Zimbra Collaboration Server, is encrypted with the number of Zimbra accounts (seats) you have purchased, the effective date, and an expiration date of 2099-12-31. When you renew your support agreement, no new perpetual license is sent to you, but your Account record in the Zimbra systems is updated with your new support end date.

### Obtaining a License

Go to Zimbra's Website to obtain a trial license from the Network Downloads area. Contact Zimbra sales regarding a trial extended license, or to purchase a regular license or perpetual license, by emailing sales@zimbra.com or calling 1-650-427-5701.

The regular and perpetual license can only be installed on the ZCS system for which it is purchased. Only one Zimbra license is required for your Zimbra Collaboration Server environment. This license sets the number of accounts that can be created.

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

## Available Documentation

The following ZCS documentation is available:

- ***Installation Guide*s**. Installation guides for single server and multi-server installation, include system requirements and server configuration instructions.
- ***Administrator Guide***. This guide provides a comprehensive product overview, including architecture, server functionality, administration tasks, configuration options, and monitoring tools.
- ***Zimbra Migration Wizard Guides***. The guides provide 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 ZWC.
- ***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 Server architecture overview in the Product Overview chapter as officially tested and certified for the Zimbra Collaboration Server. This document may occasionally note when other tools are available in the marketplace, but such mention does not constitute an endorsement or certification.

## Support and Contact Information

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

- Contact sales@zimbra.com to purchase Zimbra Collaboration Server
- 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 at www.zimbra.com/forums, to participate and learn more about the Zimbra Collaboration Server

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.

# 2 Product Overview

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

Topics in this chapter include:


- Core Functionality
- Zimbra Components
- System Architecture
- Example of a Typical Multi-Server Configuration


The Zimbra Collaboration Server 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,
- **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 Server 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 calendars, email folders, address books, and Briefcase folders 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 completion.

## Zimbra Components

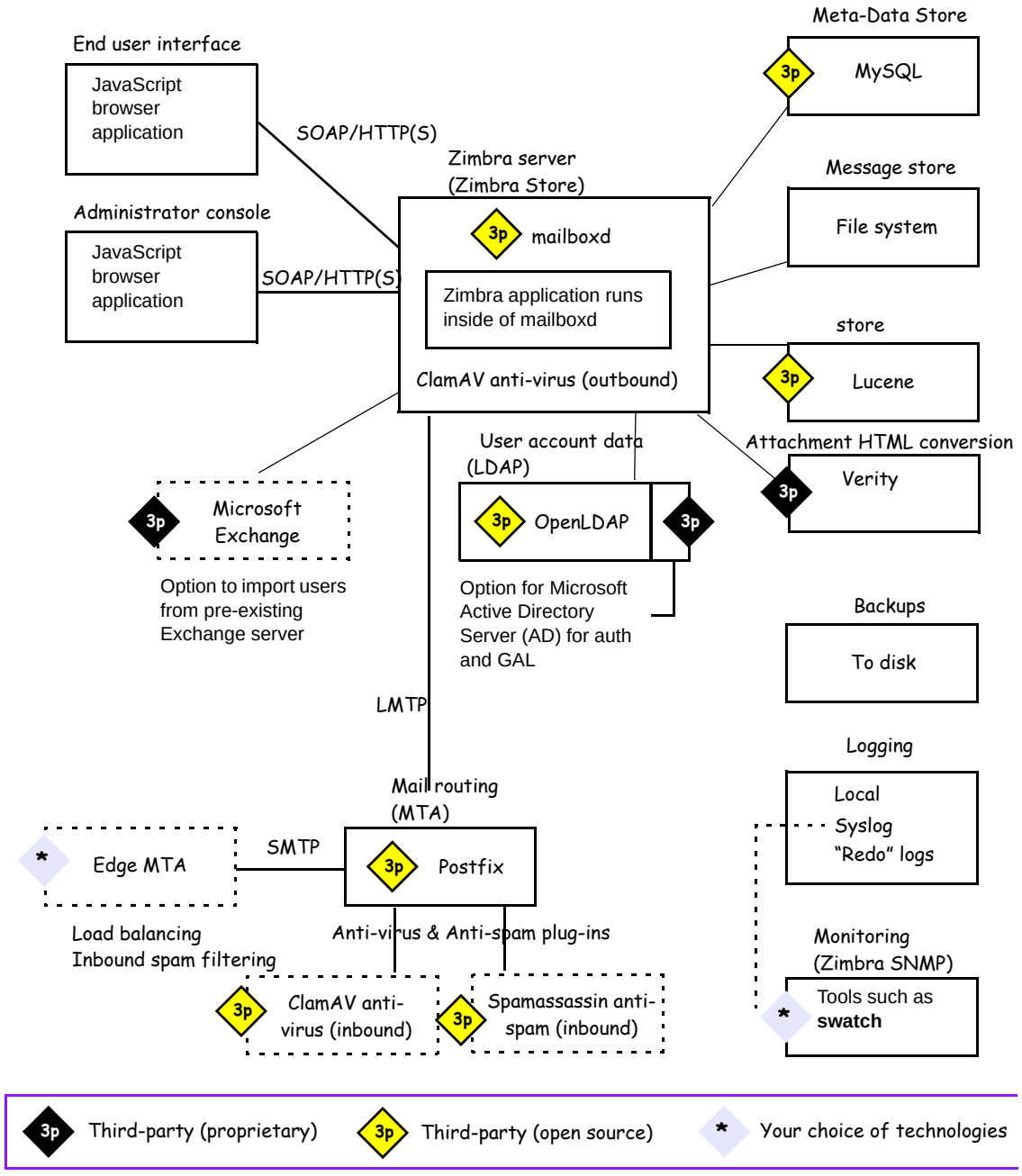
Zimbra architecture includes open-source integrations using industry standard protocols. The third-party software listed below is bundled with Zimbra software and installed as part of the installation process. These components have been tested and configured to work with the software.

- Jetty, the web application server that Zimbra software runs in.
- Postfix, an open source mail 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, a mail filter that attempts to identify spam
  - Amavisd-new interfaces between the MTA and one or more content checkers
- James/Sieve filtering, used to create filters for email

## System Architecture

The following diagram shows ZCS architectural design, including the open-source software bundled with the Suite and other recommended third-party applications.

### Zimbra Collaboration Server System Architecture




## Zimbra Packages

The Zimbra Collaboration Server includes the following application packages.

### Zimbra Core

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

zmconfigd is part of zimbra-core and is automatically enabled and runs on all systems.

### 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

ZCS 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 ZCS.

### Zimbra MTA

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 Backup and Restore on page 219.

## Zimbra System Directory Tree

The following table lists the main directories created by the Zimbra installation packages.

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

### Directory Structure for Zimbra Components

***Note:*** *The directories not listed in this table are libraries used for building the core Zimbra software or miscellaneous third-party tools.*

| 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 |
| | **data/** | Includes data directories for LDAP, mailboxd, postfix, amavisd, clamav |
| | **db/** | Data Store |
| | **docs/** | SOAP txt files and technical txt files |
| | **dspam/** | DSPAM antivirus |
| | **extensions-extra/** | Server extensions for different authentication types |
| | **extensions-network-extra/** | Server extensions for different network version authentication types |
| | **httpd/** | Contains the Apache Web server. Used for both aspell and convertd as separate processes |
| | **index/** | Index 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 |

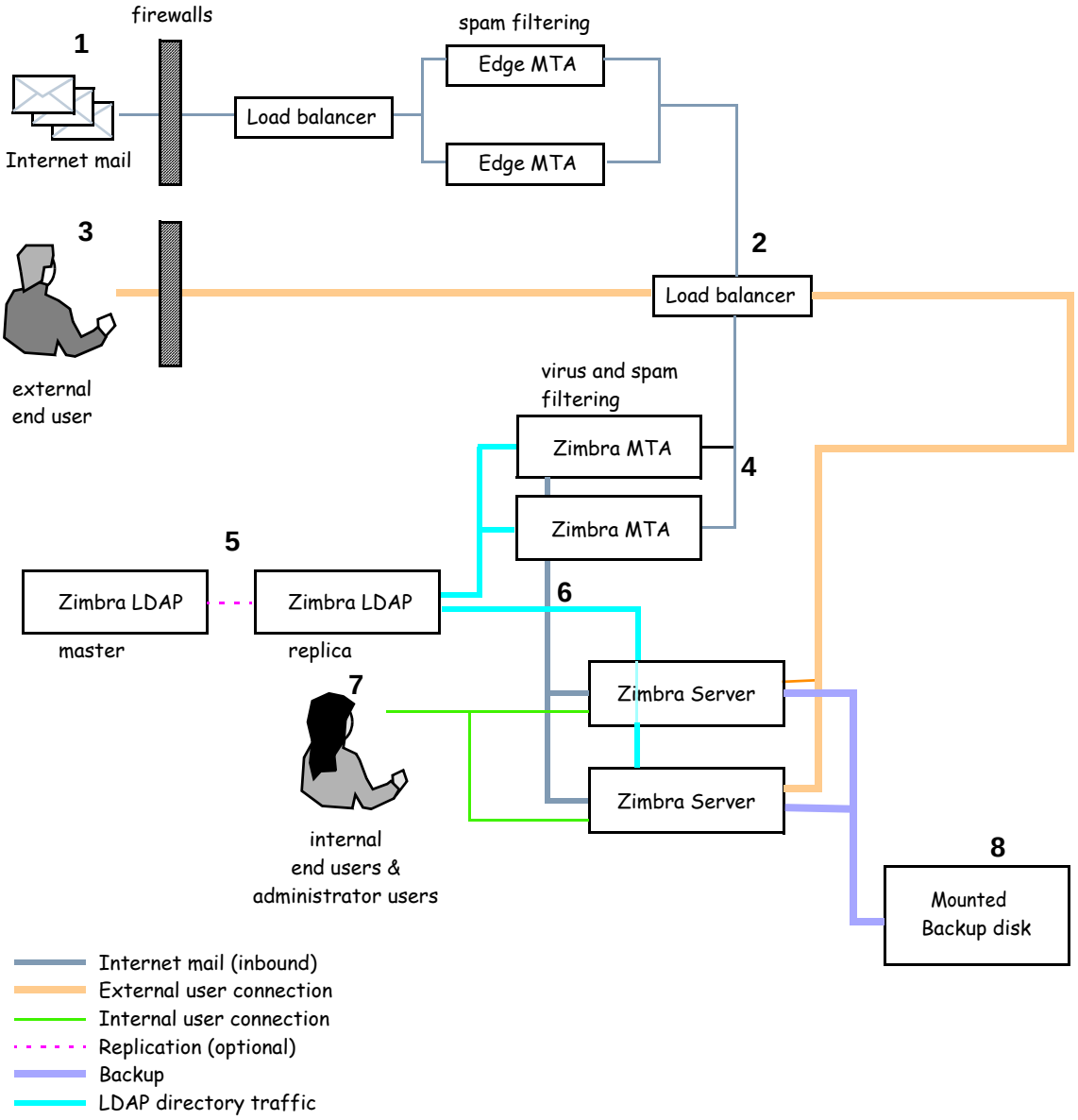
| Parent | Directory | Description |
|---|---|---|
| | **libexec/** | Internally used executables |
| | **log/** | Local logs for Zimbra server application |
| | **logger/** | RRD and SQLite data files for logger services |
| | **mysql/** | MySQL database files |
| | **net-snmp/** | Used for collecting statistics |
| | **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 |
| | **rlfe/** | A readline front-end processor provides input line editing for programs. |
| | **snmp/** | SNMP monitoring files |
| | **ssl/** | Certificates |
| | **store/** | Message store |
| | **zimbramon/** | Contains the control scripts and Perl modules |
| | **zimlets/** | Contains Zimlet zip files that are installed with Zimbra |
| | **zimlets-admin-extra/** | Admin extension not installed by the installer and not officially supported for ZCS |
| | **zimlets-deployed/** | Contains Zimlets that are available with the Zimbra Web Client |
| | **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.

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

**Typical Configuration with Incoming Traffic and User Connections**




Explanation of the above figure are:

| | |
|---|---|
| 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. |

# 3 Zimbra Mailbox Server

The Zimbra mailbox server is a dedicated server that manages all of the mailbox content, including messages, contacts, calendar, Briefcase files and attachments.

Topics in this chapter include:

- Zimbra Licenses
- Incoming Mail Routing

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 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 Server License on page 11 for a description of the license types.

The regular and perpetual license can only be installed on the Zimbra system for which it is purchased. Only one Zimbra license is required for your ZCS 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 313 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 ZCS 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 113.

### 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:

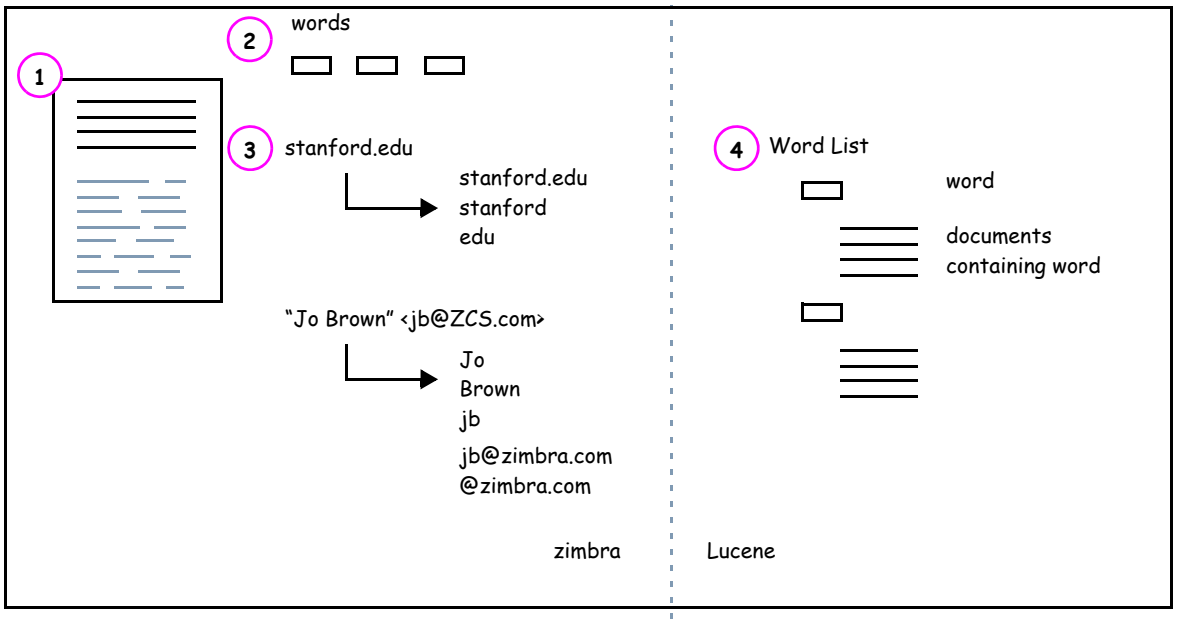
- Mailbox-account mapping. The primary identifier within the Zimbra database is the mailbox ID, rather than a user name or account name. The mailbox ID is only unique within a single mailbox server. The Data Store maps the Zimbra mailbox IDs to the users' OpenLDAP accounts.
- Each user's set of tag definitions,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

### 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 the Message Tokenization figure.*

## 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 Backup and Restore on page 219.

### 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 logs are read to re-apply any uncommitted transactions.

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

### Log

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

Selected Zimbra log messages generate SNMP traps, which you can capture using any SNMP monitoring software. See Monitoring ZCS Servers on page 199.

# 4 Zimbra LDAP 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.

Topics in this chapter include:

- Directory Services Overview
- Zimbra Schema
- Account Authentication
- Zimbra Objects
- Company Directory/GAL
- Flushing LDAP Cache

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

The LDAP server is installed 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 zmprov CLI utility.

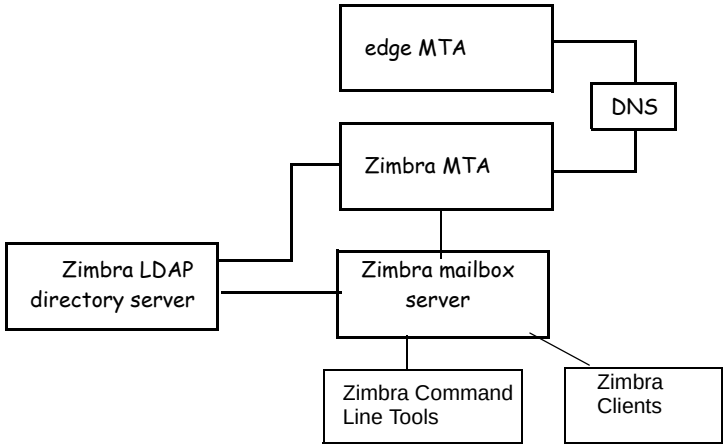
## Directory Services Overview

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.

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

**LDAP Directory Traffic**



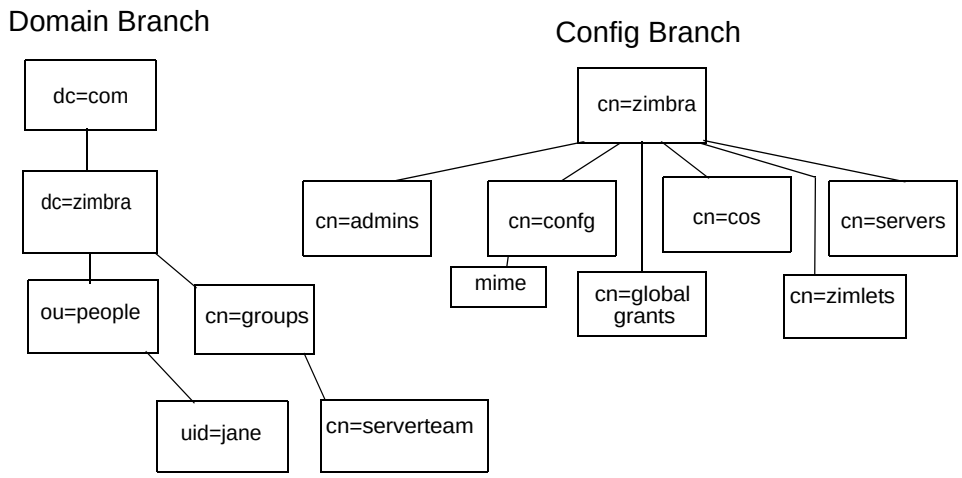

At the core of every LDAP implementation is a database organized using a *schema*. The schema specifies the types of objects that are stored in the database, and what types of attributes they have.

## LDAP Hierarchy

LDAP directories are arranged in an hierarchal tree-like structure with two types of branches, the mail branches and the config branch. Mail branches are organized by domain. Entries belong to a domain, such as accounts, groups, aliases, are provisioned under the domain DN in the directory. The config branch contains admin system entries that are not part of a domain. Config branch entries include system admin accounts, global config, global grants, COS, servers, mime types, and zimlets.

The following figure shows the Zimbra LDAP hierarchy. Each type of entry (object) has certain associated object classes.

**Zimbra LDAP Hierarchy**




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.

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. An entry with the structural object class **zimbraServer** would be a server in the Zimbra system that has one or more Zimbra packages installed.

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

## Zimbra Schema

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.

All attributes and object classes specifically created for Zimbra are prefaced by "zimbra," as in **zimbraAccount** 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
- amavisd.schema
- dyngroup.schema
- nis.schema

***Note:*** *You cannot modify the Zimbra schema.*

## Account Authentication

This section describes the following account authentication mechanisms and formatting directives that are 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://ldapserver:port/**

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

Examples include:

**ldap://server1:3268**
**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.

### zimbraAuthFallbackToLocal Attribute

The **zimbraAuthFallbackToLocal** attribute can be enabled so that the system falls back to the ZCS local authentication if external authentication fails. The default is FALSE.

## 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, **zimbraAuthMet 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", than 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 **ZimbraCustomAuth .authenticate** (). 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 Accounts 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 Managing User Accounts on page 133.

### 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 object, 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

The **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 Managing 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 **zimbraIdentity**.

### 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.

Attributes Mapped to Zimbra Contact table maps generic GAL search attributes to their Zimbra contact fields.

**Attributes Mapped to Zimbra Contact**

| Standard LDAP Attribute | Zimbra Contact Field |
|---|---|
| co | workCountry |
| company | Company |
| givenName/gn | firstName |
| sn | lastName |
| cn | fullName |
| initials | initials |
| l | workCity |
| street, streetaddress | workStreet |
| postalCode | workPostalCode |
| telephoneNumber | workPhone |
| st | workState |
| title | jobTitle |
| mail | email |
| objectClass | Not currently mapped |

### Zimbra GAL Search Parameters

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

### Modifying Attributes

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

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

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

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

## Converting OpenLDAP back-hdb to OpenLDAP back-mdb

You can convert existing LDAP nodes that are using the deprecated OpenLDAP back-hdb backend to OpenLDAP back-mdb backend that is used in ZCS 8 and later.

The steps to perform this task include running a script on an existing LDAP server as the Zimbra user. This script stops all services on the server performing the migration. Prior to migrating, verify the server has enough disk space as there will be two LDAP databases present on disk post-migration. The original back-hdb database can be removed after verifying the migration is successful.

To migrate to OpenLDAP back-mdb:

1. Upgrade all deployed LDAP servers to ZCS 7.2.6 or later
2. After the upgrade completes, on each LDAP server you want to convert run **./libexec/zmldapconvertmdb**

The script will perform the following:

- Stop zimbra (zmcontrol stop).
- Export the cn=config, accesslog (if this is a master), and primary databases to /opt/zimbra/data/tmp/mdb-conversion/
- Backup the existing raw databases by renaming them:

  data/ldap/config -> data/ldap/config.hdb.
  data/ldap/accesslog -> data/ldap/accesslog.hdb.
  data/ldap/hdb -> data/ldap/hdb.pre-mdb.
- Convert the cn=config DB to use back-mdb.
- Update localconfig for the values used by back-mdb (ldap_db_maxsize, ldap_accesslog_maxsize).
- Import the cn=config, accesslog (if this is a master), and primary databases.

3. After the migration is complete, it is suggested to run **ldap start** to validate ldap starts correctly.
4. Run **zmcontrol start** to bring up the remaining services.
5. When the migration is successful, the **data/tmp/mdb-conversion** can be removed, and the **data/ldap/config.hdb**, **data/ldap/accesslog.hdb**, and **data/ldap/hdb.pre-mdb** directories can also be removed.

***Note:*** *Any newly deployed LDAP servers in ZCS 7 will continue to default to using back-hdb, and will need to be converted to back-mdb if desired after being deployed.*

## 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 themes (skins) 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 to update the server is 15 minutes. This setting can be changed from zmlocalconfig. To see the setting run the zmlocalconfig command, . Type as* **zmlocalconfig ldap_cache_<object>_maxage**.

- 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.

The CLI, zmprov describe can be run to determine if the action requires a restart. Type **zmprov desc -a <attributename>**. Note the **requiresRestart** value in the output.

***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 zimbraImapClearTextLoginEnabled**.

   ***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**

# 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.

Topics in this chapter include:

- Zimbra MTA Deployment
- MTA Functionality
- Receiving and Sending Mail through Zimbra MTA

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) with learned data stored in /opt/zimbra/data/amavisd or an alternative MySQL database.
- Amavisd-New, a Postfix content filter used as an interface between Postfix and ClamAV / SpamAssassin.
- Milter servers filter applications that can be configured to filter email ReciptTo content for alias domains and to filter restricted sender addresses for distribution lists.

In the Zimbra Collaboration Serverconfiguration, mail transfer and delivery are distinct functions. Postfix primarily acts as a 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.

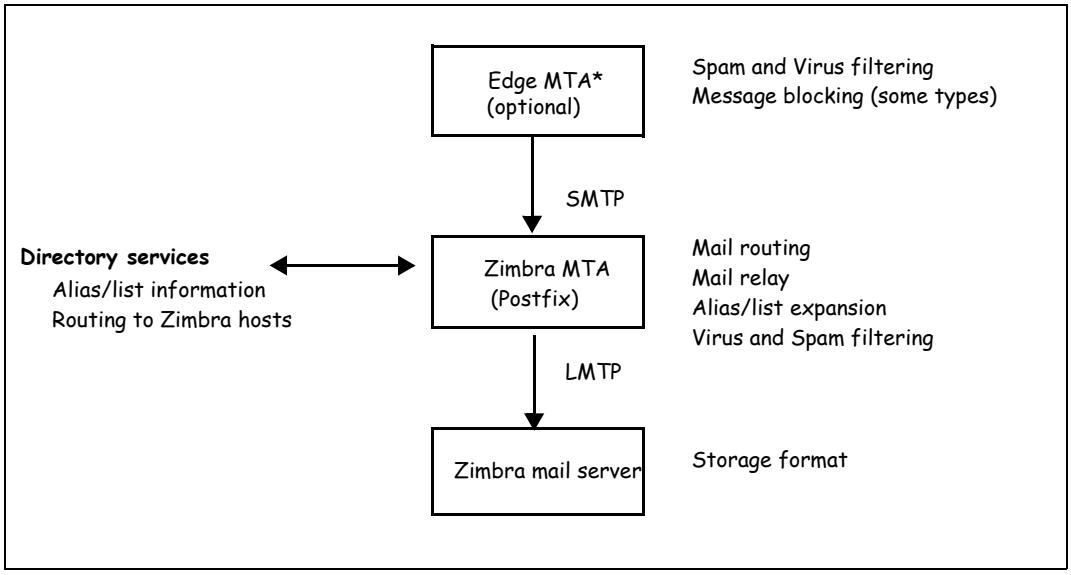
## Zimbra MTA Deployment

ZCS 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. 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.

**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 ZCS:

- **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 a 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 ZCS 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, and Briefcase files contribute to the quota. Account quotas can be set by COS or per account.

How message delivery is handled when a Zimbra user's mailbox exceeds the set quota is set either by the COS or for individual accounts. The MTA can be configured to either send the message to the deferred queue or send the message to the mailbox, even if the quota has been exceeded.

- Temporarily send the message to the deferred queue to be delivered when the mailbox has space is the default behavior.

  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.*

- Delivering the message to the mailbox that exceeds its quota can be configured in the **zimbraMailAllowReceiveButNotSendWhenOverQuota** attribute.

  When this attribute is set to TRUE, a mailbox that exceeds its quota is still allowed to receive new mail and calendar invites.

  This quote bypass is only implemented for messages. All other mail items are still affected by the quota.

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 ZCS as the virus protection engine. The anti-virus protection is enabled for each server and a global virus quarantine mailbox is created during installation.

The Clam anti-virus software is configured to quarantine messages that have been identified as having a virus to the virus quarantine mailbox. An email notification is sent to recipients letting them know that a message has been quarantined. The message lifetime for this mailbox is 30 days.

By default, the Zimbra MTA checks every two hours for any new anti-virus updates from ClamAV.

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

### Anti-Spam Protection

SpamAssassin, a mail filter that attempts to identify unsolicited commercial email (spam) with learned data stored in either the Berkeley DB database or a MySQL database.

***Note:*** *For information about how to customize SpamAssassin, see the Zimbra wiki article SpamAssassin Customizations.*

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. The ZCS default is to use data in the Berkeley DB database.

SpamAssassin can alternatively be configured to use a MySQL-backed database for spam training. To use this method, set **zmlocalconfig antispam_mysql_enabled** to TRUE on the MTA servers. When this is enabled, Berkeley DB database is not enabled. See the Scalable Anti-Spam Using Spamassassin and MySQL wiki article at wiki.zimbra.com.

***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 spam, but should be.
- **Non-spam (referred to as ham) training user** to receive mail notification about mail that was marked as spam, 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 spam or not spam by sending them to their junk 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 spam or not spam 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 Spam. 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 defaults 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**

4. Restart, type **postfix start**

### Email Recipient Restrictions

RBL (Real-time black-hole lists) can be turned on or off in the Zimbra MTA from the administration console or using the Zimbra CLI. From the administration account go to the Global Settings>MTA tab.

For protocol checks, the following three RBLs can be enabled:

- Hostname in greeting violates RFC - reject_invalid_hostname
- Client must greet with a fully qualified hostname - reject_non_fqdn_hostname
- Sender address must be fully qualified - 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

As part of recipient restrictions, you can also use the **reject_rbl_client <rbl hostname>** option. In the **Global Settings>MTA>DNS checks** section on the administration console specify the list of RBLs. For a list of current RBL's, see the *Comparison of DNS blacklists* article at http://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists.

### Adding RBLs using the CLI

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

   **zmprov mcf zimbraMtaRestriction [RBL type]**

   To add all the possible restrictions, the command would be

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

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

## Receiving and Sending Mail through Zimbra MTA

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

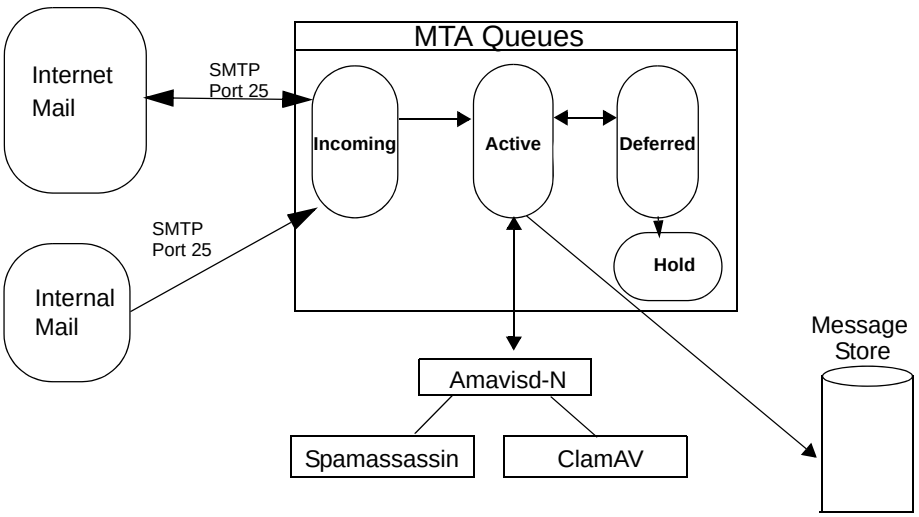
remote host. For incoming messages, the MTA must be able to accept connection requests from remote mail servers and receive messages for the local users.

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

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

### Zimbra MTA Message Queues

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




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

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

**Deferred.** Messages that cannot be delivered for some reason are placed in the deferred queue. The reasons for the delivery failures are 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 five days. You can change the default MTA value for **bounce_queue_lifetime** from the **zmlocalconfig** CLI.

Before the bounce queue lifetime sends the message back to the sender, senders can be notified that the message they sent is in the Deferred queue and has not been delivered. This is set up from the **zmlocalconfig** CLI. The following attributes are configured to send a warning message to the sender:

- **postfix_delay_warning_time=0h**.The time after which the sender receives the message headers of email that is still queued.
- **postfix_bounce_notice_recipient=postmaster**. The recipient of postmaster notifications with the message headers of mail that the MTA did not deliver.
- **postfix_notify_classes=resource,software**. The list of error classes that are reported to the postmaster.

***Note:*** *See Postfix documentation for details on the impact of changes to these Postfix attributes.*

**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 204.

# 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.

Topics in this chapter include:

- Zimbra Proxy Components
- Zimbra Proxy Architecture and Flow
- Customizing Zimbra Proxy Configuration
- Zimbra IMAP/POP Proxy
- Configuring ZCS HTTP Proxy
- Configuring Zimbra Proxy for Kerberos Authentication

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.

## 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 **zmconfigd** 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 Server (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* **zmproxyconfig -r,** *to run against a remote host. 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/zmproxyconfig -e -m -H mailbox.node.service.hostname**

This configures the following:

- **zimbraImapBindPort** to 7143
- **zimbraImapProxyBindPort** to 143
- **zimbraImapSSLBindPort** to 7993
- **zimbraImapSSLProxyBindPort** to 993
- **zimbraPop3BindPort** to 7110
- **zimbraPop3ProxyBindPort** to110
- **zimbraPop3SSLBindPort** to 7995
- **zimbraPop3SSLProxyBindPort** to 995
- **zimbraImapCleartextLoginEnabled** to TRUE
- **zimbraReverseProxyLookupTarget** to TRUE
- **zimbraPop3CleartextLoginEnabled** to TRUE

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

   **zmcontrol restart**

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:

   - **zimbraImapBindPort** to 7143
   - **zimbraImapProxyBindPort** to 143
   - **zimbraImapSSLBindPort** to 7993
   - **zimbraImapSSLProxyBindPort** to 993
   - **zimbraPop3BindPort** to 7110
   - **zimbraPop3ProxyBindPort** to110
   - **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:

- **zimbraImapBindPort** to 7143
- **zimbraImapProxyBindPort** to 143
- **zimbraImapSSLBindPort** to 7993
- **zimbraImapSSLProxyBindPort** to 993
- **zimbraPop3BindPort** to 7110
- **zimbraPop3ProxyBindPort** to110
- **zimbraPop3SSLBindPort** to 7995
- **zimbraPop3SSLProxyBindPort** to 995
- **zimbraImapCleartextLoginEnabled** to TRUE
- **zimbraReverseProxyLookupTarget** to TRUE
- **zimbraPop3CleartextLoginEnabled** to TRUE
- **zimbraReverseProxyMailEnabled** to TRUE

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

**zmcontrol restart**

## 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, Zimbra Connector for BES, and Zimbra Mobile Sync devices are also supported by the proxy.

***Note:*** *When ZCB is configured in ZCS, the proxy configuration must be changed from the directions here. See the Zimbra wiki article Installing Blackberry Enterprise Server in a Zimbra Proxy Environment at http://wiki.zimbra.com/wiki/Installing_Blackberry_Enterprise_Server_%28ZCB/BES%29_in_a_Zimbra_Proxy_Environment.*

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

   **zmcontrol restart**

3. Configure each domain with the public service host name to be used for REST URLs, 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 HTTP.

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.
   - **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 HTTP.

   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

**zmcontrol restart**

Configure each domain with the public service host name to be used for REST URLs, email and Briefcase folders. Type

**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.

### Setting Proxy Trusted IP Addresses

When proxy is configured with ZCS, each proxy server's IP address must be configured in LDAP attribute **zimbraMailTrustedIP** to identify the proxy addresses as trusted when uses log in through the proxy. The proxy IP address is added to the X-Forwarded-For header information. The **X-Forwarded-For** header is automatically added to the localconfig **zimbra_http_originating_ip_header** attribute. When a user logs in, this IP address and the user's address are verified in the Zimbra mailbox log.

You set each proxy IP address in the attribute. For example, if you have two proxy servers, you would run the command as follows:

```
zmprov mcf +zimbraMailTrustedIP {IP of nginx-1} +zimbraMailTrustedIP {IP of nginx-2}
```

***Note:*** *To verify that X-Forwarded-For was correctly added to the localconfig, type* **zmlocalconfig | grep -i http.** *You should see* **zimbra_http originating_ip_header = X-Forwarded-For***.*

## 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 Zimbra LDAP 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 restart**

# 7 Managing Legal Requests for Information

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.

Topics in this chapter include:

- Legal Intercept for Law Enforcement
- Create Mailbox Snapshots for Legal Discovery

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 for Law Enforcement

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:

| | |
|---|---|
| **zimbraInterceptAddress** | 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 |
| **zimbraInterceptSendHeadersOnly** | The default is **False**. Change to **True** to have only the message headers sent, not the message body |
| **zimbraInterceptFrom** | Used to construct the **From**: header content used in the intercept message. The default is **Postmaster@<address.com>** |
| **zimbraInterceptSubject** | 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>"** |
| **zimbraInterceptBody** | 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> zimbraInterceptAddress <account@intercept_example.gov>**
   - If enabling by account, type **zmprov ma <accountname@domain.com> zimbraInterceptAddress <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 <text> 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.

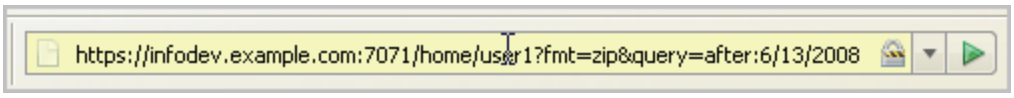
When the file is unzipped, each messages is displayed as an .eml file. The attachments are saved in the format they were delivered.

### 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 *Zimbra Web Client Search Tips* wiki page for keyword examples at *http://wiki.zimbra.com/index.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.

# 8 Using the Administration Console

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

Topics in this chapter include:

- Logging In
- Changing Administrator Passwords
- About the Administration Console
- Creating Message of the Day for Administrators
- Checking for ZCS Software Updates
- Searching from the Administration Console

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 Zimbra Collaboration Server:

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

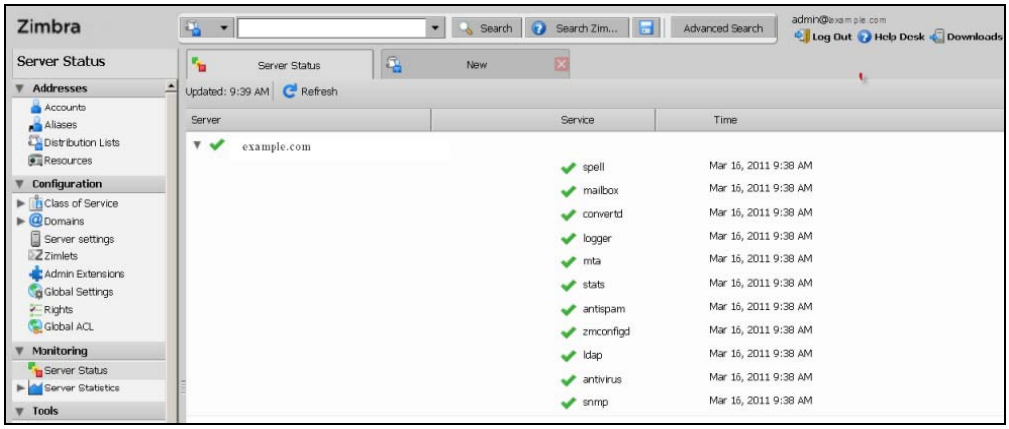
## About the Administration Console

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.
- **Search Zimbra** 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 ZCSdocumentation
- **Downloads** includes a link to download migration wizards, import wizard, and other useful downloads.

### Administration Console - Server Status Page




The Navigation pane on the left 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.
- **Account Migration**. Zimbra migration tool used to import users mailboxes, including messages, calendars, and contacts to ZCS.
- **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
- Use the account migration wizard to import many accounts at once
- 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 other Zimbra migration tools from the administration console's downloads page.

See the Managing ZCS Configuration chapter 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 for details about the commands.

- Start, stop, and restart 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.

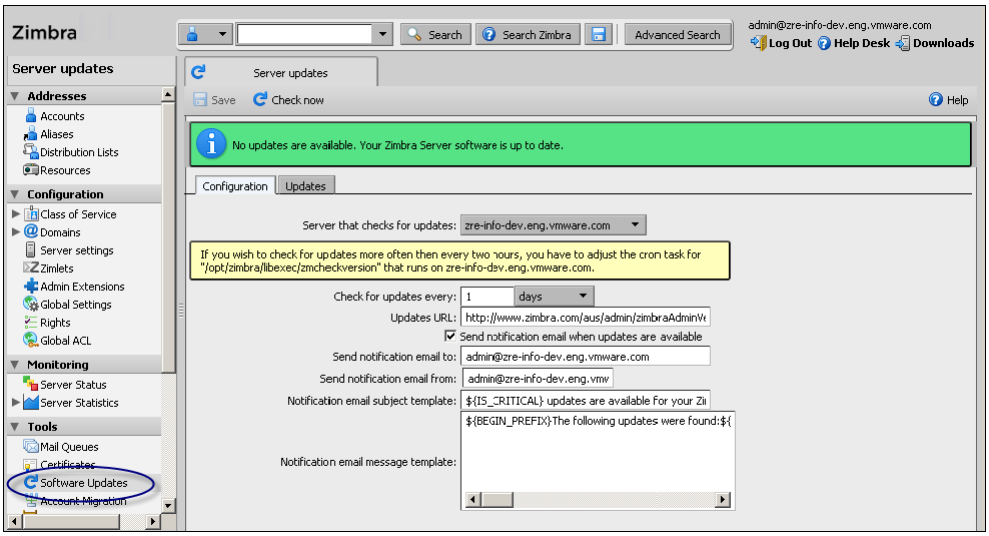
```
zmprov md domainexample.com -zimbraAdminConsoleLoginMessage "message to display"
```

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:

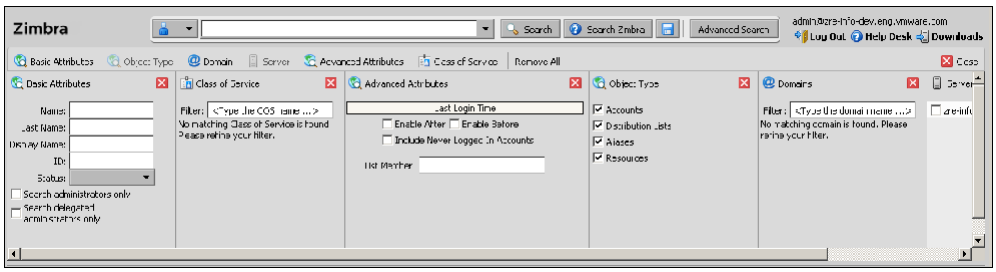
- **Server that checks for updates**. The pull-down tab lists all available servers. Only one server is configured. The selected server checks for updates and the result of the update response from www.zimbra.com is stored in LDAP.
- **Check for updates every x**. The default is to check once a day. 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.

## Searching from the Administration Console

The Search bar offers three search options:

- Search
- Zimbra Search
- Advanced Search




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

Zimbra 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. The Class of Service pane can be configured to search for a specific COS. Select the COS from the list. The COS ID is added to the Search field. When you click Search, accounts in the COS are listed in the Content pane.

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.

# 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.

Topics in this chapter include:

- Delegated Administration Terminology
- How Delegated Administration Rights are Granted
- Implementing Delegated Administration
- Revoking Rights
- Viewing Rights Granted to Administrators
- Predefined Delegated Administrator Role
- Specific Access Rights

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 logging 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 | If the right is applicable to distribution lists, the distribution list and all distribution lists under this distribution list.<br>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. |
| Domain | Domain entry is only applicable to a specific domain, not to any sub-domains.<br>Sub-domains must be explicitly marked as targets.<br>When domain is the target, the rights granted can be given for all accounts, calendar resources and distribution lists in the domain. |
| Config | Grants specific to global config |
| Global ACL | 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.<br>Delegated administrator accounts that are granted this right can create accounts in all domains in the system. |
| 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.

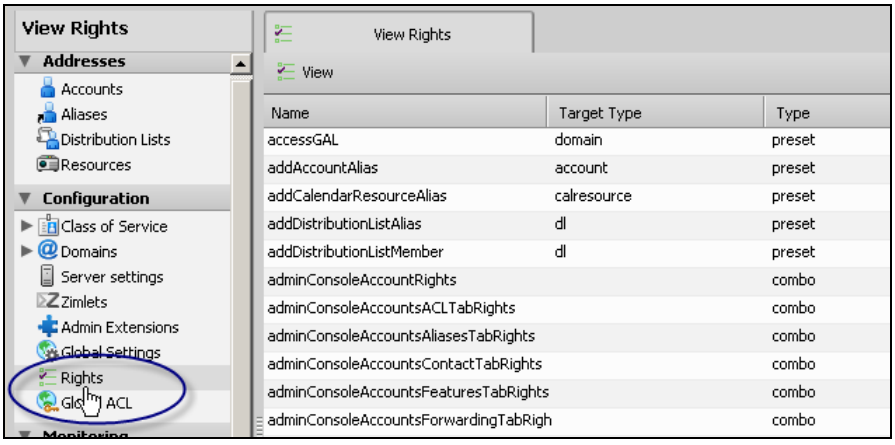
- Associated with a fixed target type. For example, createAccount is a right only on a domain; renameAccount is a right on an account; see Server is a right on a server
- Independent of other rights on the same target. No other rights are required to administer that action on the target.
- Possibly requires 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**

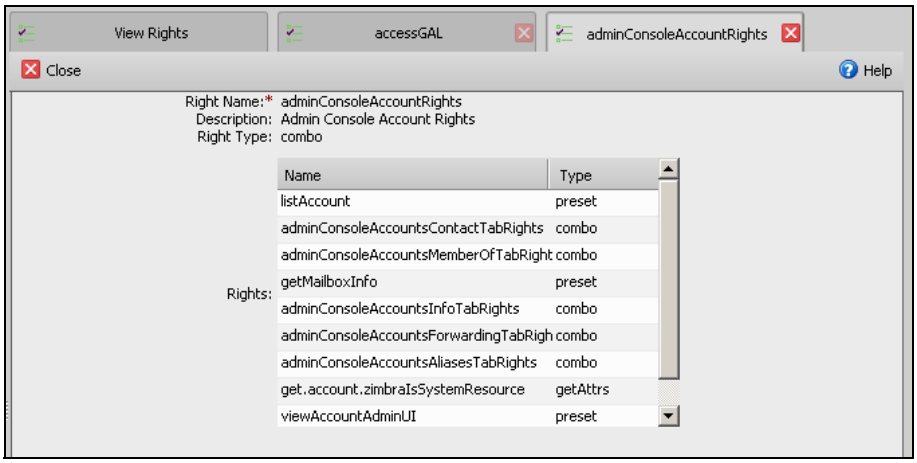



When you select a right on the page and click on it, another page displays more information

- 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.

**Combo Rights Lists.** You can use the zmprov CLI to see combo rights.

- Direct sub rights of a combo right, type as **zmprov gr adminConsoleDLRights**
- Second level sub-rights of the combo, type as **zmprov gr adminConsoleDLRights -e**

**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

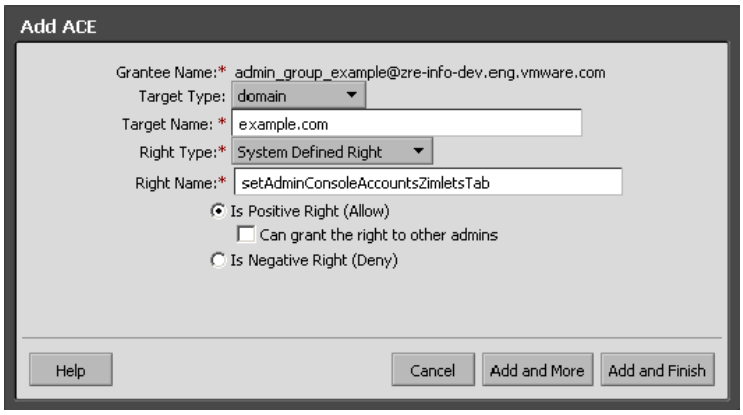
An attribute right is specific to a defined attribute. Granting rights at the attribute level allow a delegated administrator/administrator group to modify or view (or not modify or view) a specific attribute on a target.

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.




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.*

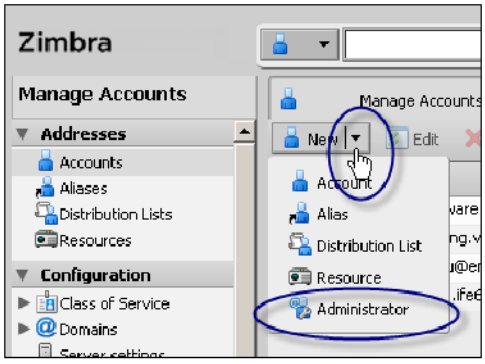
Delegated administration rights can be set up in one of the following methods:

- **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

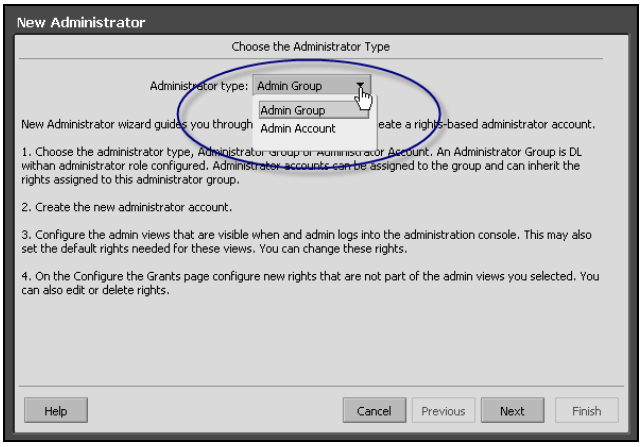
accounts, add views and grant rights. On the Accounts toolbar, select **Administrator** from the New drop-down menu.



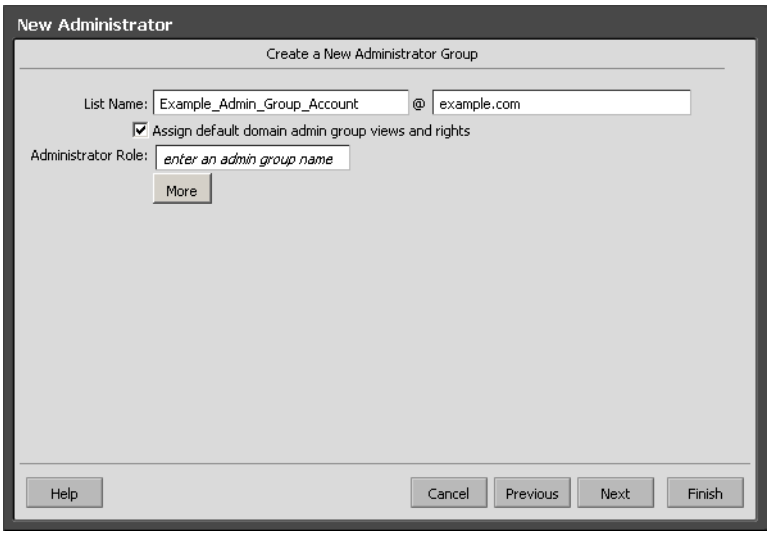

The wizard walks you through the following steps.

1. Create the administrator account, select to create either an Admin Group or an Admin Account.

   - **Admin Groups** are distribution lists (DL) that have Admin Group enabled, which flags it as a delegated administrator DL. After the admin group administrator is created and configured with rights and admin views, you add administrator user accounts to the admin group.
   - **Admin Account** is a user account that has Administrator enabled on the account.




2. Create the administrator account. For these images the Administrator Group was selected.

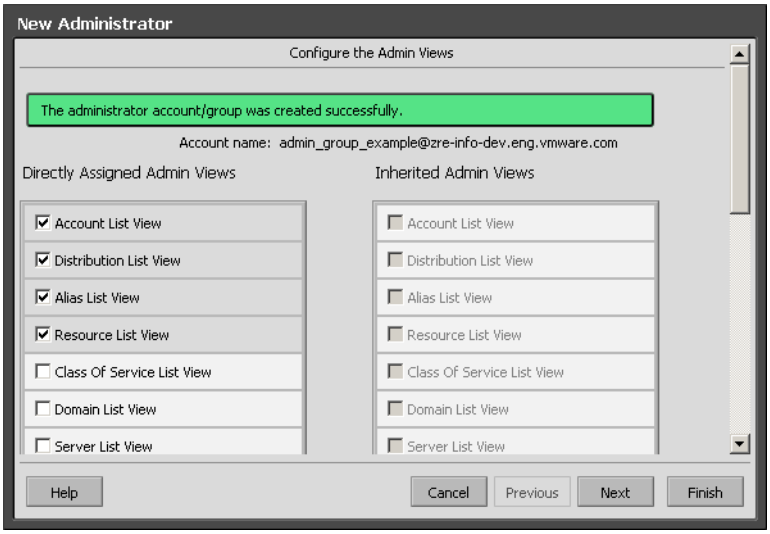



3. When you click **Next or Finish**, the account is provisioned. If you select Next you configure the admin views for the account.

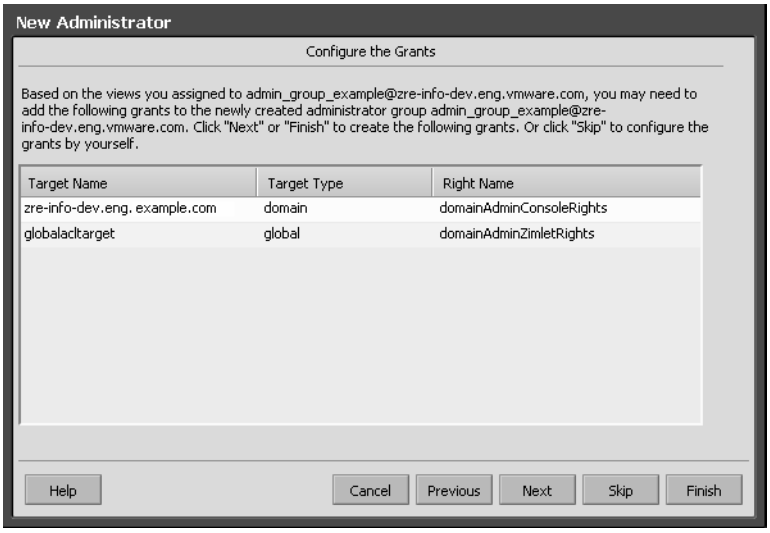
   If you selected an **Administrator Role** for this account and do not want to add other rights or views, click Finish. The account is provisioned and added to the administration group specified in the Administrator Role field.

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.

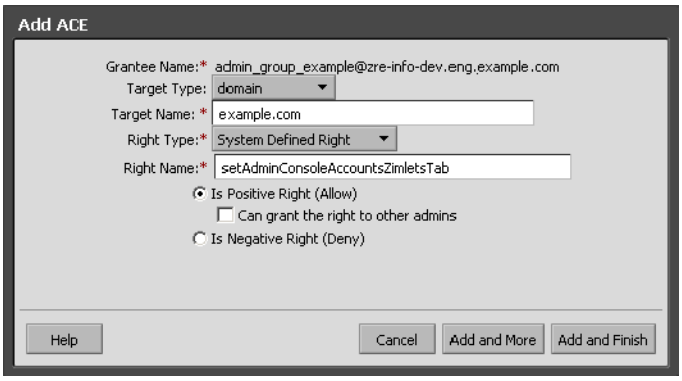
   If you had assigned an Administrator Role when you created the account, the Inherited Admin Views column would highlight the views that are inherited from the role you assigned.




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.

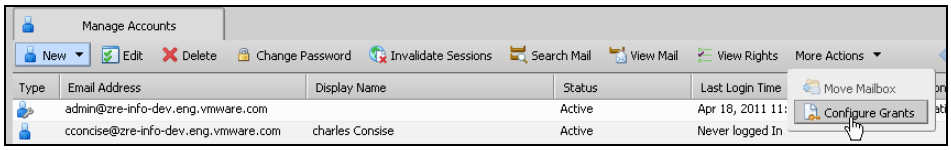



6. Click **Next** to accept the rights and add additional rights. Add access rights (ACE) to the account. Select the target type, the target name to administer, and the rights to be granted. You can add multiple rights and they can be either positive or negative.




### 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 inherited 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.

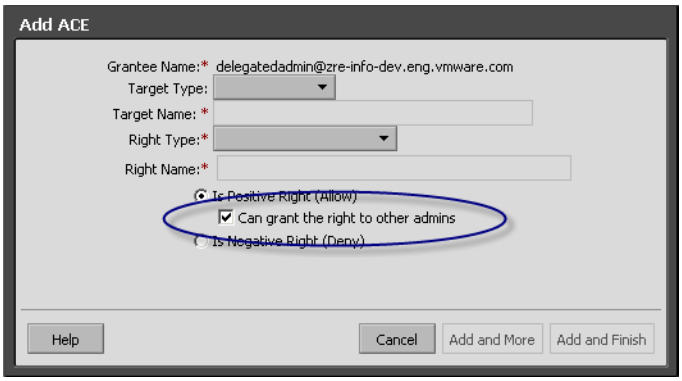
## Revoking Rights

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.




## 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




## 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

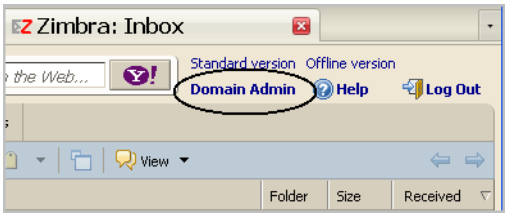
When domain administrators log onto the administration console, only the functions they are authorized to manage are displayed on the console's Navigation pane.

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 Microsoft 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.

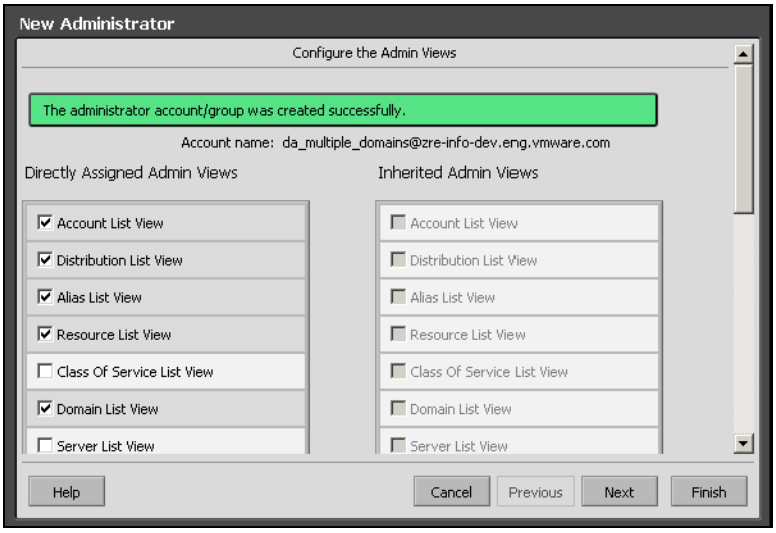
### Manage multiple domains

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.

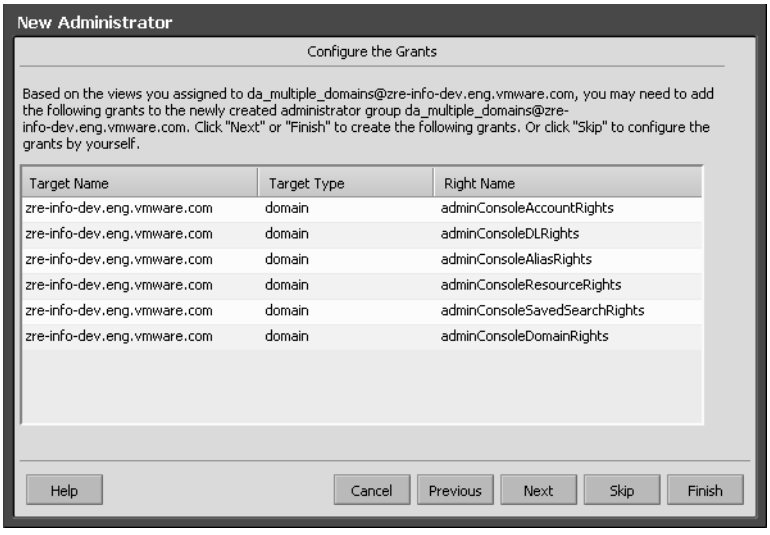
For example, to set up domanadministrator1@example.com to manage domainexample1 and domainexample2.com. Create a new administrator account on one of the domains to be managed.

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
    - Class of Service List View
    - Domain List View
    - Server List View
    - Zimlets List View
    - Global Settings View
    - Global Server Status View
    - Saved Searches View
    - Help Search View
    - Mail Queue View

- Per Server Statistics View
- Certificates View
- Software Updates
- Account Migration Cross Mailbox Search View
- Right List View
- Global ACL View
- Backups




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.

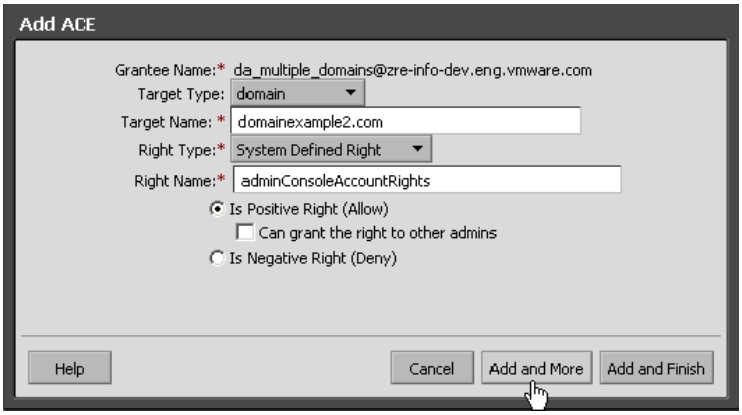



Click **Next.** The informational box shows the grants were created.

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**




   - 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**:<br>account<br>domain<br>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<br>Verb: **Write**<br>AR Target: **account** |

### 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<br>domain | server name or domain address | SD Right |
| **adminConsoleAccountsZimletsTabRights** | server<br>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 |

# 10 Managing ZCS Configuration

This chapter describes the Zimbra Collaboration Server components that you manage.

Topics in this chapter include:

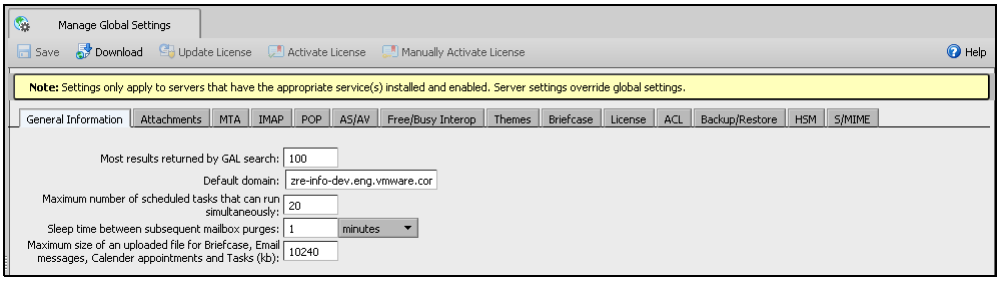
- Managing Global Configurations
- Managing Domains
- Managing Servers
- Managing Other Functions

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.

**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 Zimbra CLI Commands 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 and anti-virus options for messages received that may have a virus
- Set up free/busy scheduling across a mix of ZCS servers and third party email servers.
- Customize themes color scheme and add your logo to the themes
- Configure the company name that displays when external guests log on to see a shared Briefcase folder.
- 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 176.

  ***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 Briefcase files (kb).** This is the maximum size of a file that can be uploaded into 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 the Zimbra MTA chapter.

| | |
|---|---|
| Authentication | ■ **Authentication** should be enabled, to support mobile SMTP authentication users so that their email client can talk to the Zimbra MTA.<br>■ **TLS authentication only** forces all SMTP auth to use Transaction Level Security to avoid passing passwords in the clear. |
| Network | ■ **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.<br>■ The **Relay MTA for external delivery** is the relay host name. This is the Zimbra MTA to which Postfix relays non-local email.<br>■ 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 zimbraInboundSmtpHostname setting, if set. If this attribute is not set, the domain MX setting is checked against zimbraSmtpHostname.<br>■ MTA Trusted Networks<br>■ 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.<br>■ If **Allow domain administrators to check MX records from Admin Console** is checked, domain administrators can check the MX records for their domain. |
| Milter Server | ■ If **Enable Milter Server** is checked, the milter enforces the rules that are set up for who can send email to a distribution list. |
| Messages | ■ Set the **Maximum messages size** for a message and it's attachments that can be sent. Note: To set the maximum size of an uploaded file to Briefcase, go to the General Information tab.<br>■ 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 | ■ The **Protocol** fields are checked to reject unsolicited commercial email (UCE), for spam control. |
| DNS checks | ■ 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.<br>■ Add other email recipient restrictions to the **List of RBLs** field. |

***Note:*** *RBL (Real time black-hole lists) can be turned on or off from the Zimbra CLI. See the section* *Adding RBLs using the CLI on page 56**.*

### 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.

IMAP and POP3 polling intervals can be set from the COS>Advanced tab. The default is to not set the polling interval.

### 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 53.

RBL (Real time black-hole lists) can be turned on or off in SpamAssassin from the Zimbra CLI. See the section Adding RBLs using the CLI on page 56.

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, or 2010 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 http://wiki.zimbra.com/index.php?title=Free_Busy_Interop_for_Exchange.*

#### Exchange 2003/2007/2010 Setup Requirements.

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 email address 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 on the Global Config Free/Busy Interop tab, the Domain Free/Busy Interop tab or on 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 email address for the account. 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 Free/Busy Interop tab on the administration console. Here you configure the Exchange server settings as follows:

- Microsoft Exchange Server URL. This is the Web interface to the Exchange.
- Microsoft 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.
- Microsoft Exchange Server Type, either **WebDav** or **ews**
  - Select WebDAV to support free/busy with Exchange 2003 or Exchange 2007.

- Select ews (Exchange Web Service) to support free/busy with Exchange 2010, SP1.

- Microsoft 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.

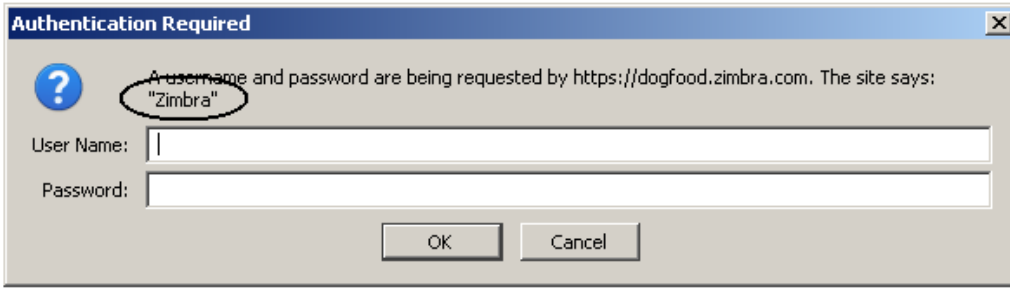
### Global Settings Advanced Tab

The features configured in the Advanced tab include:

- Replacing "Zimbra" in the Briefcase authentication dialog box.
- Configuring the email validation setting's regular expression for invalid email addresses.

### Briefcase Share Configuration

When a Briefcase folder is shared with an external guest, they must log in to view the shared item.




The Authentication Required dialog that displays references the company name "Zimbra". You can change the company name from Zimbra to your company name in the Global Settings or Domains Advanced tab.

### Setting Account Email Validation Rules

The ZCS server validates an email address or domain name using javax.mail.internet.InternetAddress when accounts, groups, or domains are created or renamed.

You can define additional email validation rules to validate email addresses for messages sent from the advanced Zimbra Web Client. This validation is done from the Zimbra Web Client.

1. Go to the administration console Global Settings Advanced tab.

2. In the **Regular expression for invalid email address** field enter a regular expression (regex) to filter out email addresses that should be considered invalid. You can add multiple regular expressions.

Example of regular expressions:

- **test@\\d+.com**. This regular expression identifies email addresses with a number in the domain name as invalid. That is test@123.com or test@1.com are not valid addresses.
- **mail@donotreply.com** (any specific address). This type of regular expression identifies a specific email address that is invalid.

***Note:*** *This validation does not work when messages are sent from the standard Zimbra Web Client.*

### 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 Changing ZWC Theme Colors and Logo on page 257 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 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 spam 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**.

***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. The **Activate License** link on the toolbar activates the license.

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. Click **Activate License**. Upgraded ZCS versions require an immediate activation to maintain network feature functionality.

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

### License Usage by ZCS Account Type

A mailbox license is required for an account assigned to a person, including accounts created for archiving. Distribution lists, aliases, locations and resources do not count against the license.

Below is a description of ZCS accounts and if they impact your license limit.

- **System accounts**. System accounts are specific accounts used by ZCS. They include the spam filter accounts for junk mail (spam and ham), virus quarantine account for email messages with viruses, and GALsync account if you configure GAL for your domain. Do not delete these accounts! These accounts do not count against your license.
- **Administrator accounts**. Administrator accounts count against your license.
- **User accounts**. User accounts count against your license account limit. When you delete an account, the license account limit reflects the change.
- **Alias accounts**. Aliases do not count against your license.
- **Distribution lists**. Distribution lists do not count against your license.
- **Resource accounts**. Resource accounts (location and resources) do not count against your ZCS license.

## 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 Backup and Restore on page 219

## Setting Up S/MIME

S/MIME is a standard to send secure email messages. S/MIME messages use digital signature to authenticate and encrypt messages.

### Prerequisites

- To use S/MIME, users must have a PKI certificate and a private key. The private key must be installed in the user's local certificate store on Windows and Apple Mac and in the browser certificate store if they use the Firefox browser. See the appropriate computer or browser documentation for how to install certificates.
- Users can use any of the following browsers:
  - Mozilla Firefox 4 or later
  - Internet Explorer 8, 9
  - Chrome 12 or later
- Users computers must have Java 1.6 SE deployed to use S/MIME. If they do not, they see an error asking them to install it.

### S/MIME License

You must have a ZCS license that is enabled for S/MIME.

### Enable S/MIME Feature

The S/MIME feature can be enabled from either the COS or Account Features Tab.

1. Select the COS or account to edit.
2. In the Features tab S/MME features section, check **Enable S/MIME**.
3. Click **Save**.

Users can send encrypted messages to recipients if they have the recipients' public-key certificate stored in the recipient's contact page in their Address Book, stored in the local OS or browser keystore, or stored in an external LDAP directory. See Configure External LDAP Lookup Certificates.

### Configure External LDAP Lookup for Certificates

If you use an external LDAP to store certificates, you can configure the Zimbra server to lookup and retrieve certificates from the external LDAP, on behalf of the client. You can configure the external LDAP server settings from either the **Global Settings>S/MIME** tab or the **Domains>S/MIME** tab.

***Note:*** *Global Settings override Domain settings*

1. From the administration console, edit the global settings page or select a domain to edit. Open the **S/MIME** tab.
2. In the **Configuration Name** field, enter a name to identify the external LDAP server. Example, **companyLDAP_1**
3. In the **LDAP URL** field, enter the LDAP server's URL.
   Example, **ldap://host.domain:3268**
4. To use DN to bind to the external server, in the **S/MIME LDAP Bind DN** field, enter the bind DN. Example, **administrator@domain**

   If you want to use anonymous bind, leave the Bind ND and Bind password fields empty.
5. In the **S/MIME Ldap Search Base** field, enter the specific branch of the LDAP server that should be searched to find the certificates.

   Example**, ou=Common Users, DC=host, DC=domain**

   Or, check **Automatically discover search base** to automatically discover the search base DNs. For this to work, the S/MIME Search Base field must be empty.
6. In the **S/MIME Ldap filter** field, enter the filter template for the search. The filter template can contain the following conversion variables for expansion:
   - %n - search key with @ (or without, if no @ was specified)
   - %u - with @ removed (For example, mail=%n)
7. In the **S/MIME Ldap Attribute** field, enter attributes in the external LDAP server that contain users' S/MIME certificates. Multiple attributes can be separated by a comma (,).

   Example, "userSMIMECertificate, UserCertificate"
8. Click **Save**.

To set up another external LDAP server, click **Add Configuration**.

## 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. The following can be configured 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.
- The maximum number of accounts that can be created on the domain
- Free/Busy Interop settings for use with Microsoft Exchange.
- Domain SSL certificates

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 124.

***Note:*** *Domain settings override Global settings.*

### 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 119.
- 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' 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.
- **Shutdown**. When the domain status is changed to Shutdown, the server is doing major and lengthy maintenance work on the domain. For example, renaming the domain or moving LDAP entries. Modification and deletion of the domain can only be done internally by the server when it is safe to release the domain, they cannot be done in the admin console or using zmprov.

### 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 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 Zimbra LDAP Service on page 33.

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.

### Creating GAL sync accounts

To give users faster access to GAL, when you configure an internal or external GAL, you can set up an account in ZCS that is configured to sync to the GAL data. You define the GAL datasource and the contact data is syncd to address book. The gal sync account is a system account and does not use a Zimbra license.

If the mode **Both** is selected, an address book is created for each LDAP data source.

When a datasource is configured in this 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 address book for that GAL. During the sync, the address book is updated with new contact, modified contact and deleted contact information. You should not modify the address book directly. When the LDAP syncs the GAL to the address book, changes you made directly 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,

**Changing GAL sync account name.** The default name for the GAL sync account is **galsync**. When you configure the GAL mode, you can specify another name. After the GAL sync account is created, you cannot rename the account as the data sync will not work.

To change the account name you delete the existing GAL sync account and configure a new GAL for the domain.

1. Select the domain where you want to change the GAL sync account name.
2. Select **Configure GAL** to open the configuration wizard and change the GAL mode to internal. Do not configure any other fields. Click **Finish**.
3. In the domain's account Content pane, delete the domain's galsync account.

4. Select the domain again and select Configure GAL to reconfigure the GAL. In the GAL sync account name field, enter the name for the account. Complete the GAL configuration and click **Finish**. The new account is displayed in the Accounts Content pane.

### 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 Server 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.

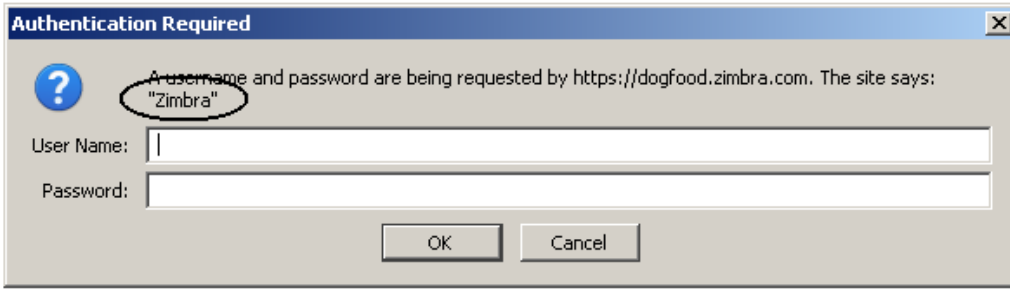
### Domain Advanced Tab

The features configured in the Advanced tab include:

- Replacing "Zimbra" in the Briefcase authentication dialog box.
- Configuring the email validation setting's regular expression for invalid email addresses.

#### Briefcase

When a Briefcase folder is shared with an external guest, they must log in to view the shared item.




The Authentication Required dialog that displays references the company name "Zimbra" in the prompt. You can change the company name from Zimbra to your company name in the **Domain>Advanced** tab. This also can be configured as a global setting.

### Setting Account Email Validation Rules

The ZCS server validates an email address or domain name using javax.mail.internet.InternetAddress when accounts, groups, or domains are created or renamed.

You can define additional email validation rules to validate email addresses for messages sent from the advanced Zimbra Web Client. This validation is done from the Zimbra Web Client.

1. Go to the administration console **Domains Advanced** tab.
2. In the **Regular expression for invalid email address** field enter a regular expression (regex) to filter out email addresses that should be considered invalid. You can add multiple regular expressions.

Example of regular expressions:

- **test@\\d+.com**. This regular expression identifies email addresses with a number in the domain name as invalid. That is test@123.com or test@1.com are not valid addresses.
- **mail@donotreply.com** (any specific address). This type of regular expression identifies a specific email address that is invalid.

***Note:*** *This validation does not work when messages are sent from the standard Zimbra Web Client.*

### 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 110.

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.

### Zimlets on the Domain

Zimbra Collaboration Server includes pre configured Zimlets, see Managing Zimlets on page 187. 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, 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.

## Adding a Domain Alias

A domain alias allows different domain names to direct to a single domain address. For example, your domain is domain.com, but you want users to have an address of example.com, you can create example.com as the alias for the domain.com address. Sending mail to user@example.com is the same as sending mail to user@domain.com.

***Note:*** *A domain alias is a domain name just like your primary domain name. You must own the domain name and verify your ownership before you can add it as an alias.*

You can create a domain alias from the administration console Domain tool bar>**Add a Domain Alias** link. The domain alias is listed in the administration console Navigation pane under Domains.

## Installing a SSL Certificate for a Domain

An SSL certificate can be installed for each domain on a ZCS server. Zimbra Proxy must be installed on ZCS and correctly configured to support multiple domains. For each domain, a virtual host name and Virtual IP address are configured with the virtual domain name and IP address.

Each domain must be issued a signed commercial certificate that attests that the public key contained in the certificate belongs to that domain.

To install the SSL Certificate for a Domain:

1. Configure the Zimbra Proxy Virtual Host Name and IP Address. Type **zmprov md <domain> +zimbraVirtualHostName {domain.example.com} +zimbraVirtualIPAddress {1.2.3.4}**

   ***Note:*** *The virtual domain name requires a valid DNS configuration with an A record.*

2. Go to the administration console and edit the domain. Copy the domain's issued signed commercial certificate's and private key files to the **Domain>Certificate** tab.

   Copy the root certificate and the intermediate certificates in descending order, starting with your domain certificate. This allows the full certificate chain to be validated.

   Make sure you remove any password authentication from the private key before the certificate is saved. See your commercial certificate provider for details about how to remove the password.

   Click **Save**.

The domain certificate is deployed to **/opt/zimbra/conf/domaincerts**.

## 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 ZCSInstallation 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:
  - zimbraImapCleartextLoginEnabled=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 Server 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 113. 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 and their status - 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 Managing Zimlets chapter for information about Zimlets.

### Admin Extensions

You can create custom modules to add to the Zimbra administration console user interface. The admin extension framework allows developers to add new views to the administration console, manage new data objects in the administration console, extend existing objects with new properties, and customize existing views.

You upload and install your modules from the administration console

Go to the Zimbra Wiki, Extending Admin UI for documentation about how to create an extended admin UI module.

### Adding Words to ZCS Spell Dictionary

If ZWC users frequently uses words, abbreviations or acronyms that are marked as spelled incorrectly with the ZWC spell check, you can update the COS or domain attribute **zimbraPrefSpellIgnoreWord** with the words that should be ignored when spell check is run.

For example, to configure words to ignore for a domain, run

### Setting System-wide Signatures

```
zmprov md domainexample.com +zimbraPrefSpellIgnoreWord ZXY
+zimbraPrefSpellIgnoreWord DDE
```

You can create system-wide mandatory signatures. The signatures are added to every message sent out. These types of signatures can be used to set up company signatures, legal notices, and company disclaimers. The following attributes are used to enable this feature:

- **zimbraDomainMandatoryMailSignatureEnabled (TRUE/FALSE)** TRUE enables this feature.
- **zimbraDomainMandatoryMailSignatureText.** This creates the plain text version.
- **zimbraDomainMandatoryMailSignatureHTML.** This creates the HTML version.

1. To create a system wide mandatory signature, enter the following

```
zmprov mcf zimbraDomainMandatoryMailSignatureEnabled TRUE

zmprov mcf zimbraDomainMandatoryMailSignatureText <“some text”>

zmprov mcf zimbraDomainMandatoryMailSignatureHTML
"<html><body>some html text</body></html>”
```

2. Restart Amavis to apply the configuration and global signature files. Type:

```
/opt/zimbra/bin/zmamavisdctl restart
```

The global signature is not visible when an email is composed, but displays in the recipient's email message.

# 11 Managing User Accounts

You create accounts and configure features and access privileges from either the administration console or using CLI commands.

Topics in this chapter include:

- Setting up Accounts
- Managing Class of Services
- Managing Distribution Lists
- Managing Resources

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 **Account Migration 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 **zmmboxmove** 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 for information about how to use these commands.

## Setting up Accounts

You can configure one account at a time with the New Account Wizard or you can use the Account Migration feature to create many accounts at once. This section also contains information about how to manage aliases.

### 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 Customizing Accounts, Setting General Preferences and Password Rules on page 155.

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 as many accounts as you have licenses. In the administrator's console, the Account Migration Wizard guides you through provisioning multiple accounts and importing account data from the external directory for those accounts.

The Migration Wizard is used to provision accounts and import user's email messages from the following types of servers:

- Generic IMAP Server
- MS Exchange Server
- MS Exchange IMAP Server
- Zimbra Collaboration Server

The **Account Migration>Provisioning tasks** tab content pane lists the migrations that have been performed.

The Migration Wizard is used for the following:

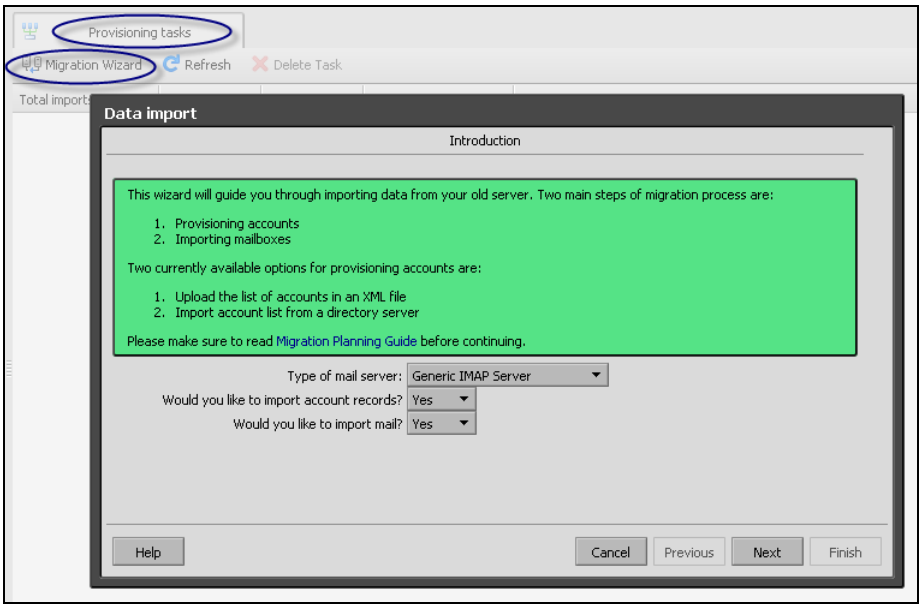
- Provision multiple accounts at once. Two ways to provision accounts include:
  - Import account information directly from a server to ZCS
  - Create an .xml file to provision accounts and migrate account data
- Import data
  - Define data to import and then import the data from external directory servers
  - Create an .xml file that defines the data type to import

#### Provisioning Multiple Accounts and Migrating Account Data

The steps in this section show you how to provision multiple accounts and migrate account data.

1. Select **Tools>Account Migration**.

2. On the Provisioning tasks tab, select **Migration Wizard**. The Data import dialog displays.




3. Select the **Type of mail server** that accounts and data are migrating from.
   - Generic IMAP Server
   - MS Exchange Server
   - MS Exchange IMAP Server
   - Zimbra Collaboration Server
4. If you are migrating accounts, set **Would you like to import account records** to **Yes.**

   If the account's data is being imported now, set **Would you like to import mail** to **Yes**.

   If you already migrated the accounts, but did not import the account data and now want to do so, set **Would you like to import account records** to **No** and set **Would you like to import mail** to **Yes**. See Importing Account Data on page 137.
5. Depending on the type of mail server you selected in Step 3, you can either create an XML file with the migrating account data or specify how account information is imported:
   - If you selected **MS Exchange Server** as the type of server accounts are migrating from, you create an .xml file with the migrating accounts data. You select the data migration options and Active Directory logon information. This information is used to create an .xml file from the data on the Active Directory. After the. xml file is created, use the Zimbra

Migration Wizard one-step process to migrate the accounts and data. See Creating an XML File for Account Provisioning and Migration on page 139.

- If you selected a server **other than MS Exchange Server** you can specify how account information will be imported:
  - from an Active Directory on MS Exchange Server
  - from another type of LDAP server directory
  - from a Zimbra LDAP server directory or from an XML file you already created. See Migrating Accounts Directly on page 137.

After the accounts are provisioned, you import the account data. You can select specific accounts or select an XML file with a list of accounts. See the next section, Importing Account Data on page 137.

### Importing Account Data

On the **Import options** dialog, you can specify the list of accounts whose mail you want to import by either selecting the accounts to import data, or by using an XML file to import data.

#### Selecting specific accounts to import data

1. Select **Select accounts to import** to go to a list of accounts that have been provisioned. Select the accounts that should have their data imported.
2. Enter the information necessary to connect to the exporting server's IMAP, this includes the IMAP host name, port and administrator login information.
3. Review the data import options and click **Next**. The data import task starts.

#### Using an XML file to import data

1. Select **Upload list of accounts in XML format** to upload the .xml file you created. See the Zimbra Migration Wizard for Microsoft Exchange guide for more information about creating an .xml file.

***Note:*** *The accounts listed in the XML file must be provisioned before data can be uploaded.*

### Migrating Accounts Directly

These step provisions accounts on the Zimbra server.

1. On the **Overview** dialog, select whether to migrate account information from Active Directory (AD); from another LDAP server, or from an XML file.
2. On the **Directory connection** dialog,
   a. Enter the details for connecting to your Active Directory or another LDAP server.

b. Enter the maximum accounts to import at one time. The default is 0, which means that no limits are set.

c. Enable **Automatically create missing domains**, so that when an account is imported and the domain they were on is not created already created on ZCS, the domain is automatically created.

   If you do not enable this, accounts from domains that do not exist on ZCS are not created. Disabling this option, makes it easy to import accounts from specific domains that have been pre created on ZCS.

d. Enter the following information about the AD or LDAP server:

   - Server Name. The LDAP URL is entered as ldap://ldapdirectory.example.com
   - By default the port is 3268 for Active Directory and port 389 for LDAP, but you can change this
   - Use Security. Check SSL if this is used
   - Bind DN and bind password
   - LDAP filter. In this field enter the LDAP search filter to run. Here you can define search criteria to collect the type of account information you want to import. The filter in the field (objectClass=organizationalPerson), is set to gather account information, including email address, individual first, middle, last names, postal and phone information if it is available. You can change the filter.
   - LDAP search base is used to configure what subsection of the LDAP forest to search.

After you complete this dialog, click **Next**.

3. Set the password configuration option for the accounts to be provisioned.

   Set either

   - **Generate a random password for each account**. If the wizard generates random passwords for each account, you must download the .csv file that is created as this file lists the passwords that were created. You need to give the password information to each user.

   or

   - **Use the same password for all new accounts**.

   - Check **Require users to change the password after first login**.

4. Set the **Length of generated password.** The default is 8 characters. The password can be from 6 to 64 characters.

5. For split domain configurations, set the SMTP Host name and port.

6. Click **Next**.

The Migration Wizard connects to the directory server and generates a report showing the number of domains found; number of accounts found on the server and how many of those accounts are already created on ZCS. This dialog also shows the password options you configured.

7. Click **Next**. The accounts are provisioned on the ZCS server.

   A Provision Accounts dialog displays the number of accounts imported and number of accounts that failed to be imported. A .csv file is created with the list of all provisioned accounts. This list includes the password information for each account.

8. Download the .csv file that lists the provisioned accounts and their passwords. The .csv file is deleted when you close the wizard.

When this is complete, the wizard generates a .csv file with a list of new accounts. Download this file for future reference. Choose a secure location to store the file as it may contain password information for the user accounts you provision. *If you do not download the file, you cannot access the report later.*

### Creating an XML File for Account Provisioning and Migration

Zimbra's migration tools can be used to import users' email messages, calendars, contacts, and task lists from an existing Microsoft Exchange server to the Zimbra server. When the user's files are migrated, the folder hierarchy is maintained.

Migrating accounts to Zimbra is a two step process.

- **Step 1** is to run the migration tool to create a .xml file with the migrating accounts data.
- **Step 2** is to run the Zimbra Migration Wizard for Exchange one-step migration option which uses the .xml file data to create accounts and import account content. See the Zimbra Migration Wizard for Microsoft Exchange guide on the Zimbra website for detailed information about the one-step migration process.

Before you begin, identify the MAPI profile to use to log into the Exchange server. You enter this MAPI profile information in Step 2.

#### Creating the XML File

1. In the Migration from MS Exchange dialog that opens, configure the account provisioning options

   Set either

   - **Generate a random password for each account**. If the wizard generates random passwords for each account, you must download the .csv file that is created, as this file lists the passwords that were created. You give this password information to each user.

   or

- **Use the same password for all new accounts**. Enter the password to use and confirm the password.

- Check **Require users to change the password after first login**.
- **Length of generated password**. The default is 8 characters. The password can be from 6 to 64 characters.
- Check **Create user accounts in ZCS**. This creates the account element in the .xml file used to create the account. Uncheck this box if the accounts were already created on ZCS.
- Select the items to import the accounts: **email messages, contacts, tasks,** and **calendar**.
- Select whether to import items from the account's Trash folder (deleted items) or Junk folder.
- If some accounts were migrated before, select **Ignore previously imported emails** so accounts do not have duplicate email messages.
- **Ignore invalid SSL certificate** is checked. If this is not checked and you do not have a commercial certificate installed before you migrate accounts, the Zimbra Migration Wizard for Exchange fails to migrate the accounts because the server certificate is not valid.

2. On the **Mail server information** dialog configure the ZCS server and Microsoft Exchange server connection information.
   - In the **Target domain** field enter the domain name where accounts are migrated to. This domain should be created on ZCS.
   - The administrator account is automatically configured. Enter the password for this account.
   - Enter the MAPI profile that is used to connect to the Microsoft Exchange server.
   - MAPI profile name. This is the MAPI profile you create for use with the Zimbra Migration Wizard to conduct the migration.
   - MAPI server name is the name of the name of the Microsoft Exchange server from which data is collected.
   - Enter the MAPI logon user DN.

   Click **Next**.
3. On the **Active Directory information** dialog, enter the following information:
   - Enter the maximum accounts to import at one time. The default is 0, which means that no limits are set.
   - **Server Name**. The LDAP URL is entered as ldap:// ldapdirectory.example.com.
   - By default the port is 3268, but you can change this.
   - Check SSL if this is used.

- **Bind DN** and bind password.
- **LDAP filter**. In this field enter the LDAP search filter to run. Here you can define search criteria to collect the type of account information you want to import. The filter in the field (objectClass=organizationalPerson), is set to gather account information, including email address, individual first, middle, last names, postal and phone information if it is available. You can change the filter.
- **LDAP search base** is used to configure what subsection of the LDAP forest to search.

After you complete this dialog, click **Next**. The migration wizard connects to the Exchange server.

4. The next page shows the migration options you have configured. If the information is correct, click **Next**. If you need to fix any of the options, click Previous.

   When you click Next, the .xml file is created.

5. Click **Download XML file for MS Exchange migration utility** and save the file to a folder on the computer. IMPORTANT: The .xml file is not available after you close the migration tool. If you do not download the .xml file, you will need to rerun the migration tool again to create a new .xml file.

6. Click **Download MS Exchange migration utility** to download the Zimbra Migration Wizard for Exchange executable file.

You can run the Zimbra Migration Wizard for Exchange executable file at any time. The Zimbra Migration Wizard one-step migration makes it easy to create accounts and import the content you selected for those accounts.

***Note:*** *See the Zimbra Migration Wizard for Microsoft Exchange guide for information about the migration wizard's one-step migration process.*

### Examples of XML Files

Below are three examples of the XML file structure to provision accounts and import data.

**Example of provisioning accounts**. The following example shows an XML file that is used to provision multiple email accounts without importing mail:

```
<?xml version="1.0" encoding="UTF-8"?>
<ZCSImport>
<ImportUsers>
<User>
<sn>Sample</sn>
<givenName>Sam</givenName>
<displayName>Sam Sample</displayName>
<RemoteEmailAddress>ssample@example.com</RemoteEmailAddress>
<password>test123</password>
<zimbraPasswordMustChange>TRUE</zimbraPasswordMustChange>
</User>
<User>
<sn>Zackry</sn>
<givenName>Zak</givenName>
<displayName>Zak Zackry</displayName>
<RemoteEmailAddress>zzackry@example.com</RemoteEmailAddress>
<password>test123</password>
<zimbraPasswordMustChange>TRUE</zimbraPasswordMustChange>
</User>
</ImportUsers>
</ZCSImport>
```

**Example of provisioning accounts from externally hosted domains**. The following example shows an XML file that is used to provision multiple email accounts for externally hosted domain without importing mail. In this example, the zimbraMailTransport attribute of newly provisioned accounts will be set to point to external SMTP server instead of the ZCS server.

```
<?xml version="1.0" encoding="UTF-8"?>
<ZCSImport>
<SMTPHost>smtp.example.com</SMTPHost>
<SMTPPort>25</SMTPPort>
<ImportUsers>
<User>
<sn>Sample</sn>
<givenName>Sam</givenName>
<displayName>Sam Sample</displayName>
<RemoteEmailAddress>sam@example.com</RemoteEmailAddress>
</User>
<User>
<sn>Zackry</sn>
<givenName>Zak</givenName>
<displayName>Zak Zackry</displayName>
<RemoteEmailAddress>zzackry@example.com</RemoteEmailAddress>
</User>
</ImportUsers>
</ZCSImport>
```

**Example of importing email**. The following example shows an XML file that is used to import email for one account via IMAP from a gmail account without provisioning the email account in ZCS. The account must be provisioned on ZCS before running this type of XML file.

```
<?xml version="1.0" encoding="UTF-8"?>
<ZCSImport>
<IMAPHost>imap.gmail.com</IMAPHost>
<IMAPPort>993</IMAPPort>
<ConnectionType>ssl</ConnectionType>
<UseAdminLogin>0</UseAdminLogin>
<ImportUsers>
<User>
<sn>Sample</sn>
<givenName>Sam</givenName>
<displayName>Sam Sample</displayName>
<RemoteEmailAddress>sam@example.com</
RemoteEmailAddress><RemoteIMAPLogin>sam@example.com</
RemoteIMAPLogin><remoteIMAPPassword>test123</remoteIMAPPassword></User>
</ImportUsers>
</ZCSImport>
```

### Managing 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.

## Managing Class of Services

Class of Service (COS) determines what default attributes an account has and which features are enabled or denied. The following can be configured in a COS:

- ZCS features for accounts assigned the COS
- Default settings for user preferences
- Themes that users can use in the Zimbra Web Client
- Zimlets that users can use in the Zimbra Web Client
- Servers that are added to the server pool to distribute accounts across
- Advanced functions including setting rules for attachment blocking, account quotas, data source polling intervals, for proxy-allowed domains, and policies for passwords, login, timeout, email retention, and free/busy interop
- Zimbra Mobile sync rules

For more information about features, preferences, advanced functions, see Customizing Accounts, Setting General Preferences and Password Rules.

A default COS is automatically created during the installation of Zimbra Collaboration Server. 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 be assigned this COS. You can create numerous COSs and specify which COS(s) are availably for a domain. If the domain does not have a COS defined, the original 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.*

### COS Calendar Preference to Set 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 a Change Password Page When Using External Authentication

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
```

## Setting Polling Intervals

Polling intervals determine how often accounts poll the server for new data. Polling intervals can be set in the COS/account tab for POP, IMAP, Calendar updates, RSS feeds, and CalDAV invites.

If the polling interval is not set, data is not automatically polled.

## View an Account 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 Account 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.

An account's status can be one of the following:

- **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.

***Note:*** *Maintenance status is automatically set on an account when a backup is being run, or when importing/exporting or restoring an account.*

- **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 status can be set, if you suspect that a mail account has been hacked or is being used in an unauthorized manner.
- **Closed**. When a mailbox status is closed, the login is disabled, and messages are bounced. This status is used to soft-delete an account before deleting the account from the server. A closed account does not change the account license.
- **LockOut**. This is set automatically when users who try to log in do not enter their correct password and are then locked out of their account. You cannot set this status manually. You set up a login policy with a specified number of consecutive failed login attempts that are allowed before they are locked out. How long the account is locked out is set by COS or Account configuration, but you can change the lockout status at any time.

## Deleting an Account

You can delete accounts from the administration console. This removes the account from the server, deletes the message store, and changes the number of accounts used against your license. Before you delete an account, you can run a full backup of that account to save the account information. See the Backup and Restore chapter.

## Moving a Mailbox to a New Server

Mailboxes can be moved between Zimbra servers that share the same LDAP server.

You can move a mailbox from either the administration console or use the CLI command **zmmboxmove** to move a mailbox from one server.

The destination server manages the move process. The move runs in the background and the account remains in active mode until most of the data has been moved. The account is locked briefly to move the last data and then returned to active mode.

The mailbox move process goes through the following steps:

- Mailbox blobs are copied to the new server
- When most of the content has been copied, the account is put into maintenance mode
- Database tables, index directories and any changed blobs are copied
- Account is switched to the new server and is put back into active mode

All the files are copied to the new server and the LDAP is updated. A copy of the mailbox still remains on the older server, but the status of old account is closed. Users cannot log on and mail is not delivered. Check to see that all the mailbox content was moved successfully before purging the old mailbox.

### Set Global Options to Exclude Items from the Mailbox Move

Global configuration options for moving a mailbox can be set in the CLI to exclude search indexes, blobs, and HSM blobs when mailboxes are moved.

Set the following global configuration options to exclude these items.

- **zimbraMailboxMoveSkipSearchIndex**. If you do not include the search index data, the mailbox will have to be reindexed after the move.

  **zmprov mcf zimbraMailboxMoveSkipSearchIndex TRUE**

- **zimbraMailboxMoveSkipBlobs**. Blobs associated with the mailbox, including primary and secondary volumes (HSM) are excluded.

  **zmprov mcf zimbraMailboxMoveSkipBlobs TRUE**

- **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.

**zmprov mcf zimbraMailboxMoveSkipHsmBlobs TRUE**

### Move A Mailbox from the Administration Console

1. In the Account Content pane, select the account to move to a different server.
2. Click **Move Mailbox** on the toolbar. A new page opens with the account name displayed in the Select account field.
3. Select the target server and click **Export**.
4. When the move is complete, select **View Mail** to verify that the accounts content is displayed and can be opened.
5. After you verified that the account was moved successfully, click **Purge**.

---

***Note:*** *If you closed the move page before you purged the account, you must purge the account using CLI* **zmpurgeoldmbox***.*

**zmpurgeoldmbox -a <email@address> -s <oldservername>**

---

### Move Mailboxes Using CLI zmmboxmove

1. To move a mailbox to a new server

   **zmmboxmove -a <email@address> --from <servername> --to <servername>**

2. To verify that the content of the mailbox was moved successfully, go to the administration console, select the account that was moved. Click **View Mail** on the toolbar. When the account opens, verify that the account's content is displayed and can be opened.

3. Purge the mailbox from the old server

   **zmpurgeoldmbox -a <email@address> -s <oldservername>**

### View Progress of Mailbox Moves

After you run the **zmmboxmove** command, you can run **zmmboxmovequery** to see the progress of mailbox moves on the servers, both move-ins and move-outs.

**zmmboxmovequery -a <email@address> -s <severname>**

## 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.

### Manage Access to Distribution Lists

You can manage who can view members of a distribution list and who can send messages to a distribution list. The default is all users have access to all distribution lists.

If you want to limit who can access distribution list, you can grant rights to individuals users on a domain or if you want only member of a domain to access distribution lists, you can grant rights on the domain. When you grant the right on the domain, all distribution lists in the domain inherit the grant.

Or you can grant the right on individual distribution lists and configure specific users that are allowed to access the distribution list.

You can restrict access to a distribution list from the CLI **zmprov grant rights** (**grr**) command.

***Note:*** *For more information about how granting rights works, see Delegated Administration.*

### Manage Who Views Members of a Distribution List

The default is that all users can view members addresses in a distribution list. A distribution list address displays a **+** in the address bubble. Users can click on this to expand the distribution list. A list of the addresses in the distribution list is displayed. Users can select individual addresses from the expanded list

To restrict who can view addresses in distribution lists to individuals or to a domain:

- For individual users, type: **zmprov grr domain <domain_name> usr <user1@example.com> viewDistList**
- For all users in a domain, type:. **zmprov grr domain <domain_name> dom <example.com> viewDistList**

To grant rights on a distribution list and let specific users view the list, type: **zmprov grr dl <dll_name@example.com> usr <user1@example.com>**

### Managing Who Sends to a Distribution List

The default is that all users can send messages to all distribution lists. You can grant rights to a distribution list or to a domain that defines who can send messages to a distribution list. When users attempt to send to a distribution list that they are not authorized to use, a message is sent stating that they are not authorized to send messages to the recipient DL.

To restrict who can send messages to a distribution list to individuals or to a domain:

- Grant rights to an individual user in a domain to send messages to all distribution lists. **zmprov grr domain <domain_name> usr <user1@example.com> sendToDistList**
- Grant rights to all users in a domain to send messages to all distribution lists. **zmprov grr domain <domain_name> dom <example.com> sendToDistList**

To restrict access to individual distribution lists to different users:

- Specific internal users. Type as **zmprov grr dl <dlname@example.com> usr <username@example.com> sendToDistList**
- Only to members of the distribution list **zmprov grr dl <dlname@example.com> grp <dlname2@example.com> sendToDistList**

- All users in a domain **zmprov grr dl <dlname@example.com> dom <example.com> sendToDistList**
- All internal users **zmprov grr dl <dlname@example.com> all sendToDistList**
- All public email addresses **zmprov grr dl <dlname@example.com> pub sendToDistList**
- Specific external email address **zmprov grr dl <dlname@example.com> gst <someone@foo.com> "" sendToDistList**

In addition to granting rights, the **Milter Server** must be enabled from the administration console **Global Settings>MTA** tab.

### Enable View of Distribution List Members for Active Directory Accounts

To view Active Directory distribution list members in messages or in the address book, the GAL group handler for Active Directory must be configured in the ZCS GALsync account for each Active Directory.

To update the GALsync account for each Active Directory, you must know the GALsync account name and all data sources on that GALsync account.

1. To find the GALsync account name type

   **zmprov gd {domain} zimbraGalAccountId**

   The above command displays zimbraId of the GALsync account. To find the name, type

   **zmprov ga {zimbraId-of-the-GAL-sync-account} | grep "# name"**

2. To find the data sources for the GALsync account, type

   **zmprov gds {gal-sync-account-name-for-the-domain}**

3. To enable the group handler for the Active Directory, type

   **zmprov mds {gal-sync-account-name-for-the-domain} {AD-data-source-name} zimbraGalLdapGroupHandlerClass com.zimbra.cs.gal.ADGalGroupHandler**

### 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. In order for partial acceptance of a series to work, both fields must be set to nonzero values.

### 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.

# 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.

Topics in this chapter include:

- Zimbra Web Client Versions
- Zimbra Messaging and Collaboration Applications
- Other Account Configuration Preferences

***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 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 Server provides the following messaging and collaboration solutions:

- Email messaging
- Calendar and scheduling
- Address books
- Tasks
- Briefcase for sharing files and document management
- Advanced search capability

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 in the following table. Note that the third column is the tab name where the feature can be enabled. Many of these features can than be managed from the 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, in the Features tab, remove the check for Preferences.

| Feature Name | Description | COS/ Account Tabs |
|---|---|---|
| Mail | Enables the email application. This is enabled by default. | Features |
| Conversations | Messages can be displayed grouped into conversations or as a message list. Conversations group messages by subject. If this feature is enabled, conversation view is the default. You can change the default on the COS Preferences tab.<br>Users can change the default from the Mail toolbar, View link. | Features |
| HTML compose | Users can compose email messages with an HTML editor. They can specify default font settings for HTML compose in their account Preferences tab. | Features |
| Draft auto save interval | Configure how frequently draft messages are automatically saved. The default is to save messages being composed every 30 seconds. Users cannot change the time, but they can turn off the feature to automatically save drafts while composing. | Preferences |
| Mail send later | When this is enabled, users can select the Send option **Send Later** to send a message at a later time. They configure a date and time to send an email message and it is saved in the Draft folder. | Features |
| Message priority | When this is enabled, users can set the priority of the message - High, Normal, or Low. The recipient in ZWC sees the priority flag if it is high or low. | Features |
| Enable attachment indexing | Attachments to email messages are indexed. If attachments are indexed, they can be searched. | Advanced |

| | | |
|---|---|---|
| Allow the user to specify a forwarding address | Users can create a forwarding address for their mail. When this feature is enabled in the COS, in the account configuration, you can specify a default forwarding address that the user can use and enable the function so that a copy of the forwarded message is not saved in the user's mailbox. Users can change the information from their account Preferences tab.<br>In the account configuration, you can also specify forwarding addresses that are hidden from the user. A copy of each message sent to the account is immediately forwarded to the designated forwarding address. | Features tab in COS<br>Forwarding tab in Accounts |
| Out of office reply | Users can create an email message that automatically replies to incoming messages. This is commonly used as a vacation message. By default the 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.<br>Users can also set the start and stop dates for the message. You can change this setting in the COS or Account setup. | Features<br>Preferences |

| | | |
|---|---|---|
| New mail notification | Allows users the option to specify an address where to be notified of new mail to their ZWC account. They can turn this feature on or off and designate an address from their account Preferences tab.<br>An email with information about the email's subject, sender address and recipient address is sent to the address.<br>**Note**: See zmprov (Provisioning) on page 269 in Appendix A CLI commands, for information about how to change the email template. | Features tab in COS<br>Preferences tab in Accounts |
| Persona | The name and address configured for the account creates the primary account persona. This is the information that user use as the From address.<br>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.<br>The number of personas that can be created is set to 20. You can change this from the CLI **zmprov mc zimbraIdentityMaxNumEntries** | Features |
| Maximum length of mail signature | You can set the maximum number of characters that can be in a signature. The default is 1024 characters.<br>Users can create signatures for different roles. The number of signatures users can create is configured in **zimbraSignatureMaxNumEntries** | 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 |

| | | |
|---|---|---|
| Search for people | A People Search bar is added to the users ZWC page and users can search the GAL for people within their organization. They see detailed information from the GAL, including phone numbers, office location, and a contact's photo. | Features |
| Initial search preference | When this feature is enabled, the default search mailbox can be changed. The Inbox folder is the default. The default folder can be changed in the Preferences tab and users can change this from their Preferences>Mail page.<br>The default mail search folder is the folder that is searched when the Get Mail link in ZWC is clicked. | 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 | Users can define a set of rules and corresponding actions to apply to incoming and outgoing 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.<br>**Enabling the Forward Address Filter**<br>The action to set a Forward to Address in filters is not enabled by default. It is enabled from the CLI. To enable, type<br>**zmprov mc <cos> zimbraFeatureMailForwardingInFiltersEnabled TRUE**<br>***Note:*** *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 spam, users can create a spam white list from the Preferences Mail folder to identify email addresses that should not be marked as spam.* | Features |
| Tagging and Flagging | Users can create tags and flags and assign them to messages, contacts, and files in Briefcase folders. | Feature |
| Enable keyboard shortcuts | Users can use keyboard shortcuts within their mailbox.<br>The shortcut list can be printed from the Preferences Shortcuts folder. | Preferences |

| | | |
|---|---|---|
| Dumpster folder | Users can recover items that they have deleted from their Trash folders. When this is enabled, users can right-click on the Trash folder and select **Recover Deleted Items** to display items deleted up to 30 days before. | Feature |
| GAL access | Users can access the company directory to find names for their email messages. | Features |
| Autocomplete from GAL | When this is enabled, users enter a few letters in their compose header and names listed in the GAL are displayed ranked by usage. Users can turn this feature on or off from their Preferences tab. See How Autocomplete Ranks Names. | Features |
| IMAP access | Users can use third party mail applications, such as Thunderbird or Outlook, to access their mailbox using the IMAP protocol.<br>You can set the polling interval from the COS/Account Advanced tab, Data Source>IMAP polling interval section. The polling interval is not set. | 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.<br>Users can configure how mail from the POP server is downloaded to ZCS from their Preference>Mail page. The options are<br>• **Allow all mail, including old mail, to be downloaded.** Default<br>• **Allow only mail from now to be downloaded**<br>You can set the polling interval from the COS/Account Advanced tab, Data Source>POP3 polling interval section. The polling interval is not set. | Features |

### How Autocomplete Ranks Names

When users use the autocomplete feature, names appear ranked by mailed-to contacts first and than non mailed-to contacts. When users view an autocomplete list, the most frequently recalled contact is listed at the top. If the contact name that appears first should not be listed at the top, the user can click **Forget** and the contact names are re-ranked.

### Email Preferences Users Manage

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.
- 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.
- Adjust the default font size for printed messages. The default is 12 points.
- Users can set up their own Spam 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.**
- 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.

### Using Import/Export Page

In the advanced Web Client, the Preference, Import/Export page 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.

### Setting Up Trusted Addresses Preferences

Users have a Trusted Addresses page in their Mail Preferences folder. When users receive email with external images that are not displayed, in the message they can select to always display images sent from that address or domain. This address or domain name is added to the users Trusted Address folder. They can also add or remove addresses directly in this folder.

### Subscribing to RSS Feeds

Users can create a folder and subscribe to Websites that provide RSS (Really Simple Syndication) and podcast feeds and receive updated information directly to their mailboxes. The maximum number of feeds that can be returned is 50. RSS feeds count against users' account quota.

The default is to automatically update the RSS data every 12 hours. You can change the polling interval from the COS/Account Advanced tab, Data

Source>RSS polling interval section. Users can right-click on an RSS feed folder to manually load new feed.

## 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.

***Important:*** *To allow users to share their address books, calendars, and Briefcase files, 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 page. 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.
- Enable the ability to use the Global Access List when using the contact picker to look up names.
- Enable the options to include the GAL addresses and names in shared address books when using autocomplete to address a message.

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 page.

## 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 Briefcase files, 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. A nested calendar grouping can be imported through migration as well.<br>The CLI command to define the grouping is<br>**zmmailbox -z -m user1 cf -V appointment /<Calendar Name>/ <sub-calendar name**>.<br>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.<br>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 **zmcalchk** 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, zmcalchk on page 289.

### Setting Remote Calendar Automatic Update Interval

Remote calendars are automatically updated every 12 hours by default. You can change the frequency of these updates in the COS/Account Advanced>Data Source section, Calendar polling interval.

### 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.

### Disable Attendee Edits to Appointments

Attendees can edit appointments in their calendars. Unless they are the originator of the appointment, any changes are made only to their appointments. The originator and other attendees are not notified of the changes. If the organizer makes changes to the appointment, these changes overwrite the attendees edits. The option for attendees to edit their appointments can be disabled from the COS attribute, **zimbraPrefCalendarApptAllowAtendeeEdit**. To disable the ability for invitees to edit appointments they received, run the following:

```
zmprov mc <cosname> zimbraPrefCalendarApptAllowAtendeeEdit FALSE
```

### 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.

- **Time zone**. This sets the default time zone that is displayed in the user's Preferences. See COS Calendar Preference to Set Default Time Zones. If the time zone is configured in the COS, the time zone configured in the domain is ignored.
- **Number of minutes before an appointment to show reminder**. This sets the time before the meeting a reminder notice should be sent.
- **Initial calendar view**. This sets the default view. Options are Day, Work Week, 7-Day Week, Month, List, or Schedule.
- **First day of the week**. This set the default first day of a user's work week.
- **Default appointment visibility**. Options are Public or Private. This sets the default visibility options on the new appointment page. The default is Public, appointments details can be viewed by others. In addition to setting the default appointment option, when the default is Private, all incoming calendar invites are marked as private on the user's calendar and details are hidden.
- **Use iCal delegation model for shared calendars for CalDAV interface**. Apple iCal can be configured to access users' calendars using the CalDAV protocol. When this is enabled, shared calendars are displayed in users' iCal account's Delegation tab and they can delegate access to their calendars. For automatic polling, the polling interval can be set up in the COS/Account Advanced tab, Data Source>CalDAV polling interval field.
- **Enable past due reminders**. When this is enabled, when users log into the ZWC and have old meeting reminders they did not dismiss, the reminder notifications for the last two weeks pop up. When this is disabled, ZCS silently dismisses the old reminders.
- **Enable toaster notification for new calendar events.** When this is enabled, a popup displays in ZWC when new calendar events are received.
- **Allow sending cancellation email to organizer**. When this is enabled, when users receive an invitation they cannot attend at the scheduled time, they have the option to click **Propose New Time** and select another time. The meeting organizer receives an email with the proposed time.
- **Automatically add invites with PUBLISH method**. A calendar invitation email should have method=REQUEST in the calendar object but some third-party email clients incorrectly set method=PUBLISH. These emails are not processed as invitations by default. You can relax the rules by enabling this option.

- **Automatically add forwarded invites to calendar**. When this is enabled, invites that have been forward to users are automatically added to the forwarded recipient's calendar.
- **Flash browser title on appointment reminder**. When this is enabled, when appointment reminders pop up, the browser flashes until the user closes the pop-up.
- **Enable audible appointment notification**. When this is enabled, when an appointment reminder pops up, users can be notified by a beep on their computer. Users must have either QuickTime or Windows Media installed.
- **Auto-decline invites from users who are denied from inviting this user**. Users can configure who can send them messages invites in their Calendar preferences. When Auto-decline invites is enabled, an auto-reply message is sent to those users to let them know they do not have permission to invite the user.
- **Automatically add appointments when invited.** When this is enabled, appointments are automatically added to user's default calendar and declined appointments display on the ZWC calendar in a faded view. **Note**: Mobile devices do not see the deleted invite information in a faded view and may not know that the invite was deleted.
- **Notify of changes made via delegated access**. Users that delegated their calendar are notified of changes made to an appointment by a delegated access grantee.
- **Always show the mini-calendar**. The mini-calendar automatically displays in the Calendar view.
- **Use the QuickAdd dialog when creating new appointments**. When this option is enabled, the QuickAdd dialog displays when users double-click or drag on the calendar.
- **Show time zone list in appointment view**. A time zones list displays in their appointment dialog, giving them the opportunity to change time zones while making appointments.

## 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 |

## Briefcase

Briefcase can be used to share and manage documents that users create in Briefcase or documents and images that users upload to their Briefcase. Users can access these files whenever they log into their account from any computer.

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

| Feature Name | Description | COS/ Account Tabs |
|---|---|---|
| Briefcase | 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.<br>The New Document feature is enabled by default. Users can create new documents using the Zimbra tool. You can disable this features in COS or Accounts Feature tabs, Briefcase Features section. | Features |

In addition, you can enable Zimbra Mobile for users to access their accounts from their mobile devices. See Zimbra Mobile on page 179

## Enabling Sharing

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

## Enable SMS Notification

The Preferences>Notification page lets users configure an email address or SMS alert to their mobile device to receive a reminder message for a task or a meeting on their calendar. Notification by email is enabled by default. You can enable the SMS notification from the zmprov CLI.

- To enable SMS notification by COS, type
  **zmprov mc <default> zimbraFeatureCalendarReminderDeviceEmailEnabled TRUE**
- To enable SMS notification by account, type
  **zmprov ma <user1> zimbraFeatureCalendarReminderDeviceEmailEnabled TRUE**

Users select a region and a carrier when setting up their SMS alert. The list of SMS/email gateways is in **ZmSMS.properties**. You can customize this list to add SMS/email gateways that are not listed.

## Disabling Preferences

Preferences is enabled by default. Users can modify the default preferences that are configured for their account. You can disable preferences and the Preferences tab does not display in users' mailboxes. They cannot change the default configuration for 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, files in Briefcase and RSS feed folders. 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. Alternately, you can configure the **zimbraMailAllowReceiveButNotSendWhenOverQuota** attribute to TRUE. When set to TRUE, a mailbox that exceeds its quota is still allowed to receive new mail and calendar invites. See Account Quota and the MTA.

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 Email Policies

You can set up security policies either by COS or for individual accounts.

### Setting Password Policy

If internal authentication is configured for the domain, you can configure ZCS to impose requirements on what type of password a user can create, and to require users to periodically change their 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 |
| The following settings set the rules for what characters are required for a password. Setting these can make users create more complex passwords. Users must use at least the minimum characters set in each of these fields in their password if they are configured. If a settings is 0, the character is not required to create a valid password. | | |
| Minimum upper case characters | Upper case A-Z | Advanced |
| Minimum lower case characters | Lower case a-z | Advanced |
| Minimum numeric characters | Base 10 digits 0 - 9 | Advanced |
| Minimum punctuation symbols | Non-alphanumeric:<br>! $ % & ' ( ) * + , - / ; < = > ? [ ] ^ { } ~ | Advanced |
| You can set specific punctuation symbols to use in the attribute, **zimbraPasswordAllowedPunctuationChars**.<br>**zmprov mc <cosname> zimbraPasswordAllowedPunctuationChars [!$%'()*+,-/;<=>?\[\]^{}~]**<br>When this attribute is configured, only these punctuation symbols can be used in passwords. | | |

| | | |
|---|---|---|
| Password validation using either numbers or punctuation symbols | A password validation rule can be configured that requires users to include a minimum number of either numerical characters or punctuation symbols in their passwords. This is configured from the CLI.<br>**zmprov mc <cosname> zimbraPasswordMinDigitsOrPuncs [X]**<br>When this is set, passwords must include at least the number of digits or the number of punctuation symbols specified in addition to any other configured minimum requirements. | From the CLI |
| 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 autho 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. This includes data in RSS folders. 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.*

## Recovering Deleted Items From the Dumpster

The dumpster feature allows users to recover items deleted from their account. When the dumpster feature is enabled by Class of Service or for individual accounts, a dumpster folder is created for each account and the **Recover Deleted Items** option is added to the Trash folder's right-click menu.

Items put into dumpster no longer count against the account's quota. Note that items in the dumpster use disk storage space outside of the account's quota.

When users click **Recover Deleted Items**, users can search for the items to recover. When users recover an item from the dumpster, the item is copied to the account's folder. The item still remains in the dumpster.

Items are put into the dumpster when

- Users empty the Trash folder
- Users right-click a folder and select **Empty Folder**
- An item is removed from the account based on the email retention policy

Users can recover items that are deleted from their Trash folder up to the number of days configured in the **zimbraMailDumpsterLifetime** attribute. The default is to purge items more than 30 days old.

### Enable Dumpster

In the administration console, enable **Dumpster folder** from either the COS or from the account's Features tab.

### Configure Item Lifetime in Dumpster

- To configure a COS, **zmprov mc {cosname} zimbraMailDumpsterLifetime** <#>
- To configure an account, **zmprov ma {account} zimbraMailDumpsterLifetime** <#>

### Delete Dumpster Items Manually

Dumpster is deleted for each account as follows

- To delete specific items from dumpster, **zmmailbox -z -m {name} dumpsterDeleteItem {item-ids}**
- To empty the dumpster, **zmmailbox -z -m {name} emptyDumpster**

### Letting Users Select 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 Managing Zimbra Mobile 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 Server 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 un deployed from here. See Chapter 14, Managing 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. See Chapter 14, Managing Zimlets.

## 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 the 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 their 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 lets users select all items in the Content pane at once.

**Preferences Import/Export.** The Preferences Import/Export tab lets users export all of their account data, including mail, contacts, calendar, tasks, and Briefcase folders. They can export specific items in their account and save the data to their computer or other location. The account data is saved as a tar-gzipped (tgz) archive file so that it can be easily imported to restore their account. Individual contacts are saved as .csv files, and individual calendar files are saved as .ics files. The data are not removed from their accounts. The exported account data file can be viewed with an archive program such as WinRAR archiver. Any of these files can be imported into their account from the same tab.

If you do not want users to the Import/Export capability, you can disable the feature from the COS or Admin Features tab.

# 13 Managing Zimbra Mobile

Zimbra Mobile is the Zimbra synchronization program enabled on the 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 mailbox server.

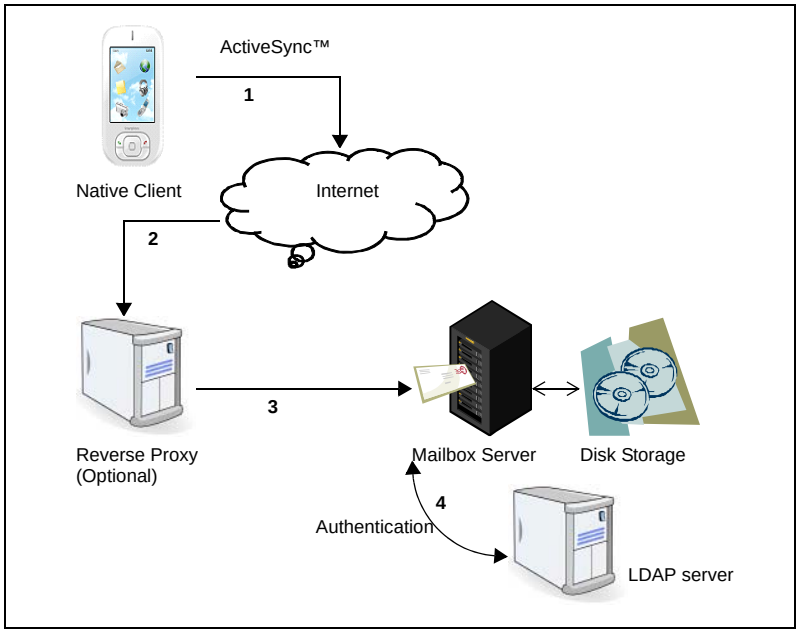
Topics in this chapter include:

- Setting Up Mobile Devices
- Setting up Mobile Device Security Policies
- Changing Mobile Device Password Policy

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 ActiveSync™ 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.

1. 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

Mobile sync is enabled either in the COSprofiles 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 host name 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 certification 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 a numbered PIN can still be used. |
| **Force PIN on device** | Forces the user to create a personal identification number on the mobile device. |
| **Require alpha-numeric password for device** | Requires that the password includes both numeric and alpha characters. |

| **Password Strength Policy Settings** | |
|---|---|
| **Minimum length of device PIN** | Specifies the minimum length of a password. |
| **Number of consecutive incorrect PIN input before device is wiped** | 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 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 mobile 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 account.

### 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 ZWC 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, there is 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.*

# 14 Managing Zimlets

This chapter describes how to deploy, configure, and manage Zimlets™ on the Zimbra server.

Topics in this chapter include:


- Accessing Zimlets
- Deploying Zimlets
- Enabling, Disabling, or Making Zimlets Mandatory
- Undeploying Zimlets
- Configuring Zimlets
- Viewing Zimlet Status
- Upgrading a Zimlet


Zimlets were created 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 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 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 more detailed information about creating Zimlets, see the Zimlet Development section on the Zimbra Wiki.

## Accessing Zimlets

Zimlets are available from the default Zimlets included with ZCS, from the Zimlet Gallery, or by developing your own customized Zimlets, as described in this section.

### Default Zimlets included in ZCS

ZCS includes preconfigured Zimlets when installed. You select which default Zimlets to enable, disable or make mandatory, as described in Enabling, Disabling, or Making Zimlets Mandatory.

The following is a list of default Zimlets included in your ZCS installation.

| Zimlet | Description |
|---|---|
| Attach Contacts | Allows attaching contacts when composing a new message. |
| Email Attacher | Attach email messages when composing a new message. |
| Date | Highlights dates, previews associated appointments and creates a link to the calendar. |
| Drag-n-Drop Attachments | Provides ability to drag-n-drop file attachments when composing an email message. |
| Email Contact Details | Highlights and previews associated contact details for an email address. |
| LinkedIn | Hooks on to email Zimlet; shows LinkedIn search result for a given email. |
| Phone | Highlights a phone number to make a call with your soft-phone, if you soft-phone capabilities. |
| S/MIME | If the S/MIME feature is enabled this zimlet is required. |
| Social | Access social services like Twitter, Facebook, Digg and TweetMeme from Zimbra. |
| Search Highlighter | After a mail search, this Zimlet highlights Search terms with yellow color. |
| URL Links | Highlights Web URLs for linking in email messages. |
| WebEx | Easily schedule, start or join WebEx meetings. |

Some of these Zimlets do not appear in the navigation pane list but come into play by enhancing the user experience when users use certain ZWC features, such as the Email Attacher and URL Links. Other Zimlets, such as LinkedIn and WebEx Zimlets display in the navigation pane.

### Zimlets from the Zimbra Gallery

In addition to the default Zimlets included in your ZCS installation, you can also download and deploy Zimlets from the Zimlet Gallery, which is located on the Zimbra web site.

See Deploying Zimlets for more information on how to deploy Zimlets.

### Developing Customized Zimlets

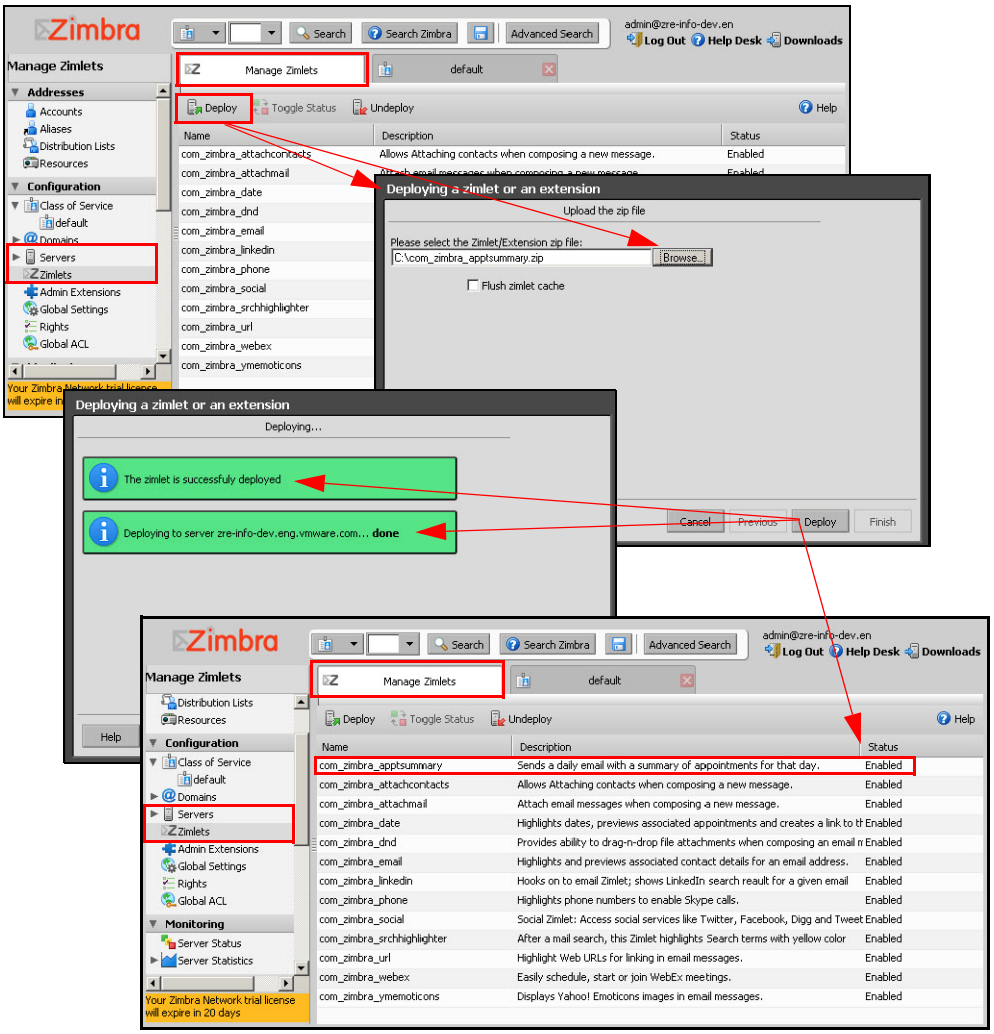
For information about how to develop your own custom Zimlets, see the Zimlet Developers Guide on the Zimbra Wiki. This is an extensive guide which shows you how to set up your development environment, create a basic Zimlet and learn the principles of building, debugging and deploying a Zimlet.

## Deploying 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 deploy Zimlets from the admin console or the CLI, as described in this section.

### Deploying a Zimlet from the Admin Console

1. From the **Configuration>Zimlets** view, click **Deploy**. The **Deploying a zimlet or an extension** view displays.
2. Browse to the Zimlet zip file you want to upload and deploy. Click **Deploy**. In the example below, we are deploying com_zimbra_apptsummary.zip.
3. The Zimlet deploys to the server. A dialog displays indicating the server name where the Zimlet is deployed and the status of the deployment.
4. Verify the Zimlet is enabled by viewing the Zimlets page in the admin console.




## Deploying a Zimlet from the CLI

You can deploy Zimlets from the CLI, including first modifying the COS before deploying to the default COS, or granting access to a COS other than the default COS.

1. Copy the Zimlet zip file to **/tmp** folder on your Zimbra server.
2. Login as zimbra user:

   **su – zimbra**

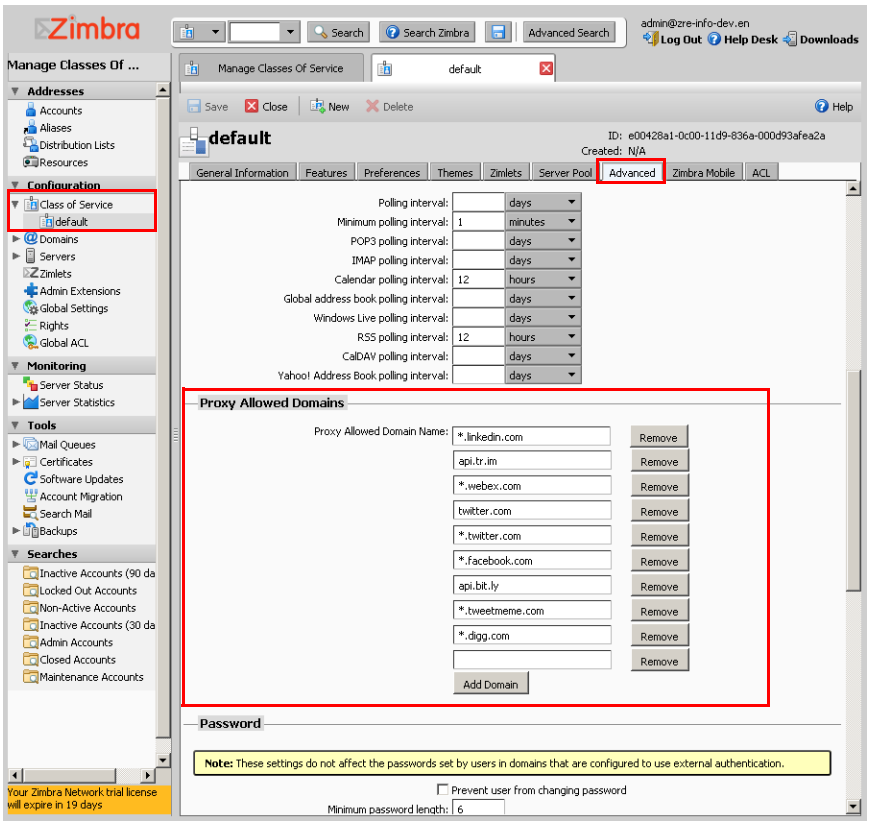
3. Run the following command to deploy your zimlet:

   **zmzimletctl deploy /tmp/<zimlet>.zip**

## Adding Proxy Allowed Domains to a Zimlet

To add proxy allowed domains to a Zimlet:

1. From the **Configuration>default** view, click the **Advanced** tab.
2. Scroll down to the **Proxy Allowed Domains** section.
3. Add or remove domain names.




## Adding Proxy Allowed Domains to a Zimlet using the CLI

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

1. 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.

### Deploying a Zimlet and Granting Access to a COS

To deploy a Zimlet to one or more COSs other than the default:

1. Install the Zimlet, then adjust the ACL on the COSs.
2. Login as zimbra user:

   **su – zimbra**
3. Copy the Zimlet zip file from Gallery to **/tmp** folder. Or, select a zimlet from **/opt/zimbra/zimlets-extra** directory.
4. Run **zmzimletctl deploy <path-to-zimlet.zip>**. For example:

   **zmzimletctl deploy /tmp/<zimlet>.zip**

   This will install the Zimlet just to **default** COS.
5. To deploy the zimlet to additional COS's, run:

   **zmzimletctl acl <zimletname> <cosname1> grant**

   This will grant permission to cosname1. You can also grant access to more than one COS on the same command line. Enter as:

   **zmzimletctl acl <zimletname> <cosname1> grant <cosname2> grant**
6. Finally, add **zimbraproxyalloweddomain** information by running the following for each COS:

   **zmprov mc <COSname1> +zimbraProxyAllowedDomains <*. domain.com>**

   **zmprov mc <COSname2> +zimbraProxyAllowedDomains <*. domain.com>**

## Enabling, Disabling, or Making Zimlets Mandatory

You can enable or disable Zimlets, or make them mandatory. You can also use the toggle feature to enable or disable an installed Zimlet. This feature can be managed using the admin console or the CLI.

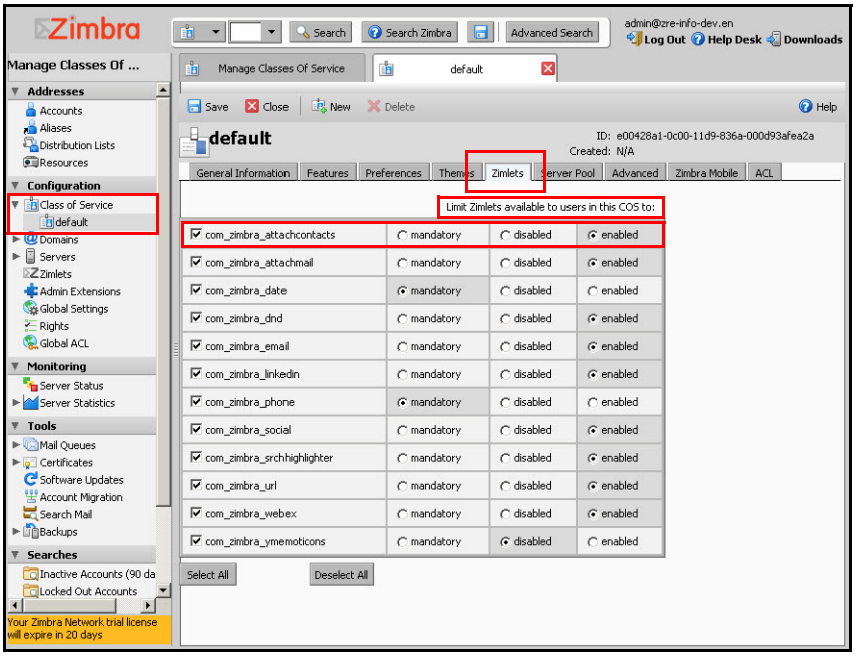
### Default Zimlets

From the **Class of Service>default** view, select which default Zimlets you want to enable, disable, or make mandatory as described below. Default Zimlets do not require any configuration to work.

- **Mandatory**. If you want a Zimlet to be mandatory and always 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.
- **Enabled**. All Zimlets that are deployed are enabled. Users can disable a Zimlet from their account's Preferences>Zimlet page.

***Note:*** *Users can only enable or disable Zimlets which are optional. If you select a Zimlet to be mandatory, it cannot be disabled by the user.*

***Note:*** *Default Zimlets cannot be removed from ZCS.*

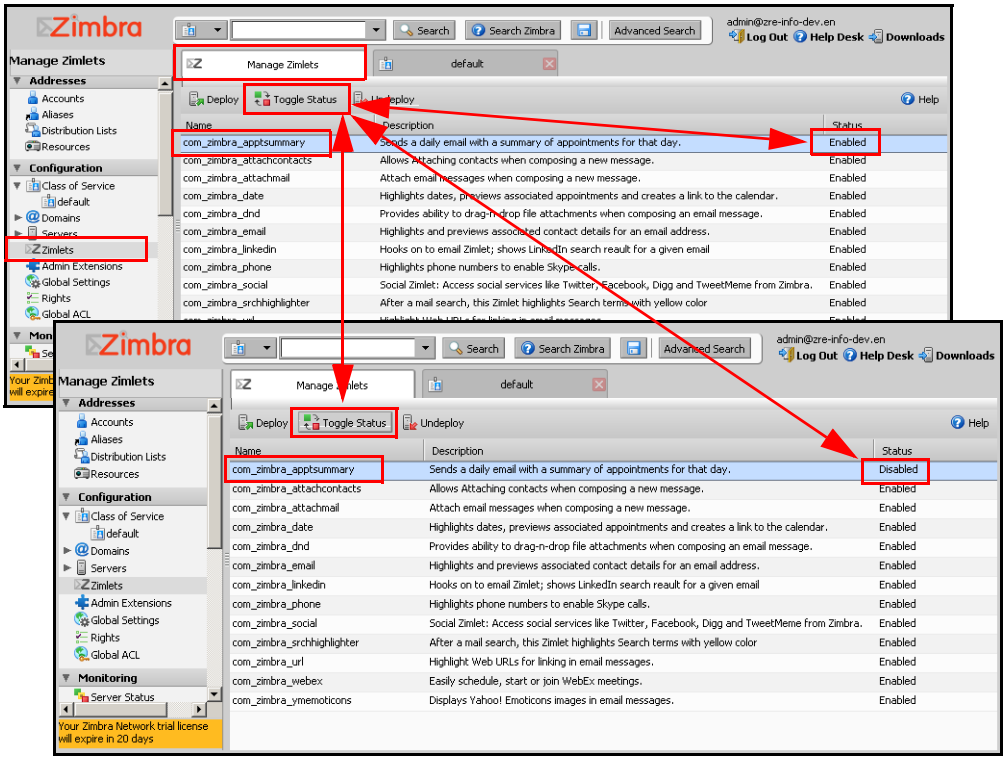



## Toggling a Zimlet between Enabling and Disabling

You can easily switch a Zimlet status from Enabled to Disabled by using the **Toggle Status** button located on the Manage Zimlets toolbar.

To toggle a Zimlet status:

1. On the admin console navigation pane, select **Zimlets**.
2. On the Managing Zimlets view, select the Zimlet you want to change from Enabled to Disabled, or vice versa.
3. Click the **Toggle Status** button. The status is now changed for the Zimlet.




## Disabling a Zimlet using the CLI

You can turn off access to a Zimlet from a COS or disable the Zimlet from the server using the CLI.

### 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>**

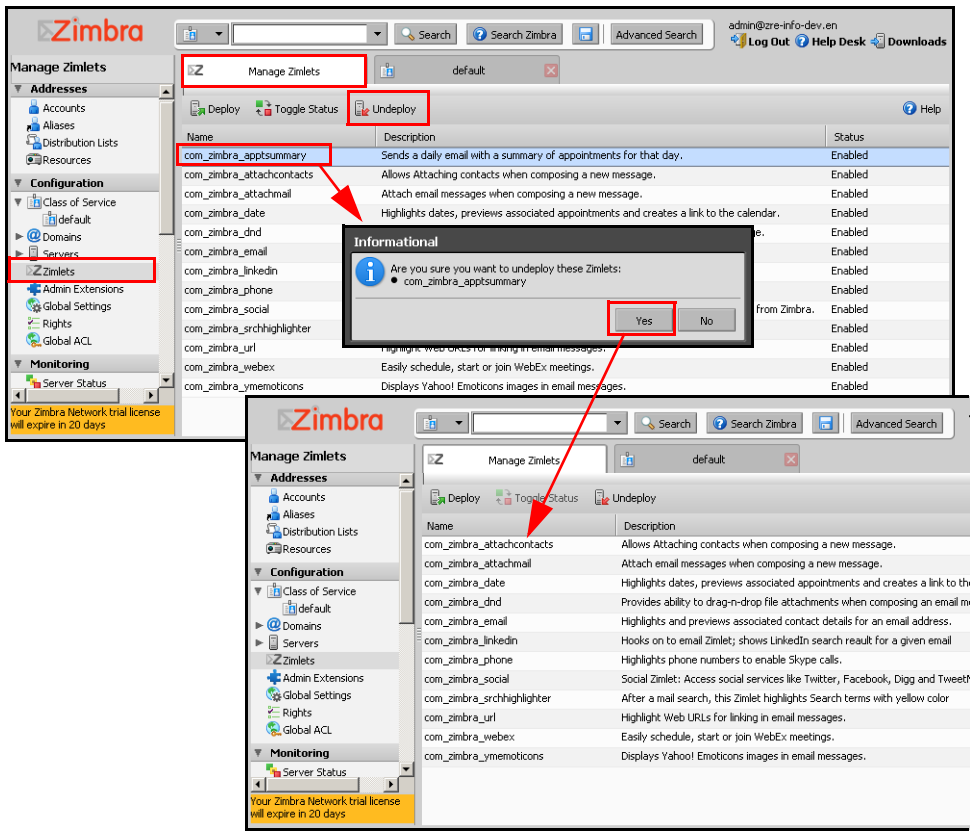
## Undeploying Zimlets

When a Zimlet is undeployed from the server, it is removed from all COSs and then removed from the LDAP. You can undeploy a Zimlet from the admin console or using the CLI utility.

***Important:*** *Only remove your custom Zimlets. You should not remove Zimlets that are included in the Zimbra Collaboration Server. If you do not want to have the Zimbra Zimlets available, disable them.*

### Undeploying a Zimlet from the Admin Console

1. On the admin console navigation pane, select **Zimlets.**
2. On the Managing Zimlets view, select the Zimlet you want to undeploy and click **Undeploy**.
3. Click **Yes** to confirm you want to undeploy the selected Zimlet.
4. The Zimlet is removed. You can confirm by viewing the Zimlet list on the Manage Zimlets view.



### Undeploying a Zimlet using the CLI

1. Type **zmzimletctl undeploy <zimletname>**

   The Zimlet and all associated files are uninstalled.

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

## Configuring Zimlets

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 configuration template allows you to make 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, including the *Zimlet Developers Guide* for details about developing and deploying Zimlets.

### Changing Zimlet Configurations

To change a Zimlet configuration:

1. To extract the configuration template, type

   **zmzimletctl getConfigTemplate <zimlet.zip>**

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

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

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

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

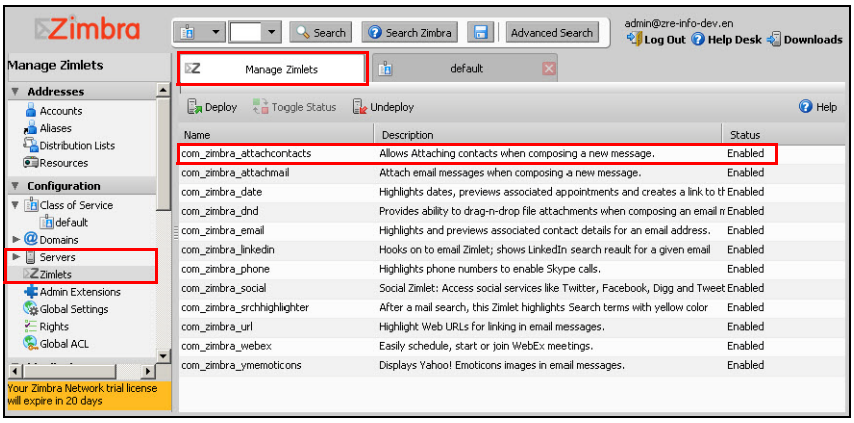
   **zmzimletctl configure config_template.xml**

## Viewing Zimlet Status

You can view a list of Zimlets that are installed on the Zimbra server, and which are enabled or disabled on the LDAP server, from the admin console or from the CLI.

### Viewing Zimlet status using the Admin Console

From the admin console, the Zimlet tab displays all Zimlets that are deployed and shows the status of the Zimlet:




### Viewing Zimlet Status using the CLI

At the CLI command prompt, enter

- **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, or
- **zmzimletctl listZimlets all** to view a list of all Zimlets that are on the server and their status.

## Upgrading a Zimlet

Upgrading a customized Zimlet is performed by using the same steps as deploying a new Zimlet.

### Upgrading a Zimlet

To upgrade a 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 coped to the **/opt/zimbra/jetty/webapps/zimlet/<zimletnamefolder>**.

3. In order for the newer version to be available, flush the cache. From the admin 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.

# 15 Monitoring ZCS Servers

The Zimbra Collaboration Server 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.

Topics in this chapter include:


- Zimbra Logger
- Monitoring Disk Space
- Monitoring Servers
- Monitoring Mail Queues
- Monitoring Mailbox Quotas
- Monitoring Authentication Failures
- Log Files
- Reading a Message Header
- SNMP
- Checking MySQL
- Checking for Latest ZCS Software Version


***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/libexec/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 Max 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

   **<sting>/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.

- Message are received and checked by Amavisd for spam and viruses before being delivered to all recipients in the message. The message count shows the number of recipients who received messages.

- 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 205.

### 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.

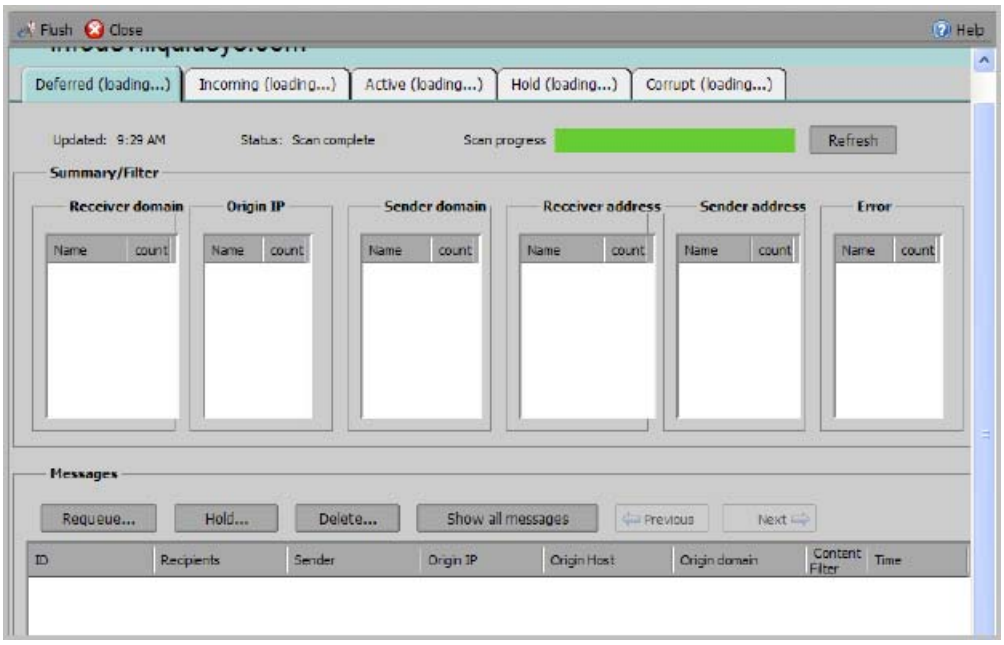
- **threads.csv**: JVM thread counts. Counts the number of threads with a common name prefix.
- **vm.csv**: Linux VM statistics (from the vmstat command).
- **io-x.csv** and **io.csv** store data from the iostat(1) command (io-x.csv with iostat -x).

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 57.

### 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, and briefcase files 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 Server 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.
- **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.
- **myslow.log**. This slow query log consists of all SQL statements from the mailbox server that took more then long_query_time seconds to execute. Note: long_query_time is defined in /opt/zimbra/conf/my.cnf.
- **spamtrain.log**. This log contains output from zmtrainsa 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, zmconfigd, 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/mailbox.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 or TRACE log levels.

To change the logging levels, edit the log4j properties, **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** | 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.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 |

Changes to the log level take affect immediately.

**Table 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. |

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

| Level | Local? | Syslog ? | SNMP Trap? | When Used |
|---|---|---|---|---|
| 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.

### Protocol Trace

Protocol trace is available in the following logging categories with TRACE logging level:

- zimbra.smtp
- zimbra.lmtp
- zimbra.soap
- zimbra.imap
- zimbra.imap-client
- zimbra.pop
- zimbra.pop-client

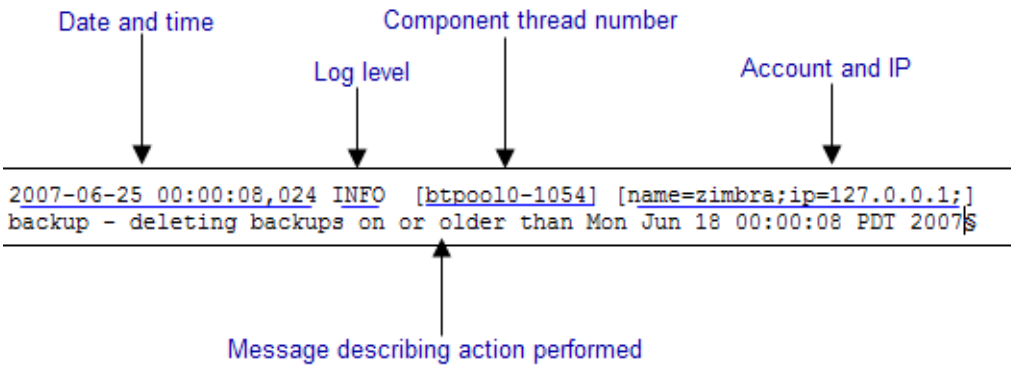
### Reviewing mailbox.log Records

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 filing up mailbox.log with log messages for unrelated accounts. See Appendix A Command-Line Utilities, the zmprov miscellaneous section.*

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




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

### Handler Exceptions and Stack Traces

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

```
007-06-25 00:00:10,379 INFO  [btpool0-1064] [name=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 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

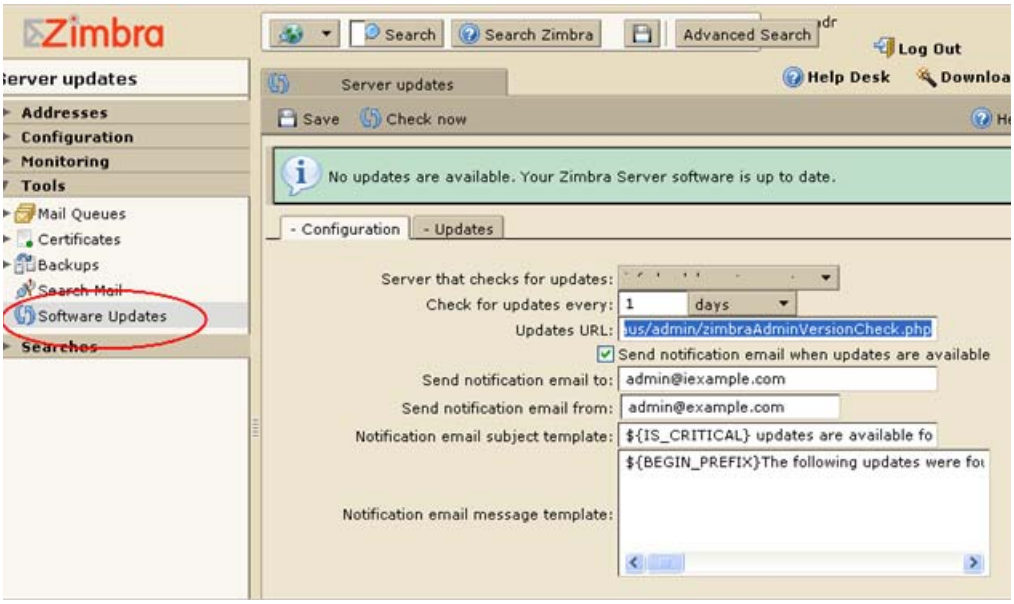
The MySQL database is automatically checked weekly to verify the health of the database. This check takes about an hour. If any errors are found, a report is sent to the administrator's account. The report name that runs the MySQL check is **zmbintegrityreport,** and the crontab is automatically configured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

## Updating ZCO Connector msi on ZCS Downloads Page

When a new version of the Zimbra Connector for Outlook msi becomes available after ZCS is released, you can update the link on the administration console Downloads page with a link to the newer version.

1. Optain the newer version of the ZCO msi file from Zimbra Support Portal.
2. .Add the msi file to a /tmp directory on your ZCS server.
3. From **/opt/zimbra/libexec** run **zmupdatezco**

   **./zmupdatezco </tmp/ZCOfilename.msi>**
4. Restart the server

   **zmcontrol restart**

   The new msi file is available from the administration console Downloads page. The old file is deleted.

# 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.

Topics in this chapter include:

- Zimbra Backup Methods
- Directory Structure for Backup Files
- Backup and Restore Using the Administration Console
- Backup and Restore Using the Command Line Interface
- Backing up using the Standard Method
- Aborting Full Backup In Progress
- Backing up using the Auto-Grouped Method
- Backup Options
- Restoring Data
- Disaster Recovery for Specific Situations
- Using snapshots to backup and restore

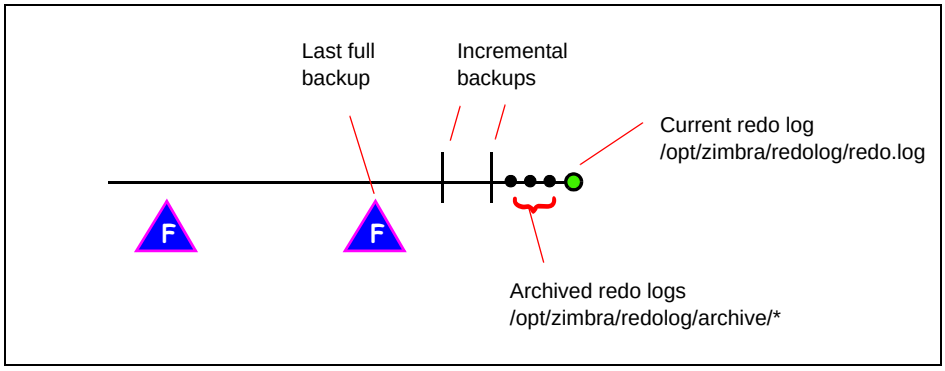
The backup process writes a consistent snapshot of mailboxes to a designated backup directory.

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

The Sample backup timeline figure that follows 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.

**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 are backed up over interval. 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.

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 Standard Backup directory structure. 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.

The redo log directory is located at **/opt/zimbra/redolog/redo.log**. When the redo log file size reaches 100MB, it is renamed and moved into the **/opt/zimbra/redolog/archive** subdirectory.

Redo operations are time critical, therefore a directory move is performed instead of a copy-then-delete function. This directory move can only be performed if the source and destination paths are on the same file system volume. In other words, the redo log and redo-archive log must be on the same file system volume because the archive files are a subdirectory of the redo log file system.

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.

**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 zimbraIds 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. |
| ***<.../zimbraId>/*** | 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 files 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/..../<zimbraID>/ldap.xml*** | |
| | incr-<timestamp> does not include accounts/.../<zimbraId>/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, **Tools>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 225.

### 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

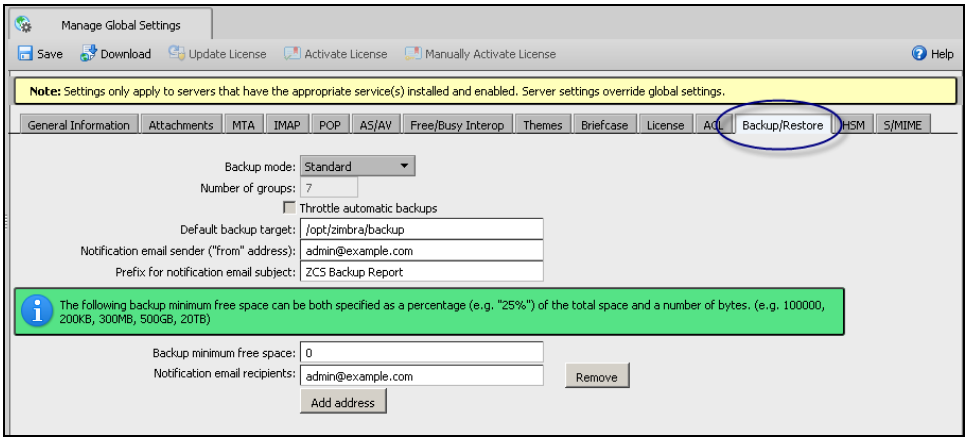
The auto-grouped backup schedule can only be set from the CLI using the **zmschedulebackup** command. See Scheduling Backups on page 230.

### 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 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 230 to run **zmschedulebackup -D** to set the default schedule for auto-grouped backups.

**Throttling option with auto-grouped backup.** The auto-grouped backup method automatically backs up mailboxes that have never been backed up when the next backup is scheduled. This may not be the best option every time a full backup is required on all mailboxes, such as immediately after massive mailbox migrations or after a major upgrade. Enabling **Throttle automatic backups** limits the mailbox count in a daily backup to T/N. This breaks the constraint of backing up all mailboxes in N days, but it helps backup to finish during off hours.

When all mailboxes are backed up at least once, disable throttling.

```
zmprov mcf zimbraBackupAutoGroupedThrottled TRUE
```

## 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.
- **zmbackup**. 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.
- **zmbackupabort**. This command stops a full backup that is in process.
- **zmbackupabort -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.

See Appendix A Command-Line Utilities 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**

```
0 1 * * 6 /opt/zimbra/bin/zmbackup -f - all
0 1* * 0-5 /opt/zimbra/bin/zmbackup -i
0 0 * * * /opt/zimbra/bin/zmbackup -del 1m
```

Read as follows:

- **0 1 * * * 6 /opt/zimbra/bin/zmbackup -f - all** means that the full backup runs on 1 a.m. on Saturdays.
- **0 1* * 0-5 /opt/zimbra/bin/zmbackup -i** means that an incremental backup runs at 1 a.m. from Sunday through Friday.
- **0 0 * * * /opt/zimbra/bin/zmbackup -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/zmbackup -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 section.

### 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.

  **zmbackup -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 **zmbackupquery** 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

  **zmbackupquery -lb full-20070712.155951.123**

- Full backup sets since a specific date

  **zmbackupquery --type full --from "2007/01/01 12:45:45"**

- All full backup sets in the backup directory

  **zmbackupquery --type full**

- Best point in time to restore for an account by specifying a time window

  **zmbackupquery -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, **zmbackupabort** 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 **zmbackup** first starts. If you do not know the full backup label, use **zmbackupquery** to find the label.

Example

- Stop the backup, if you know the label name

  **zmbackupabort -lb full-20070712.155951.123 -s server1**

- Stop the backup, if you do not know the label

  a. **zmbackupquery**

  b. **zmbackupabort -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, zmbackup section.

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 and to backup the MySQL database.

### Backup Up content Options

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 no backed up. Set this if zimbraBackupSkipBlobs is FALSE but you want to skip** blobs on HSM volumes.

### Backing up MySQL Database

You can configure ZCS backups to run mysqldump to backup your MySQL database during backup sessions. When this is enabled, a mysqldump backup runs with each full, incremental and auto-grouped backups.

The MySQL dump files are gzipped and placed in the backup target directory, or to /opt/zimbra/backup, if no directory is specified.

These files can be quite large. Make sure that the free disk space is at least three times greater than the actual mySQL database file for each mySQL database backup file that is saved.

To enable mysqldump to run automatically with your backups, type

**zmlocalconfig -e mysql_backup_retention=<N>.**

**N** is the number of copies of the mySQL database backups that are retained.

***Note:*** *This chapter does not cover how to restore a MySQL database. Contact Zimbra support for assistance.*

***Note:*** *The mysqldump is a backup of your MySQL database at a specific time. Data changes that occur later than the dump file are written to the binary log.To recover to a specific point in time, binary logging must be enabled. See the Zimbra wiki article, MySQL Backup and Restore.*

## Managing Disk Space for Backups

Full or auto-grouped backup sessions fail if the backup target disk does not have enough space. All data backed up in the backup session is discarded and deleted. Configuring the **zimbraBackupMinFreeSpace** attribute helps you manage running backup session by notifying you when your disk may not have enough space to complete the backup. When you know that disk is almost full, you can take appropriate action, either add another disk or delete other files to make room.

To avoid having a backup session start when the free disk space may not be enough for the files in the backed up session, set the value for attribute **zimbraBackupMinFreeSpace** to the amount of free space required on the backup target disk before a backup session is run. If the disk has less space than the value set in the attribute, the backup session will not run and an email notification is sent to the administrator.

***Note:*** *If backing up the mysqldump is enabled, make sure you set the value large enough to include the myslqdump file size.*

The value for this attribute can be specified as a percentage of the total disk space, for example 25%, or as number of bytes, for example 300MB, 50GB, etc. The default value is 0, meaning the check is disabled and backup is always allowed to start.

The attribute can be set globally or by server.

- As global, type **zmprov mcf zimbraBackupMinFreeSpace <value>**
- By server, type **zmprov ms <server hostname> zimbraBackupMinFreeSpace <value>**

Backup sessions run if the free disk space is at least the value you set. If your backup file is larger than the value, the backup session fails. You should monitor the size of the backup files and adjust the attribute value if the backup require more space than the configured value.

## 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 Zimbra Connector for Microsoft 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 **--contineOnError** (**-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 redolog 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.

#### Example**s**

- 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 Network Edition Disaster Recovery on the Zimbra Wiki.

### 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 Server

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 Zimbra Collaboration Server 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 Zimbra Collaboration Server 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 **zmbackup -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 Collaboration Server 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 than 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 **zmplayredo** command to replay changes from 8:00:00.

**zmplayredo --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.

# 17 Zimbra Archiving and Discovery

Zimbra Archiving and Discovery is an optional feature for the Zimbra Collaboration Server (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

Topics in this chapter include:


- How Archiving Works
- How Discovery Works
- Installing Archiving Package as an Update to ZCS
- Creating Dedicated Archive COS in a Multi-Server Environment
- Archiving Attribute
- Creating Archive Mailboxes
- Searching 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. Each account enabled for archiving requires a Zimbra archive license. 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 Zimbra Collaboration Server Single Server Installation 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 in 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 restart**

### 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 Zimbra Collaboration Server Multi-Server Installation 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-a1a5-7391d4763616 d6b9a0 266e-25ca-a1a5-7451d4951616
```

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

4. 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.

Archiving is to a single account defined by **amavisArchiveQuarantineTo**. The attribute, **zimbraArchiveAccount** is a multi-valued attribute containing all the accounts that have been archived for the given account.

### 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.

When the template based on the **zimbraArchiveAccountDateTemplate** attribute is set up, **amavisArchiveQuarantineAccount** is updated to the new template name when **zmconfigarchive** is run.

## 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:*** *Accounts with archiving enabled are counted against the number of Zimbra licenses purchased for archiving. To see current license information, go to the administration console, Global Settings>License tab. Archive mailboxes are listed in the administration console along with the live accounts.*

### Create an archive mailbox and assign a COS

1. Log on as ZCS .
2. Type **zmarchiveconfig enable <account@example.com> archive-cos <archive>**

Archive accounts are created based on the Zimbra Archive name templates.

- The attribute **zimbraIsSystemResource** 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 Delegated Administration on page 83.

### 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 **c**ross **m**ailbox **s**earch. With this practice, all target mailboxes are listed together*

- Limit the number of messages returned by the search. The default is 500 results.
- 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 article Zimbra Web Client Search Tips at *http://wiki.zimbra.com/wiki/Search_Tips*.

  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.

# 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 from the CLI or from the administration console.

Topics in this chapter include:

- Customizing Base Theme Colors
- Replacing the ZWC Logo
- Using Command Line Interface
- Changing Theme Colors and Logo from the Admin 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.

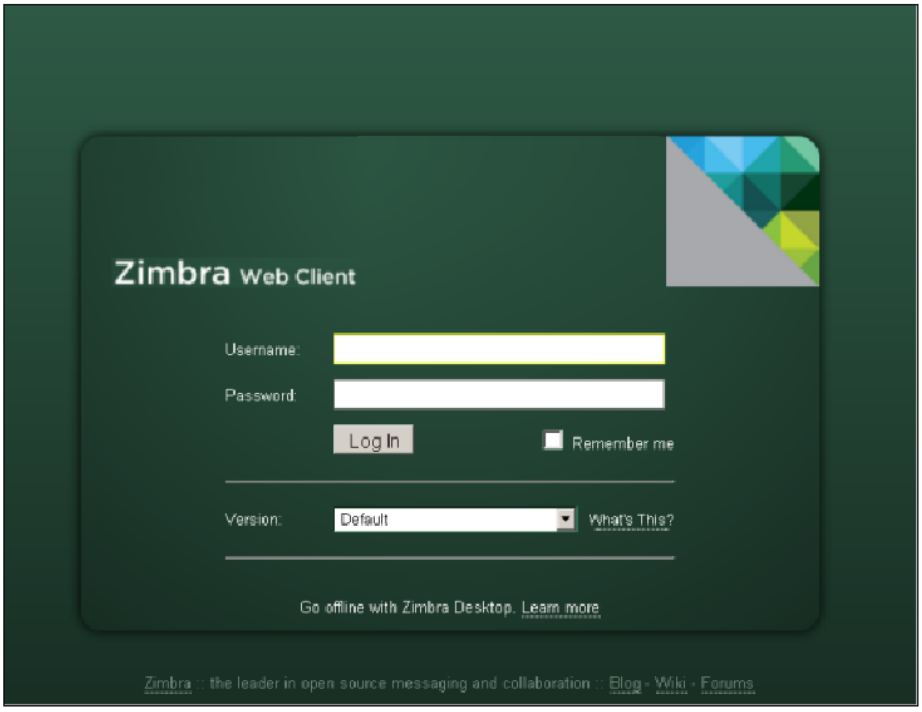
***Important:*** *If the logo and base colors are customized in multi-domain ZCS environments, you must set a virtual host as the base color and logo attributes are displayed based on the Host header sent by the browser. See* *Virtual Hosts on page 121**.*

***Note:*** *A number of Zimbra themes are included with ZCS. Some of these themes, such as lemongrass, Hot Rod, and Waves, 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.*

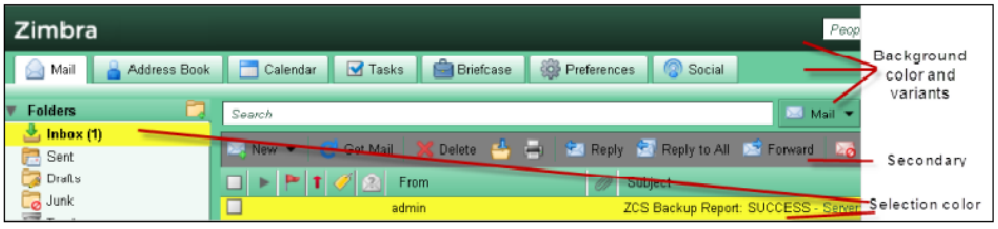
## Customizing Base Theme Colors

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.
- The selection color is the color displayed for a selected item such as a message or an item in the Overview pane.




- 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 300 x 48.
- Small company logo in the upper-left of the ZWC application and the administration console. The dimension of the graphic must be exactly 200 x 28.
- 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

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

   **zmmailboxdctl**

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

2. To apply the changes, type

   **zmmailboxdctl reload**

## Changing Theme Colors and Logo from the Admin 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 and selection headers in the Navigation pane.
- 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.

# 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 Server. The administration console is the main tool for maintaining the Zimbra Collaboration Server, but some functions can only be changed from the CLI utility.

The CLI utility can be used for the following:

- Provisioning accounts*
- Backup 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.

## 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.

**Zimbra CLI Commands**

| CLI | Description |
|---|---|
| **antispam-mysqladmin** | Send admin commands to anti=spam MySQL server |
| **antispam-mysql** | Enters interactive command-line MySQL session with the mailbox mysql |
| **antispam-mysql.server** | Start, stop the SQL instance for the mailbox package |
| **ldap** | Start, stop, or find the status of Zimbra LDAP |
| **ldapsearch** | Perform a search on an LDAP server |
| **logmysqladmin** | Send myslqadmin 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 |

### Zimbra CLI Commands

| CLI | Description |
|---|---|
| **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 |
| **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 |
| **zmantispamdbpasswd** | Changes anti-spam MySQL database password |
| | |
| **zmapachectl** | Start, stop, reload, or check status of Apache service (for spell check) |
| **zmarchiveconfig** | 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 auditswatch |
| **zmbackup** | Performs full backups and incremental backups for a designated mail host. |
| **zmbackupabort** | Stops a backup that is in process. |
| **zmbackupquery** | Find a specific full backup set |
| **zmblobchk** | Check consistency of the Zimbra blob store |
| **zmcalchk** | Check consistency of appointments and attendees in the Zimbra calendar |
| **zmcbpolicydctl** | Start, stop, and restart the cluebringer policyd service if enabled |
| **zmconfigdctl** | Start, stop, kill, restart status of the MTA configuration daemon. |
| **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/ Restart Service)** | Start, stop, restart, status of the Zimbra servers. Also can use to find the Zimbra version installed |

### Zimbra CLI Commands

| CLI | Description |
|---|---|
| **zmconvertctl** | Start, stop, the conversion server or find the status of the converted attachments conversion/ indexing |
| **zmdevicesstats** | Number of unique ActiveSync device IDs per server |
| **zmgdcutil** | (get devices count) gives the total devices system wide without the need of specifying individual servers. |
| **zmdumpenv** | General information about the server environment is displayed |
| **zmgsautil** | Create, delete the GAL sync account and initiate manual syncs. |
| **zmgsautil** | Global Address Book (GAL) synchronization command line utility. |
| **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 |
| **zmgavaext** | Execute Java and Zimbra-specific environment settings including extension based jars. |
| **zmldappasswd** | Changes the LDAP password |
| **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 7.1.2 or earlier)** | Used to move selected mailboxes from one Zimbra server to another. |
| **zmmboxsearch (Cross Mailbox Search)** | Search across mailboxes to find messages and attachments |

### Zimbra CLI Commands

| CLI | Description |
|---|---|
| **zmmboxmove** | 7.1.3 and later. Used to move selected mailboxes from one Zimbra server to another. |
| **zmmboxmovequery** | 7.1.3 and later. Used to query ongoing mailbox moves on a server |
| **zmpurgeoldmbox** | 7.1.3 and later. Purges a mailbox from the old server after a mailbox move |
| **zmmemcachedctl** | Start, stop, and restart |
| **zmmetadump** | Support tool that dumps an item's metadata in a human-readable form |
| **zmmilterctl** | Start, stop, and restart the zimbra milter server if enabled |
| **zmmtaconfigdctl** | Beginning in ZCS 7.0, this command is not used. Use **zmconfigdctl**. |
| **zmmtactl** | Start, stop, or find the status of the MTA |
| **zmmypasswd** | Change MySQL passwords |
| **zmmysqlstatus** | Status of mailbox SQL instance |
| **zmnginxconf** | Command line utility to output the reverse proxy configuration |
| **zmnginxctl** | Start, stop, and restart the zimbra reverse proxy |
| **zmproxyctl** | 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 |
| **zmproxyctl** | Start, stop, restart, and find the status of the IMAP proxy service |
| **zmproxypurge** | Purges POP/IMAP routing information from one or more memcached servers |
| **zmpurgeoldmbox** | Purges POP/IMAP routing information from one or more memached servers |
| **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 |

### Zimbra CLI Commands

| CLI | Description |
|---|---|
| **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** | 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 |
| **zmswatchctl** | Start, stop, or find the status of the Swatch process, which is used in monitoring |
| **zmsyncreverseproxy** | Decodes the sync request/responses and logs them when verbose mode is turned on. |
| **zmthrdump** | Initiate a thread dump and save the data to a file with a timestamp |
| **zmtlsctl** | Set the Web server mode to the communication protocol options: HTTP, HTTPS or mixed |
| **zmtrainsa** | Used to train the anti-spam filter to recognize what is spam or ham |
| **zmtzupdate** | Provides mechanism to process timezone changes from the command line |
| **zmupdateauthkeys** | Used to fetch the ssh encryption keys created by zmsshkeygen |

**Zimbra CLI Commands**

| CLI | Description |
|---|---|
| **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 is **zmprov [cmd] [argument]**.

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 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"
```

The attributes for the tasks zmprov can be used with are listed when you type zmprov -h. The task area divided into the following sections:

- Accounts
- Calendar
- Commands

- Config
- COS
- Domain
- Free/busy
- Distribution list
- Logging
- Miscellaneous commands
- Mailbox
- Reverse proxy
- Right - for delegated administration
- Search
- Server
- Share

| 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.

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| **Account Provisioning Commands** | | |
| **addAccountAlias** | **aaa** | {name@domain\|id\|adminName} {alias@domain}<br>**zmprov aaa joe@domain.com joe.smith@engr.domain.com** |

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| **checkPasswordStrength** | **cps** | Syntax: {name@doman\|id} {password}<br>**Note:** This command does not check the password age or history.<br>**zmprov cps joe@domain.com test123** |
| **createAccount** | **ca** | Syntax:{name@domain} {password} [attribute1 value1 etc]<br>Type on one line.<br>**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}<br>**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}<br>**zmprov ga joe@domain.com** |
| **getAccountMembership** | **gam** | {name@domain\|id} |
| **getAllAccounts** | **gaa** | Syntax: [-v] [{domain}]<br>**zmprov -l gaa**<br>**zmprov gaa -v domain.com** |
| **getAllAdminAccounts** | **gaaa** | Syntax: gaaa<br>**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...]] |

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| **modifyAccount** | **ma** | {name@domain\|id\|adminName} [attribute1 value1 etc]<br>**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}<br>**zmprov raa joe@domain.com joe.smith@engr.domain.com** |
| **renameAccount** | **ra** | {name@domain\|id} {newname@domain}<br>**zmprov ra joe@domain.com joe23@domain.com**<br>Note: After you rename an account, you should run a full backup for that account. **zmbackup -f - <servername.com> -a <newaccountname@servername.com>** |
| **setAccountCOS** | **sac** | {name@domain\|id\|adminName} {cos-name\|cos-id}<br>**zmprov sac joe@domain.com FieldTechnician** |
| **setPassword** | **sp** | {name@domain\|id\|adminName} {password}<br>**Note**: Passwords cannot included accented characters in the string. Example of accented characters that cannot be used: ã, é, í, ú, ü, ñ.<br>**zmprov sp joe@domain.com test321** |
| **Calendar Resource Provisioning Commands** | | |
| **createCalendarResource** | **ccr** | {name@domain} [attr1 value1 [attr2 value2...]] |
| **deleteCalendarResource** | **dcr** | {name@domain\|id} |

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| **getAllCalendarResources** | **gacr** | [-v] [{domain}] |
| **getCalendarResource** | **gcr** | {name@domain\|id} |
| **modifyCalendarResource** | **mcr** | {name@domain\|id} [attr1 value1 {attr2 value2...]] |
| **purgeAccountCalendarCache** | **pacc** | {name@domain\id} [...] |
| **renameCalendarResource** | **rcr** | {name@domain\|id} {newName@domain} |
| **Free Busy Commands** | | |
| **getAllFbp** | **gafbp** | [-v] |
| **getFreebusyQueueInfo** | **gfbqi** | [{provider-name}] |
| **pushFreebusy** | **pfb** | {domain \| account-id} [account-id...] |
| **pushFreebusyDomain** | **pfbd** | {domain} |
| **purgeFreebusyQueue** | **pfbg** | [{provider-name}] |
| **Domain Provisioning Commands** | | |
| **countAccount** | **cta** | {domain\|id}<br>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]<br>**zmprov cd mktng.domain.com zimbraAuthMech zimbra** |
| **deleteDomain** | **dd** | {domain\|id}<br>**zmprov dd mktng.domain.com** |
| **getDomain** | **gd** | {domain\|id}<br>**zmprov gd mktng.domain.com** |
| **getDomainInfo** | **gdi** | name\|id\|virtualHostname {value} [attr1 [attr2...]] |
| **getAllDomains** | **gad** | [-v] |

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| **modifyDomain** | **md** | {domain\|id} [attribute1 value1 etc]<br>**zmprov md domain.com zimbraGalMaxResults 500**<br>***Note:*** *Do not modify* **zimbraDomainRenameInfo** *manually. This is automatically updated when a domain is renamed.* |
| **renameDomain** | **rd** | {domain\|id} {newDomain}<br>***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]<br>**zmprov cc Executive zimbraAttachmentsBlocked FALSE zimbraAuthTokenLifetime 60m zimbraMailQuota 100M zimbraMailMessageLifetime 0** |
| **deleteCos** | **dc** | {name\|id}<br>**zmprov dc Executive** |
| **getCos** | **gc** | {name\|id}<br>**zmprov gc Executive** |
| **getAllCos** | **gac** | [-v]<br>**zmprov gac -v** |
| **modifyCos** | **mc** | {name\|id} [attribute1 value1 etc]<br>**zmprov mc Executive zimbraAttachmentsBlocked TRUE** |
| **renameCos** | **rc** | {name\|id} {newName}<br>**zmprov rc Executive Business** |
| **Server Provisioning Commands** | | |
| **createServer** | **cs** | {name} [attribute1 value1 etc] |
| **deleteServer** | **ds** | {name\|id}<br>**zmprov ds domain.com** |

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| **getServer** | **gs** | {name\|id}<br>**zmprov gs domain.com** |
| **getAllServers** | **gas** | [-v]<br>**zmprov gas** |
| **modifyServer** | **ms** | {name\|id} [attribute1 value1 etc]<br>**zmprov ms domain.com zimbraVirusDefinitionsUpdateFrequency 2h** |
| **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 nginix use). |
| **Config Provisioning Commands** | | |
| **getAllConfig** | **gacf** | [-v]<br>All LDAP settings are displayed |
| **getConfig** | **gcf** | {name} |
| **modifyConfig** | **mcf** | attr1 value1<br>Modifies the LDAP settings. |
| **createXMPPComponent** | **cxc** | {short-name} {domain} {server} {classname} {category} {type} [attr value1 [attr2 value2...]] |
| **deleteXMPPComponent** | **dxc** | {xmpp-component-name} |
| **getXMPPComponent** | **gxc** | {name@domain} [attr1 [attr2 value2]] |
| **modifyXMPPComponent** | **mxc** | {name@domain} [attr1 [attr2 value2]] |
| **Distribution List Provisioning Commands** | | |
| **createDistributionList** | **cdl** | {list@domain}<br>**zmprov cdl needlepoint-list@domain.com** |
| **addDistributionListMember** | **adlm** | {list@domain\|id} {member@domain}<br>**zmprov adlm needlepoint-list@domain.com singer23@mail.free.net** |
| **removeDistributionListMember** | **rdlm** | {list@domain\|id}<br>**zmprov rdlm needlepoint-list@domain.com singer23@mail.free.net** |

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| **getAlldistributionLists** | **gadl** | [-v] |
| **get DistributionListmembership** | **gdlm** | {name@domain\|id} |
| **getDistributionList** | **gdl** | {list@domain\|id}<br>**zmprov gdl list@domain.com** |
| **modifyDistributionList** | **mdl** | {list@domain\|id} attr1 value1 {attr2 value2...}<br>**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} |
| **Mailbox Commands** | | |
| **getMailboxInfo---** | **gmi** | {account} |
| **getQuotaUsage---** | **gqu** | {server} |
| **reIndexMailbox** | **rim** | {name@domain\|id} {start\|status\|cancel} [{reindex-by} {value1} [value2...]] |
| **RecalculateMailboxCounts** | **rmc** | {name@domain\|id}<br>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.<br><br>***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.* |
| **selectMailbox** | **sm** | {account-name} [{zmmailbox commands}] |
| **Logs** | | |

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| **addAccount Logger** | **aal** | {name@domain\|id} {logging-category} {debug\|info\|warn\|error}<br>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]<br>Shows all individual custom logger account |
| **removeAccountLogger** | **ral** | [-s/ --server hostname] {name@domain\|id} {logging-category}<br>When name@domain is specified, removes the custom logger created for the account otherwise removes all accounts all account loggers from the system. |
| See the zmprov Log Categories on page 282 for a list of logging categories. | | |
| **Search** | | |
| **searchGAL** | **sg** | {domain} {name}<br>**zmprov sg joe** |
| **autoCompleteGal** | **acg** | {domain} {name} |
| **searchAccounts** | **sa** | [-v] {ldap-query} [limit] [offset] [sortBy {attribute} [sortAscending 0\|1] [domain {domain}] |
| **searchCalendarResources** | **scr** | [-v] domain attr op value {attr op value...] |
| **Share Provisioning Commands** | | |
| For a GUI view of results, see Distribution List Shares tab on the administration console | | |
| **getPublishedDistributionListShareInfo** | **gpdlsi** | {dl-name\|dl-id} [{owner-name\|owner-id}] |
| **getShareInfo** | **gsi** | {owner-name\|owner-id} |
| **publishDistribtionListShareInfo** | **pdlsi** | {+\|-} {dl-name@domain\|id} {owner-name\|owner-id} [{folder-path\|folder-id}] |
| **Miscellaneous Provisioning Commands** | | |

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| **countObjects** | **cto** | {type} [-d {domain\|id}].<br>countObjects can only be used with zmprov -l/--ldap |
| **createBulkAccounts** | **cabulk** | {domain} {namemask} {number of accounts to create} |
| **describe** | **desc** | [[-v] [-ni] [{entry-type}]] \| [-a {attribute-name}]<br>Prints all attribute names (account, domain, COS, servers, etc.). |
| **flushCache** | **fc** | [-a] {acl\|locale\|skin\|uistrings\|license\|all\|account\|config\|globalgrant\| cos\|domain\|galgroup\|group\|mime\|server\|zimlet\|<extension-cache-type>} [name1\|id1 [name2\|i d2...]]<br>Flush cached LDAP entries for a type. See Zimbra LDAP Service chapter, Flushing LDAP Cache |
| **generateDomainPreAuthKey** | **gdpak** | {domain\|id}<br>Generates a pre-authentication key to enable a trusted third party to authenticate to allow for single-sign on. Used in conjunction with GenerateDomainPreAuth. |
| **generateDomainPreAuth** | **gdpa** | {domain\|id} {name} {name\|id\|foreignPrincipal} {timestamp\|0} {expires\|0}<br>Generates preAuth values for comparison. |
| **syncGal** | **syg** | {domain} [{token}] |
| **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. |

| Long Name | Short Name | Syntax, Example, and Notes |
|---|---|---|
| --getAllReverseProxyBackends | -garpb | Returns the list of servers that have **zimbraReverseProxyLookupTarget=TRUE.** Basically if a mailbox server is available for lookup requests from the proxy. |
| --getAllReverseProxyDomains | -garpd | Returns a list of all domains configured with **ZimbraSSLCertificate zimbraVirtualHostname** and **zimbraVirtualIPAddress** configured. This allows the proxy to configure a list of domains to serve customized/domain certificates for. |

### 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 Server 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 query if a value is set for a multi-valued attribute.

  ```
  zmprov gs server.com attribute=value
  ```

  For example, **zmprov gs example.com zimbraServiceEnabled=ldap** to find out if the ldap service is enabled.

- 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.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**

## zmarchiveconfig

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...** | | |
| **enable <account>** | | [archive-address <aaddr> [archive-cos <cos>]<br>[archive-create <TRUE/FALSE>] [archive-password <pa<br>[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 |
| **--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**

## zmbackup

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.

**zmbackup {-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]). |
| **--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. |
| **--includeBlobs** | | Include blobs in full backup. If this is unspecified, the server config is used. |
| **--includeHsmBlobs** | | Include blobs on HSM volumes in full backup. If this is unspecified, the server config is used. |
| **--includeSearchIndex** | | Include search index in full backup. If this is unspecified, the server config is used. |
| **--noZip** | | Backs up blobs as individual files rather than in zip files. |
| **--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** | Backs up blobs in compressed zip files. Ignored if --zipStore is specified. |
| **--zipStore** | | Backup blobs in zip file without compression. (default) |

### 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**

  **zmbackup -f -a all -s server1.domain.com**

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

  **zmbackup -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.

  **zmbackup -f -a user1@domain.com -s server1**

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

  **zmbackup -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 |

## zmcalchk

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 appointmen**t 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<br>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. |
| **Options that will be passed to zmbackup** | | |
| **no compression** | -n | Backs up blobs as individual files rather than in zip files |
| **compress** | **-z** | Backs up blobs in compressed zip files. Ignored if --zipStore is specified. |
| **--zipStore** | | Backs up blobs in zip file without compression. |
| **target** | **-t** | Can be used only to designate a full back target location. The default is /opt/zimbra/backup.<br><br>***Note:*** *You cannot designate a target for incremental backups. If a target (-t) location is added for incremental scheduled backups, it is ignored.* |
| **account** | **-a** | Account specific. The default is all accounts. |
| **--mail-report** | | Send an email report to the admin user. |
| **--server** | | server - Mail server hostname. Default is localhost. |
| **--sync** | | Runs full backup synchronously. |
| **--excludeBlobs** | | Exclude blobs from full backup. If unspecified, server config is used. |

| Name | Command Name | Description |
|---|---|---|
| **--includeBlobs** | | Include blobs in full backup. If unspecified, the server config is used. |
| **--excludeHsmBlobs** | | Exclude blobs on HSM volumes from full backup. If unspecified, the server config is used. |
| **--includeHsmBlobs** | | Include blobs on HSM volumes in full backup. If unspecified, the server config is used. |
| **--excludeSearchIndex** | | Exclude search index form full backup. If unspecified, the server config is used. |
| **--includeSearchIndex** | | Include search index in full backup. If unspecified, the server config is used. |
| **Cron schedule**<br>backup-type: <i \| f \| d arg> | | |
| **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. <arg> is n(d\|m\|y) |

## 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**

## zmbackupabort

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 **zmbackupquery** to find the label name.

**To stop the restore process.** The **zmbackupabort -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

**zmbackupabort [options]**

### Description

| Long Name | Short Name | Description |
|---|---|---|
| **--debug** | **-d** | Display diagnostics for debugging purposes |
| **--help** | **-h** | Displays the usage options for this command |
| **--label** | **-lb** | <**arg**> Label of the full backup to be aborted. Use the **zmbackupquery**, to find the label name. |
| **--restore** | **-r** | Abort the restore in process |
| **--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 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 |
| **--from** | | <**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 are 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 proceeded 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 |
| **--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 rodo 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 |

| Long Name | Short Name | Description |
|---|---|---|
| **--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 |
| **--label** | **-lb** | <**arg**> The label of the full backup to restore. Type this label to specify a backup file other then 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 rodo logs until this time |
| **--restoreFullBackupOnly** | **-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. |

| Long Name | Short Name | Description |
|---|---|---|
| **--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/Restart Service)

This command is run to start, to stop, or to restart services. You can also find which version of the Zimbra Collaboration Server 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. |
| **restart** | | Restarts all services and manager on this host. |
| **shutdown** | | Shutdown all services and manager on this host. When the manager is shutdown, you cannot query that status. |
| **start** | | Startup manager and all services on this host. |
| **startup** | | Startup manager and all services on this host. |
| **status** | | Returns services information for the named host. |
| **stop** | | Stop all services but leaves the manager running. |

## **zmmailboxmove** (Move Mailbox 7.1.2 or earlier)

zmmailboxmove command is used in ZCS 7.1.2 or earlier. For 7.1.3 or later use zmmboxmove (7.1.3 or later) to move mailboxes.

The zmmailboxmove 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. 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. . |
| --authtokenfile | -Y | Use auth token string (has to be in JSON format) from command line |
| --authtoken | -y | 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**

## **zmmboxmove** (7.1.3 or later)

Beginning with ZCS 7.1.3, the CLI command **zmmboxmove** is used to move mailboxes. The destination server manages the overall move process. Using the zmmboxmove command significantly reduces the account lockout time.

The CLI command **zmmboxmove** is used to move mailboxes 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 the LDAP is updated. After the mailbox is moved to a new server a copy still remains on the older server. You should check to see that all the mailbox content was moved successfully before purging the old mailbox.

### Syntax

**zmmboxmove -a <email> --from <src> --to <dest> [--sync]**

### Description

| Long Name | Short Name | Description |
|---|---|---|
| **--account** | **-a** | <**arg**> Email address of account to move |
| **--help** | **-h** | Displays the usage options for this command |
| **--from** | **-f** | <**arg**> Mail server hostname. Server where the --account mailbox is located |
| **--to** | **-t** | <**arg**> Destination server |
| **--sync** | **-sync** | Run synchronously |

## zmmboxmovequery

The CLI command, **zmmboxmovequery,** lists the information about ongoing mailbox moves on servers, both move-ins and move-outs.

### Syntax

**zmmboxmovequery -a <account email> [-s <server to query>]**

## zmpurgeoldmbox

The CLI command, **zmpurgeoldmbox**, purges the mailbox from the older server after a mailbox move.

### Syntax

**zmpurgeoldmbox -a <account email> [-s <server to purge>]**

### Description

| Long Name | Short Name | Description |
|---|---|---|
| **--account** | **-a** | <**arg**> Email address of account to purge |
| **--help** | **-h** | Displays the usage options for this command |
| **--server** | **-s** | <**arg**> Mail server hostname. Old server where the account existed |

## zmmboxsearch (Cross Mailbox Search)

The CLI command **zmmboxsearch** 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

**zmmboxsearch {-m <arg>} {-q <arg>} [-o <arg>] [-l <arg>] [-d <arg>] [options]**

### Description

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

### Example

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

**zmmboxsearch -m user1@yourdomain.com,user2@yourdomain.com -q “in:inbox” -d /var/tmp**

## zmcertmgr

The CLI command **zmcertmgr** is used to manage your global certificates from the command line. You can use the administration console to easily view, update and install global 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 |
|---|---|
| **viewdeployedcrt** | [all\|ldap\|mta\|proxy\|mailboxd]<br>View the deployed certificate. |
| **viewstagedcrt** | <self\|comm> [certfile] |
| **gencsr** | <self\|comm> [-new] [subject] [-subjectAltNames "host1,host2"]<br>Generate the certificate signing request. |
| **install** | <self\|comm> [-new] [validation_days-]<br>Install either a self signed or commercial signed certificate |
| **viewcsr** | <self\|comm> [csr_file]<br>View the certificate signing request information |
| **verifycrt** | <self\|comm> [priv_key] [certfile] |

## zmgsautil

The CLI command **zmgsautil** 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.<br>**deleteAccount [-a {galsynceaccountname}\|-i {account-id}]** |

| Long Name | Description |
|---|---|
| **trickleSync** | This syncs new and updated contact data only.<br>**trickleSync [-a {galsynceaccountname}\|-i {account-id}] [-d {datasource-id}] [-n {datsource-name}]**<br>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.<br>A cron job can be set up to run trickleSync. |
| **fullSync** | This syncs all LDAP contact data. You can also set this from the administration console.<br>**fullSync [-a {galsynceaccountname}\|-i {account-id}] [-d {datasource-id}] [-n {datsource-name}]** |
| **forceSync** | This should be used to reload the entire GAL if there is change in the filter, attribute mapping or LDAP server parameters.<br>forceSync **[-a {galsynceaccountname}\|-i {account-id}] [-d {datasource-id}] [-n {datsource-name}]** |

## 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 used with options changes other passwords.

For better security and audit trails the following passwords are generated in ZCS:

- **LDAP Admin password**. This is the master LDAP password. This is not new, but has been renamed.
- **LDAP Root password**. This is used for internal LDAP operations.
- **LDAP Postfix password**. This is the password used by the postfix user to identify itself to the LDAP serve and must be configured on the MTA server to be the same as the password on the LDAP master server.
- **LDAP Amavis password**. This is the password used by the amavis user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the password on the LDAP server.
- **LDAP Replication password**. This is the password used by the LDAP replication user to identify itself to the LDAP master and must be the same as the password on the LDAP master server.

### Syntax

**opt/zimbra/bin/zmldappasswd [-h] [-r] [-p] [-l] new password**

### Description

| Name | Syntax, Example, Notes |
|---|---|
| **-h** | Displays the help |
| **-a** | Changes **ldap_amavis-password** |
| **-l** | Changes **ldap_replication_password** |
| **-p** | Changes **ldap_postfix_password** |
| **-r** | Changes **ldap_root_passwd** |
| -c | Updates the password in the config database on replicas. Must be used with -1. |
| **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. Use **zmlocalconfig -i** to see a list of supported properties that can be configured by an administrator.

### 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 list of supported properties. |

| Long Name | Short Name | Description |
|---|---|---|
| **--format** | **-m** | <**arg**> Shows the values in one of these formats: plain (default), xml, shell, nokey. |
| **--changed** | **-n** | Shows the values for only those keys listed in the [args] that have been changed from their defaults |
| **--path** | **-p** | Shows which configuration file will be used |
| **--quiet** | **-q** | Suppress logging |
| **--random** | **-r** | This option is used with the edit option. Specified key is set to a random password string. |
| **--show** | **-s** | Forces the display of the password strings |
| **--unset** | **-u** | 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 |
| **zmmailbox help filter** | help on filter-related commands |
| **zmmailbox help folder** | help on folder-related commands |
| **zmmailbox help item** | help on item-related commands |
| **zmmailbox help message** | help on message-related commands |
| **zmmailbox help misc** | help on miscellaneous commands |
| **zmmailbox help permission** | help on permission commands |
| **zmmailbox help search** | help on search-related commands |
| **zmmailbox help tag** | help on tag-related commands |

### Examples

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

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

- To find the mailbox size for 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

**zmtlsctl [mode]**

mode = http, https, mixed, both, redirect

#### Steps to run

1. Type **zmtlsctl [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 |
| **--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 |

## zmproxyconfgen

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 |
| --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 |
| **--output** | **-o** | Specifies the format to be used for printing routing information with information. The fields that display by default are<br>• cache server<br>• account name<br>• 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.<br>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 |
| **--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.<br>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 |
| --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:<br>[/]element1[/element2][/@attr][=value] |

## zmstat-chart

This command is used to collect statistical information for the CPU, IO, mailboxd, MTAqueue, 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 SpamAssasin filter from messages users mark as "junk" "not junk" from their mailbox. See Anti-Spam Training Filters on page 53.

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 1st, 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 |
| **--help** | **-h** | Shows the help for the usage options for this tool. |
| **--id** | **-id** | <**arg**> Volume ID |
| **--list** | **-l** | Lists volumes |
| **--name** | **-n** | <**arg**> Volume name |
| **--path** | **-p** | <**arg**> Root path |
| **--server** | **-s** | <**arg**> Mail server hostname. Default is localhost. |
| **--setCurrent** | **-sc** | Sets the current volume |
| --type | -t | <**arg**> Volume type (primaryMessage, secondaryMessage, or index) |
| --turnOffSecondary | -ts | Turns off the current secondary message volume |

## zmzimletctl

This command is used to manage Zimlets and to list all zimlets on the server. See Chapter 14, Managing Zimlets. Most Zimlet deployment can be competed 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

**./zmproxyconfig [-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

## zmsyncreverseproxy

The CLI command zmsyncreverseproxy is used to reserve proxies mobile sync HTTP traffic between the source and forwarding server and port. Decodes the sync requests/responses and logs them when verbose mode is turned on.

### Syntax

**zmsyncreverseproxy [-v] [-d] [-L log4j.properties] -p <port number> -fs <fwd server> -fp <fwd port> [-sv syncversions]**

### Description

| Long Name | Short Name | Description |
|---|---|---|
| **--help** | **-h** | Displays help |
| **--verbose** | **-v** | Verbose mode, dumps full exception stack trace. |
| --debug | -d | Debug mode, dumps decoded sync messages |
| --port | -p | The port this service listens on |
| --forwardserver | -fs | The server host to forward requests to |
| --forwardport | -fp | The server port to forward requests to |
| --syncversions | -sv | Active sync versions supported |
| --logpropertyfile | -L | log4j property file, valid only with -l |

# Appendix B Configuring SPNEGO Single Sign-On for ZCS

The SPNEGO protocol mechanism can be configured on ZCS for single sign-on authentication to the Zimbra Web Client. When users log on to their Intranet through Active Directory, they can enter their ZWC mailbox without having to re-authenticate to Zimbra.

The ZCS server is configured to redirect users attempting to log on to ZWC to a URL under SPNEGO protection. The server asks for authentication with Kerberos though SPNEGO and users are redirected to their ZWC mailbox. When users log out, they are redirected to a logout URL that displays a Launch button. When users click **Launch**, they are directed to the ZWC entry page.

***Note:*** *When users log on to their ZWC accounts from the Internet, the ZWC log in page displays and they must enter their ZWC password to log on.*

***Important:*** *If SPNEGO SSO is enabled on a domain, the browsers must be configured correctly. See* *Configure Your Browser on page 337**. Improperly configured browsers may pop up a user/pass dialog and if a user enters his correct AD domain username/password, he can still log into the Zimbra mailbox, and some browsers may display a "401 Unauthorized" error.*

## Configuration Process

1. Create the Kerberos keytab file.
   - Create an Active Directory service account. This account is used to generate the Kerberos keytab file.
   - Add the service Principal Names (SPN) directory property for an Active Directory service account.
   - Create the keytab file.
2. Enable and configure the SPNEGO protocol on the ZCS server.
3. Configure browsers

## Create the Kerberos Keytab File

An Active Directory service account is created in Domain for each ZCS mailstore server.

1. Create an Active Directory service account. This is the account used to generate the Kerberos keytab file that is added to the Zimbra server.
   a. Go to the Active Directory **Start> Programs>Administrative Tools>Active Directory Users and Computers** console.
   b. To create the service account, click the AD Domain name and from the expanded content right-click **Users** and select **New >User**. Complete the New Object – User dialog.
      - **Full name**: Enter the user display name for the AC service account. Recommend that the full name be the ZCS mailbox server name. Example: **mail1**
      - **User Logon Name**: This name is the value that is set for the **zimbraSpnegoAuthTargetName** server attribute in LDAP. Write it down. Example: **HTTP/mail1.example.com**
      - **User Logon Name (pre-Windows2000):** This name is used for the **–mapUser** parameter in the **setspn** and **ktpass** commands. Example: **mail1**.
      - Click **Next**.
   c. Enter and confirm the password. This password is used for the **–pass {AD-user-password}** parameter in the **ktpass** command, configured below.
   d. Check **Password never expires** and **User cannot change password**, and click **Next**.
   e. Click **Finish** to create the user. The service account name displays in the Users directory.
2. Use the **setspn** command to map the mailbox server name as the service Principal Names (SPN) to the user account. The SPN is used in the process of mutual authentication between the client and the server hosting a particular service.
   a. From the command prompt, type **setspn –a {userlogonname} {serviceaccountname}**

   Example

   ```
   setspn –a HTTP/mail1.example.com mail1
   ```

   b. To verify that the SPN is registered, type
   **C:\>setspn –l {accountname}**
   A list of registered SPNs is displayed.
3. Create the keytab file used when signing into the Kerberos domain. Use the ktpass tool from the Windows Server toolkit to create the Kerberos keytab.

***Note:*** *A Kerberos keytab file contains a list of keys that are analogous to user passwords. Restrict and monitor permissions on any keytab files you create.*

The command to type follows:

**ktpass -out {keytab-file-to-produce} -princ {Service-Principal-Name}@{the-kerberos-realm} -mapUser {AD-user} -mapOp set -pass {AD-user-password} -crypto RC4-HMAC-NT -pType KRB5_NT_PRINCIPAL**

| | |
|---|---|
| **Ktpass -out** | The key is written to this output file.<br>Enter the directory location and keytab file name. The keytab file name is **jetty.keytab**.<br>For example, C: \Temp\spnego**jetty.keytab** |
| **-princ** | This is the principal name.<br>Enter the service Principal Name as used in **Step 2** in Setting up the Microsoft Windows Active Directory Domain Controller section. For example, HTTP/ mail1.example.com@COMPANY.COM |
| **-mapUser** | This maps –princ value to this user account.<br>Enter the AD service account user name entered in the **User Logon Name (pre-Windows2000)** set in **Step 1.b** in Setting up the Microsoft Windows Active Directory Domain Controller section. |
| **-mapOp** | This sets the mapping. The value for this parameter is **set** |
| **-pass** | This is the password to use.<br>Enter the password entered in the **User Logon Name (pre-Windows2000)** set in **Step 1.c** in Setting up the Microsoft Windows Active Directory Domain Controller section. |
| **-crypto** | This is the cryptosystem to use.<br>Enter **RC4-HMAC-NT** |
| **-pType** | Enter<br>**KRB5_NT_PRINCIPAL**<br>To avoid warning messages from the toolkit enter this value. |

Example:

**ktpass -out C: \Temp\spnego\jetty.keytab -princ HTTP/ mail1.example.com@COMPANY.COM -mapUser mail1 -mapOp set -pass password123 -crypto RC4-HMAC-NT -pType KRB5_NT_PRINCIPAL**

The command is confirmed with something similar to the example below.

```
Targeting domain controller: …
   Using legacy password setting method
   Successfully mapped HTTP/mail1.example.com to mail1.
   Key created.
   Output keytab to c:\Temp\spnego\jetty.keytab:
   Keytab version: 0x502
   keysize 71 HTTP HTTP/mail1.example.com@COMPANY.COM ptype 1
(KRB5_NT_PRINCIPAL) vno3 etype 0x17 (RC4-HMAC) keylength 16
(0xc383f6a25f1e195d5aef495c980c2bfe)
```

4. Transfer the keytab file (jetty.keytab) to the Zimbra server. Copy the file created in step 3 to the following Zimbra server location: **/opt/zimbra/jetty/etc**

***Important:*** *Do not rename the jetty.keytab file. This file name is referenced from various configuration files.*

Repeat steps 1 to 4 to create an create the keytab file (**jetty.keytab**) for each Zimbra mailstore server.

## Configure ZCS

SPNEGO attributes in Global Config and on each Zimbra server are configured and pre-authentication is set up for the domain. Use the zmprov CLI to modify the Zimbra server.

***Note:*** *Only one Kerberos REALM is supported per ZCS installation*

1. Modify the following global config attributes, with the **zmprov mcf** command.

| | |
|---|---|
| **zimbraSpnegoAuthEnabled** | Set to TRUE. |
| **zimbraSpnegoAuthErrorURL** | This is the URL users are redirected to when spnego auth fails. Setting it to **/zimbra/?ignoreLoginURL=1** will redirect user to the regular Zimbra login page, where user will be prompted for their zimbra user name and password. |
| **zimbraSpnegoAuthRealm** | The Kerberos realm in the domain controller This is the domain name in the Active Directory. (COMPANY.COM) |

To modify the global config attributes, type:

a. **zmprov mcf zimbraSpnegoAuthEnabled TRUE**

b. **zmprov mcf zimbraSpnegoAuthErrorURL '/zimbra/?ignoreLoginURL=1**

c. **zmprov mcf zimbraSpnegoAuthRealm <COMPANY.COM>**

2. On each Zimbra server, modify the following global config attributes with the **zmprov ms** command.

| | |
|---|---|
| **zimbraSpnegoAuthTargetName** | This is the user logon name from Step 1 B , User Logon Name. |
| **zimbraSpnegoAuthPrincipal** | Enter the user logon name set in zimbraSpnegoAuthTargetName and the address set in global config zimbraSpnegoAuthRealm<br>Type as **zimbraSpnegoAuthTargetName@zimbraSpnegoAuthRealm**<br>For example, **HTTP/mail1.example.com@COMPANY.COM** |

To modify the server global config attributes, type:

a. **Zmprov ms mail1.example.com zimbraSpnegoAuthTargetName HTTP/mail1.example.com**

b. **zmprov ms mail1.example.com zimbraSpnegoAuthPrincipal HTTP/mail1.example.com@COMPANY.COM**

3. The following is set up on the domain.

- Kerberos Realm
- Virtual host
- Web client login URL and UAs
- Web client logout URL and UAs

a. Set up Kerberos Realm for the domain. This is the same realm set in the global config attribute **zimbraSpnegoAuthRealm** . Type **zmprov md {domain} zimbraAuthKerberos5Realm {kerberosrealm}**

b. Set up the virtual hosts for the domain. Virtual-hostname-***** are the hostnames you can browse to for the Zimbra Web Client UI. Type **zmprov md {domain} +zimbraVirtualHostname {virtual-hostname-1} +zimbraVirtualHostname {virtual-hostname-2} ...**

c. Setup the web client log in URL and UAs allowed for the login URL on the domain.

- Set the login URL. The login URL is the URL to redirect users to when the Zimbra auth token is expired. **Zmprov md {domain} zimbraWebClientLoginURL '../../service/spnego'**

- Honor only supported platforms and browsers. **zimbraWebClientLoginURLAllowedUA** is a multi-valued attribute, values are regex. If this is not set, all UAs are allowed. If multiple values are set, an UA is allowed as long as it matches any one of the values. **zmprov md {domain} +zimbraWebClientLoginURLAllowedUA {UA-regex-1} +zimbraWebClientLoginURLAllowedUA {UA-regex-2} ...**

For example, to honor zimbraWebClientLoginURL only for Firefox, Internet Explorer, Chrome, and Safari on computers running Windows, and Safari on Apple Mac computers, type the following commands.

- **zmprov md {domain} +zimbraWebClientLoginURLAllowedUA '.*Windows.*Firefox/3.*'**
- **zmprov md {domain} +zimbraWebClientLoginURLAllowedUA '.*MSIE.*Windows.*'**
- **zmprov md {domain} +zimbraWebClientLoginURLAllowedUA '.*Windows.*Chrome.*'**
- **zmprov md {domain} +zimbraWebClientLoginURLAllowedUA '.*Windows.*Safari.*'**
- **zmprov md {domain} +zimbraWebClientLoginURLAllowedUA '.*Macintosh.*Safari.*'**

d. Setup the web client logout URL and UAs allowed for the logout URL on the domain.

- Set the logout URL. The logout URL is the URL to redirect users to when users click Logout. **Zmprov md {domain} zimbraWebClientLogoutURL '../?sso=1'**
- Honor only supported platforms and browsers. **zimbraWebClientLogoutURLAllowedUA** is a multi-valued attribute, values are regex. If this is not set, all UAs are allowed. If multiple values are set, an UA is allowed as long as it matches any one of the values. **zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA {UA-regex-1} +zimbraWebClientLogoutURLAllowedUA {UA-regex-2} ...**

For example, to honor zimbraWebClientLogoutURL only for Firefox, Internet Explorer, Chrome, and Safari on computers running Windows, and Safari on Apple Mac computers, type the following commands.

- **zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA '.*Windows.*Firefox/3.*'**
- **zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA '.*MSIE.*Windows.*'**
- **zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA '.*Windows.*Chrome.*'**
- **zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA '.*Windows.*Safari.*'**

## Configure Your Browser

When the SPNEGO SSO feature is enabled on your domain, user's browsers must be configured properly. Improperly configured browsers will behave differently depending on the browser.

The following browsers are supported:

- For computers running Windows: Internet Explorer 6.0 or later, Firefox 3.0 or later, Chrome, Safari
- Apple Mac computer: Safari

1. Firefox browser for computers running Windows
   a. In Firefox browse to **about:config**. In the Firefox browser address field, type **about:config**. The **This might void your warrant** warning displays.
   b. Click **I'll be careful, I promise!**
   c. Search in Filters, type **network.n**. Enter a comma-delimited list of trusted domains or URLs.

      Double-click **network.negotiate-auth.delegation-uris**. Enter **http://,https://**

      Double-click **network.negotiate-auth.trusted-uris**. Enter **http://,https://**

      *Or, to set specific URLs,*

      Double-click **network.negotiate-auth.delegation-uris**. Enter the domain addresses. For example, http://mail1.example.com,https://mail2.example.com

      Double-click **network.negotiate-auth.trusted-uris**. Enter the domain addresses. For example, http://mail1.example.com,https://mail2.example.com

2. Internet Explorer, Chrome, and Safari for computers running Windows
   a. In these browsers, go to **Tools>Internet Options>Security > Local Intranet>Sites**. On the Sites dialog make sure all items are checked.
   b. Select **Advanced**. Add the domain server (hostname) URL, both http:// and https://
   c. Click **OK** to close the file.
   d. Go to **Tools > Options > Advanced > Security**. Locate and check **Enable Integrated Windows Authentication.**
   e. Click **OK** and close the browser.
3. Safari for Apple Mac computers. No configuration is necessary.

## Test your setup

1. On a Windows computer or an Apple Mac computer, log in to the computer as a domain user.

Your ticket as a domain user will be saved on the computer. The token will be picked up by the spnego-aware browser and sent in the Authorization header to the Zimbra server.

2. Browse to the Zimbra Web Client log on page. You should be redirected to your ZWC inbox without being prompted for user name and password.

   If spnego auth fails, the user is redirected to an error URL.

## Troubleshooting setup

Make sure the following are true.

- The browser is in the Intranet zone.
- The user is accessing the server using a Hostname rather than IP address.
- Integrated Windows authentication in Internet Explorer is enabled, and the host is trusted in Firefox.
- The server is not local to the browser.
- The client's Kerberos system is authenticated to a domain controller.

- If the browser display the "401 Unauthorized", it's most likely that the browser either did not send another request with Authorization in response to the 401, or had sent an Authorization which is not using the GSS-API/ SPNEGO scheme.

  Check your browser settings, and make sure it is one of the supported browsers/platforms

- If you are redirected to the error URL specified in **zimbraSpnegoAuthErrorURL**, that means The SPNEGO authentication sequence does not work.

  Take a network trace, make sure the browser sends Authorization header in response to the 401. Make sure the Negotiate is using GSS-API/ SPNEGO, not NTLM (use a network packet decoder like Wireshark) .

  After verifying that the browser is sending the correct Negotiate, if it still does not work, turn on the following debug and check Zimbra logs:

  - ADD "-DDEBUG=true -Dsun.security.spnego.debug=all" (note, not replace) to localconfig key spnego_java_options
  - Add log4j.logger.org.mortbay.log=DEBUG in log4j

  Then restart the mailbox server.

  Browse to the debug snoop page: http://{server}:{port}/spnego/snoop.jsp. See if you can access the snoop.jsp

  Check zmmailboxd.out and mailox.log for debug output.

***** One of the errors at this stage could be because of clock skew on the jetty server. If this is the case, it should be shown in zmmailboxd.out. Fix the clock skew and try again.

# Appendix C 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 it data into syslog.
This is primarily so that logger can read the data and keep the administration console status up-to-date.
Status logging job runs every 2 minutes.

### Backups

Full and increment 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 then 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 es when executing SQL statements. This script is run 1:30 a.m.on Sunday.

### Report on any database inconsistencies

**zmdbintegrityreport** 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 **zmdbintegrityreport** 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 zmdbintegrityreport_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 -l 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/zmbackup -f   -a all
0 1 * * 0-5 /opt/zimbra/bin/zmbackup -i
0 0 * * * /opt/zimbra/bin/zmbackup -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/zmqueuelog
#
# 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
a/dspam/bin/dspam_logrotate -a 60 -l /opt/zimbra/data/dspam/data/z/i/zimbra/zimb
ra.log
#
# 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
s-*' -mtime +1 -exec rm -rf {} \; > /dev/null 2>&1
#
# 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 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.

### OOTO

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

### Open Source

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

### OS

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

### POP

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

### Provisioning

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

### RBH

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

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

**Redo Logs**

Detailed transaction log for the  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 293
aborting backup 229
access to distribution lists 149
account
    assign to mailbox server 145
    deleting 147
    restoring 233
account authentication 36
account distribution by COS 144
account limits by domain 124
account migration wizard 135
account provisioning, zmprov 271
account quota 172
account quota and MTA 52
account status 146
account types by COS, setting 124
account types, tracking number assigned 124
account, creation date 133
account, password restriction 145
account, provision with zmprov 280
accounts
    batch provisioning 143
accounts object 40
accounts, list all 281
accounts, number used 114
accounts, setting up and configuring 134
accounts, user 75
active status 146
add logos for a domain 261
address book size limit, configuring 165
address book, features 165
addresses, search for 80
admin console, tasks 77
admin extensions 130
admin password, change 280
administration console 16, 73
administration tasks 133
administrator message of the day 78, 79
administrator password, change 74
advanced ZWC 155
alias, add with zmprov CLI 280
anti-spam component 17
anti-spam protection 53
anti-spam settings 109
anti-spam statistics 201
anti-spam training filter 53
anti-virus component 17
anti-virus protection 53
anti-virus settings 110
anti-virus statistics 201
anti-virus updates 53, 110
application packages, Zimbra 19
appointment reminder 169
appointment reminder popup, Yahoo!BrowserPlus 169
appointments, disabling editing of 167
archive mailboxes, creating 253
archive templates 252
Archiving 245
archiving attribute 252
archiving package, installing as an update to ZCS 248
archiving, administering archive server 251
Archiving, creating dedicated COS 250
archiving, how it works 246
attachment settings
    global settings 107
attachment viewing options, setting 178
attachment viewing, setting account options 176
attachments
    blocking 107
audit log 207
auth token, immediate session end 176
authentication 36
authentication modes 121
authentication, custom 38
autho token lifetime 176
autocomplete, name ranking 163
autoCompleteGal, zmprov 278
auto-grouped backup method 129, 220
automatic purge of messages, setting up 176


## B


backup 30
    aborting 229
    auto-grouped 230
    full 227

incremental 228
interrupted 229
scheduling 225
backup administration console 223
backup CLI commands 225
backup directory structure 221
backup method, auto-grouped 221
backup method, standard 220
backup options 231
backup process, overview 22
backup ZCS 219
backup, CLI commands 285
backup, skip backup of blobs 231
backup, skip HSM blob backup 232
backup, standard method, auto-grouped method 129, 220
backup,skip backup of searh index 231
backups cron job 342
backups, auto-grouped throttling 224
batch provisioning new accounts 143
blocking attachments 107
bounced delivery report 202
Briefcase feature 170
Briefcase, company name 122


## C


calendar preferences 168
calendar resource provisioning, zmprov 273
calendar sync, zmcalchk 167
calendar, enabling personal appointments only 166
calendar, filtering appointments 167
calendar, nested 166
calender, features 165
certificate, users 116
change administrator password 74
change password page, configure 145
changing account status 146
changing password 145
checking for latest ZCS software updates 216
Clam AntiVirus software 53
clamd.log 207
class of service 143
about 40, 143
class of service object 40
class of service, COS 75
clean up amavisd/tmp cron job 343
clean up the quarantine dir cron job 342
CLI auto-grouped backup 230
CLI command to move mailbox,zmmailboxmove 134
CLI commands,provisioning 269
CLI commands,start/stop service 300
CLI for account management
zmmailbox 134
zmmboxsearch 134
zmprov 134
CLI utilities 263
closed status 147
company directory 42
company name, changing in Briefcase external share prompt 122
component thread number 211
components, Zimbra 17
config provisioning, zmprov 276
configuration, typical example 24
configure external LDAP Lookup for s/mime 116
contact 13
contact lists 165
core functionality 16
COS account types, setting 124
COS provisioning, zmprov 275
COS, list all 281
COS, password restriction 145
COS, search 80
creating accounts 143
crontab jobs 341
crontab store jobs 342
crontab, how to read 341
crontab.logger cron jobs 343
crontab.mta jobs 343
cross mailbox search 134
cross mailbox search, CLI 304
cross malbox search 254
custom authentication 38
customize external share prompt 122


## D


daily reports 202
data store 21, 29
about 29
file location 23
deleting accounts 147
dictionary, adding words to ignore in 130
directory structure 22
disable 180
disaster recovery
basic steps 238
overview 238
restoring offline 239
restoring to new server 240
discovery, how it works 247
disk full alerts 203
disk layout 28
disk space monitoring 203
distribution list provisioning, zmprov 276

distribution list used for sharing 151
distribution list, create with zmprov CLI 280
distribution list, manage 150
distribution list, maximum members 149
distribution list, sharing items 171
distribution lists object 41
distribution lists, managing 149
documentation 12
Documents, features 170
domain admin console view 97
domain admin link to admin console 97
domain provisioning, zmprov 274
domain rename process 125
domain renaming 124
domain status 118
domain status, shutdown 119
domain, account limits 124
domain, after domain is renamed 124
domain, create with zmprov CLI 280
domain, set default with zmprov CLI 281
domain, SSL certificates 125
domains
  authentication modes 121
  virtual hosts 121
domains object 41
domains, global address list mode 119
domains, managing 117
dumpster 177
dumpster lifetime 177
dumpster, delete manually 177
dumpster, enable 177

## E

edge MTA 50
email messaging, features 156
email validation settings 112
equipment resources 152
error report, daily 202
exclude items in mailbox move 148
export preferences on ZWC 164
external AD account authentication 36
external LDAP account authentication 36

## F

failed logging policy, setting 174
features, core 16
features, web client 17
filtering, calendar items 167
find backup 229
forwarding address, hidden 158
free/busy interoperability 110
free/busy, zmprov 274
full backup 227

## G

GAL 42
  LDAP search filter used 43
  search options 42
  search parameter settings 44
GAL access for COS 162
GAL attributes 43
GAL mode 119
GAL sync account 120
generateDomainPreAuth, zmprov 279
global configuration 105
global configuration object 41
global settings 76
  anti-spam 109
  anti-virus 110
  HSM 113
  license 114
  MTA 107
  POP and IMAP 109
group calendar, enabling 166

## H

ham mailbox 54
handler exceptions in mailbox log 211
hidden forwarding address 158
high availability support 15
horizontal scalability 15
HSM
  scheduling 128
HSM, CLI 313
HSM, global setting 113
HTTP proxy 63
http proxy 63
http proxy, setting up 64

## I

IMAP access 162
IMAP global settings 109
IMAP proxy, setting up 61
IMAP, class of service 144
import preferences on ZWC 164
importing account data 137
incoming mail routing 28
incremental backup 228
index messages 20
index store 21, 29
  file location 23
index volume 128
index/search

back-end technologies used 29
indexing 30
install certificate, CLI 305
install SSL certificates on domain 125
internal account authentication 36
internal authentication mechanism 36
interop 110

## K

Kerberos proxy set up 67
keyboard shortcuts, enable 161

## L

LDAP
directory traffic 34
hierarchy 34
implementation 34
overview 33
schema include files for Zimbra 35
LDAP schema 35
LDAP server, restoring 237
legal discovery 71
legal intercept 69
license ID 114
license information 114
license policy for replacing logo 259
license, number of accounts used 114
license, renew within 114
license, updating 114
linking to admin console log in page 97
local configuration, CLI 308
localconfig list of properties 308
location resources 152
lockout status 147
log files 31
log files, description of 206
log pruning cron job 342
log, how to read mailbox.log records 211
log4j pre-defined zimbra categories 208
log4j, used to configure logging 208
logger 200
logger_myslow.log 207
logging levels 208
logging on to admin console 73
Lucene 29

## M

mail filters 161
mail filters, working with spam check 161
mail identities 159
mail notification 159
mail report, change 202
mail reports 202
mailbox full notification 172
mailbox log examples 212
mailbox log records 210
mailbox log, how to read 211
mailbox management tool 134
mailbox move, CLI 301
mailbox quota, enforcing 147
mailbox quotas
specifying 172
mailbox quotas, monitoring 205
mailbox search 134
mailbox server
overview 27
mailbox snapshot for legal discovery 71
mailbox, move 134
mailbox, reindexing 146
mailbox, view from admin console 146
mailbox, zmprov 277
mailbox.log 207
mailboxes, cross mailbox search 254
main.cf file 50
management tasks 76
management tasks from CLI 77
managing resource accounts 154
managing resources 152
mandatory 180
mandatory signatures 130
mandatory zimlets 180
master.cf file 50
maximum number in distribution lists 149
message delivery, quota options 52
message header information 215
message lifetime 176
message of the day for administrators 78, 79
message search 134
message store 20, 21, 28
file location 24
single-copy 28
message store,MIME format 21
message volume 128, 201
messages received and sent report 202
messages, purging 176
migrating account data 135
migrating accounts directly 137
migrating using xml file 139
modes, set with zmtlsctl CLI 312
modify base colors 260
modify ZWC theme, attributes 260
modify ZWC theme, graphics to replace 259
Monitor for multiple mysqld tp prevent corruption cron job 342
monitoring quotas 205

monitoring server status 201
monitoring tool 200
move mailbox 134, 301
MTA functionality 51
MTA package, Zimbra 20
MTA queues 57
MTA settings, how to configure 107
MySQL 21
MySQL, database check 216

## N

nested calendars 166
ngnix 59
Notification preference 171

## O

offline restore 235
offline restore CLI 225
offline restore, CLI 297
open source components 17
out of office reply 158
over quota delivery options 52

## P

password policy, setting 172
password restriction 145
password, admin change 280
password, change password page 145
password, changing admin 74
password, failed login policy 174
performance charts 319
performance statistics 201
persona 159
polling interval for GAL sync 120
POP 109
POP proxy, setting up 61
POP3, external access 160
ports, proxy 61
Postfix 50
Postfix configuration files 50
postfix error report 202
process logs cron job 343
product overview 15
protocol, set with CLI 312
provisioning multiple accounts 135
provisioning multiple accounts at once 135
provisioning, CLI commands 269
proxy architecture 59
proxy components 59
proxy ports 61
proxy, http 63
proxy, Kerberos 67
proxy,http 63
public service host name 118
public service host name, setting up 119
publishing shares 151
punctuation symbole, setting 173
purge messages 176
purge, setting up 176

## Q

query backup, CLI 293
queue logging cron job 343
queues 57
quota out of sync 277
quota, address book 172
quota, setting up notification 172
quotas and message delivery 52
quotas, delivery options 52
quotas, monitoring 205
quotas, setting 172

## R

recalculate mailbox count command 277
recipient object 41
recipients, most active report 202
recover deleted items 177
redo log 31
reindexing a mailbox 146
relay host settings 51
rename a domain 124
renew license 114
replace ZWC logo 258
report on any database inconsistencies cron job 342
report, daily mail 202
report, database inconsistencies 342
reports, MySQL 216
resource accounts, managing 154
resource calendar, sharing 154
resource conflict rules 153
resources, maintaining calendars 153
resources, managing 152
resources, scheduling policy 153
REST URL 118
restore backup, CLI 295
restore CLI commands 225
restore live system 236
restore mailbox and exclude delete operation 235
restore process 233
restore, selection items to exclude 237
restoring an account 233
restoring LDAP server 237

restoring to new server 240

## S

S/MIME 116
s/mime 116
s/mime, configure external LDAP 116
s/mime, enable 116
schedule backups, CLI 290
scheduling backups 225
scheduling policy for resources 153
schema, LDAP 35
screen resolution, standard web client 155
search 80
search across mailboxes 134, 247
search for accounts by COS 80
searchGAL, zmprov 278
senders, most active report 202
sending to distribution lists, manage 150
server
  admin extensions 130
  managing zimlets 129
  volume settings 128
server mode, changing 312
server pool by COS 144
server provisioning, zmprov 275
server settings
  services 127
server statistics 201
  message count 201
  message volume 201
server statistics, enable on admin console 200
server status 201
server, Zimbra
  managing 126
service,start/stop 300
session idle lifetime 176
session time out policy, 175
sessions, expire 176
setting up legal intercept 70
shared items, managing 171
shares tab, distribution list 171
sharing, notifying distribuion list 151
signatures, maximum length 159
signatures, system-wide 130
single sign-on using SPNEGO 331
single-copy message storage 28
single-copy store 28
skins 178, 257
smart host 51
SMS, enable 171
SMTP authentication 51
SMTP restrictions 51
SNMP monitoring 216
SNMP package, Zimbra 21
SNMP traps, error 216
software version checking 216
spam bayes auto-expiry cron job 343
spam mailbox 54
spam message lifetime 176
spam training cleanup cron job 343
spam training cron tab 343
spam training filter 53
spam training, CLI 322
spam white list, for mail filters 161
spam, turning on/off training attributes 54
spamtrain .log 207
spell, adding words to ignore 130
SPNEGO single sign-on 331
stack traces in mailbox log 211
standard web client, setting as default 155
standard ZWC 155
start service 300
statistics 76
  anti-spam 201
status 76
status logging cron job 342
status, domain 118
stop restore 235
stop service 300
store package 20
support 13
sync.log 207
syncGAL, zmprov 279
system architecture 18
system architecture graphic 19
system-wide signatures 130

## T

Table maintenance cron job 342
tasks feature 169
tasks from admin console 77
theme colors 257
themes 178
themes, setting account options 179
third-party software bundled with 17
throttling auto-grouped backup 224
timezone, enabling for Calendar 167
training filter for spam 53
transaction log 31
trash, recover from 177
trashed message lifetime 176

## U

unread message count out of sync 277
updating a license 114

updating anti-virus software 53, 110
upgrading zimlets 197
user auth token lifetime, expire 176
user warning message, navigation from ZCS 180

## V

vacation message 158
view mailbox from admin console 146
view quota 172
viewing members of distribution lists, manage 150
virtual host 121
volume settings 128
volumes, managing with CLI 323

## W

Web client features 17

## X

x-envelope headers 246
xml files for provisioning and migration 139

## Z

Zimbra applications 156
zimbra cron jobs 341
Zimbra logger 200
Zimbra mobile 179
Zimbra monitor host 200
Zimbra MTA 49
Zimbra objects
    ldap 39
Zimbra Schema 35
Zimbra web client, import/export account data 164
zimbraMailReferMode, use with proxy 66
zimbraProxyAllowedDomains, zimlets 191
zimlet gallery 189
zimlet, enable 180
Zimlets, configuring for accounts 179
zimlets, disabling 194
zimlets, listing all 325
zimlets, managing 129
zimlets, remove 196
zimlets, upgrading 197
zmbackup 285, 295
zmconfigd 20
zmdbintegrityreport 342
zmdbintegrityreport disable 342
zmmboxmove CLI, 7.1.3 or later 147
zmprov CLI 269
zmstat-chart 319
zmtrainsa CLI command for spam training 53
zmtrainsa spam training tool 54
ZWC versions 155