SGI Internet Server for Messaging Guide

Document Number 007-3878-001

CONTRIBUTORS Written by Kevin Slywka, Messaging Direct, Ltd. Updated by Bob Bernard Illustrated by Kevin Slywka Edited by Rick Thompson Production by Karen Jacobson Cover design by Sarah Bolles, Sarah Bolles Design, and Dany Galgani, SGI Technical Publications

COPYRIGHT

© 2000 Silicon Graphics, Inc. All rights reserved. The contents of this document may not be copied or duplicated in any manner, in whole or in part, without the prior written permission of Silicon Graphics, Inc.

MessagingDirect software is Copyright © MessagingDirect Limited, 1993-2000 Edmonton, Alberta, Canada. MessagingDirect software is a compilation of software of which MessagingDirect Limited is either the copyright holder or licensee. Acquisition and use of this software and related materials for any purpose requires a written license agreement from MessagingDirect Limited, or a written license from an organization licensed by MessagingDirect Limited to grant such a license.

LIMITED AND RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in the Rights in Data clause at FAR 52.227-14 and/or in similar or successor clauses in the FAR, or in the DOD, DOE or NASA FAR Supplements. Unpublished rights reserved under the Copyright Laws of the United States. Contractor/manufacturer is Silicon Graphics, Inc., 1600 Amphitheatre Pkwy., Mountain View, CA 94043-1351.

TRADEMARKS

SGI and the SGI logo are trademarks and IRIX is a registered trademark of Silicon Graphics, Inc.

Simeon, Execmail and MessagingDirect are trademarks of MessagingDirect Limited.

All products and services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations and MessagingDirect Limited disclaims any responsibility for specifying which marks are owned by which companies or organizations.

Portions of this software are Copyright © 1996-2000 Carnegie Mellon University. This product includes software developed by the University of California, Berkeley, and its contributors.

"M-Store" is Copyright © MessagingDirect Limited, Edmonton, Alberta, Canada 1993-2000.

Linux is a registered trademark of Linus Torvalds used by permission.

Record of Revision

Version	Description
001	June 2000 Initial Release

Figures	•									•	•	•		. xi
Tables														. xiii
Summary of Contents														. xv
Audience														. xvi
Typographical Conventions										•	•	•		. xvi
Installation														
Installation Planning														. 3
Capacity Planning														. 3
Server Performance Considerations														. 3
M-Store - Message Service														. 3
Sendmail Mail Transfer Agent (MTA)														. 4
M-Store - Server Component Requirements														. 4
Capacity Planning Summary														. 5
Hardware Requirements														. 5
Key Server Components														. 6
Network Requirements														. 7
Linux Platform System Parameters														. 7
Preparation for Installation Work Sheet	•									•	•	•		. 8
Administration														
Messaging System Overview														. 13
Introduction										•	•			. 13
	Figures	Figures . . . Tables . . . Summary of Contents . . Audience . . Audience . . Typographical Conventions . . Typographical Conventions . . Installation . . Installation Planning . . Capacity Planning . . Server Performance Considerations . . M-Store - Message Service . . Sendmail Mail Transfer Agent (MTA) . . M-Store - Server Component Requirements . . Capacity Planning Summary . . . Hardware Requirements . . . Key Server Components . . . Network Requirements . . . Inux Platform System Parameters . . . Preparation for Installation Work Sheet . . . Introduction . . .	Figures . . . Tables . . . Summary of Contents . . . Audience . . . Audience . . . Typographical Conventions . . . Installation . . . Installation Planning . . . Capacity Planning . . . Server Performance Considerations . . . M-Store - Message Service . . . Sendmail Mail Transfer Agent (MTA) . . . M-Store - Server Component Requirements . . . Capacity Planning Summary . . . Hardware Requirements Network Requirements Inux Platform System Parameters Preparation for Installation Work Sheet Introduct	Figures										

	Store Component Overview																•	. 14
	Servers																	. 15
	authproxyd Server																	. 15
	M-Store Command Line Interface																	. 15
	Database Organization																	. 16
	Mailbox Organization																	. 17
	Store Concepts																	. 18
	Partitions																	. 18
	Domains																	. 18
	Mailbox Hierarchy.																	. 19
	Quotas																	. 19
	Mailbox Access Control																	. 20
	User Accounts																	. 20
2	Managing the Store																	21
5.	Application Runtime Control	•	•	•	•	•	•	•	•	•	•	•	•	•	•	·	·	. 21
	Starting	•	•	•	•	•	•	·	·	•	•	•	•	•	·	·	·	. 21
	Starting	•	•	•	•	•	•	·	·	•	•	•	•	•	•	·	·	. 21
	Database Administration	•	•	•	•	•	•	·	·	•	•	•	•	•	•	·	·	. 21
	Validation	•	•	•	•	•	•	·	·	•	•	•	•	•	•	·	·	. 22
		•	•	•	•	•	•	·	·	•	•	•	•	•	•	·	·	. 22
	Backups	•	•	•	•	•	•	·	·	•	•	•	•	•	•	·	·	. 24
		•	•	·	•	•	•	·	·	•	•	•	•	·	•	•	•	. 20 20
	Recovery	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	. 20
4.	Tuning the Store	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	. 31
	Store Configuration	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	. 31
	Required Configuration	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	. 32
	Recommended Configuration .	•	•		•	•	•	•	•	•	•	•	•				•	. 34
	Optional Configuration	•	•		•	•	•		•			•	•				•	. 35
	authproxyd Configuration	•			•	•	•						•				•	. 37
	Store Manager		•									•					•	. 39
	Filesystem Parameters												•					. 40
	Inode counts												•					. 40
	Adding New Partitions		•									•			•		•	. 40

	Operating System Parameters	41
5.	Troubleshooting	43
	Correcting File Permissions	43
	Mailbox Cache Recovery	43
	Example	44
	Files	45
	Database Corruption	45
	Files	46
	Transaction Logs	46
PART III	Web Administration	
6.	Site Administration	49
	Accessing Site Administration	49
	Site Administration	51
	Domain Management	52
	Site Administrators	55
7.	Domain Administration	57
	Accessing Domain Administration	57
	Domain Administration	58
	User Accounts.	59
	Shared Mailbox Management	62
8.	Account Management	67
	User Passwords	67
	Change User Password Page	67
PART IV	Reference	
9.	File and Directory Layouts	71
	Configuration Files	71
	Runtime Control	72
	Executable Support Files	73

	Runtime Data Files			•	•			•		•				. 75
	M-Store Database Files							•						. 80
	M-Store Physical Mailbox Files .				•			•	•		•	•		. 81
10.	File Descriptions							•				•		. 83
	Message Store Configuration (ms.con	f) .						•					•	. 83
	Required Configuration													. 84
	Recommended Configuration .													. 86
	Optional Configuration	•						•	•			•		. 87
	authproxyd Configuration	•						•	•			•		. 90
	M-Store rc.m-store Script			•	•			•				•		. 92
	Synopsis			•	•			•				•		. 92
	Store Manager (stormgr)			•	•			•				•		. 93
	Synopsis			•	•			•				•		. 93
	Message Tables			•	•			•				•		. 95
	Shutdown file for imapd/pop3d. $% \left({{\left({{{{\bf{n}}_{{\rm{s}}}}} \right)}_{{\rm{s}}}}} \right)$.				•			•	•		•	•		. 95
11.	Server Commands				•			•			•	•		. 97
	Authentication Server (authproxyd) .			•	•			•		•				. 97
	Synopsis			•	•			•				•		. 97
	Configuration			•	•			•				•		. 99
	Authentication Mechanisms							•						101
	Account Migration	•						•	•			•		102
	M-Store Message Server (imapd)	•						•	•			•		103
	Synopsis	•						•	•			•		103
	IMAP4 Standard Extensions	•						•	•			•		105
	LMTP Delivery Server (lmtpd)	•						•	•			•		107
	Synopsis	•						•	•			•		107
	POP3 Message Service (pop3d)													110
	Synopsis				•			•	•		•	•		110
12.	Administration Commands													113
	Starting and Stopping M-Store			•		•				•				113
	Starting			•		•				•		•		113
	Stopping											•		114

007-3878-001

	IM-Store Administration Command Interpreter (msadm_tclsl	h).							.114
	Synopsis			•				•	.114
	Generic Commands			•		•		•	.115
	Site Administration Commands.			•		•			.115
	Domain Management Commands			•		•			.116
	Account Management Commands			•		•			.117
	Bulk Administration Tools			•		•		•	.125
	Add Users in Bulk to M-Store (msadm_bulkadd)								.125
	Delete Multiple Domains and Users (msadm_bulkdel) .								.128
	Database Management Utilities								.129
	Database Archive Tool (msdb_archive)						•		.129
	Database Backup Tool (msdb_backup)						•		.131
	Database Checkpoint Tool (msdb_checkpoint)						•		.134
	Database Recovery Tool (msdb_recover)						•		.136
	Database Restore-From-Backup Tool (msdb_restore) .						•		.138
	Database Test Tool (msdb_test)						•		.140
	M-Store Mailbox Cache Files Reconstruction (reconstruct) .						•		.141
	M-Store Database Creation (msdb_upgrade)		•	•		•	•		.143
13.	Mail Delivery to M-Store Mailbox Tool (deliver)								.145
	deliver Synopsis								.145
	Examples								.146
	Index								.149

Figures

Figure 2-1	M-Store Mail Component Overview
Figure 2-2	M-Store Component Architecture
Figure 6-1	Web Administration Tools Welcome Page
Figure 6-2	Site Administration Login Page
Figure 6-3	Sort Order Icon (Domain Management)
Figure 6-4	Add Domain Dialog
Figure 6-5	Modify Domain Dialog
Figure 7-1	M-Store Web Administration Tools Welcome Page
Figure 7-2	Add New User Dialog
Figure 7-3	Modify User Dialog
Figure 7-4	Shared Mailbox Management Page
Figure 7-5	New Shared Mailbox Dialog
Figure 7-6	Add Rights Dialog
Figure 7-7	Modify Shared Mailbox Dialog
Figure 7-8	Modify Rights Dialog
Figure 8-1	Change User Password Pagefc

Tables

Table i	Typographical Conventions
Table 1-1	Messaging Usage for Minimum Hardware Requirements 6
Table 1-2	Hard Drive Space Requirements by OS Platform 7
Table 1-3	Important File Locations
Table 1-4	List of Installation Settings
Table 3-1	msdb_test Options
Table 3-2	Default Directory Structure of a Backup
Table 3-3	msdb_recover Options
Table 4-1	ms.conf Required Options
Table 4-2	SASL Plugin Options
Table 4-3	SASL Plugin Examples
Table 4-4	Recommended M-Store Configuration Options
Table 4-5	Optional ms.conf Entries
Table 4-6	authproxyd Options
Table 4-7	storemgr Options
Table 5-1	reconstruct Options
Table 5-2	reconstruct Examples
Table 6-1	Administration Permission Levels
Table 9-1	/etc/md/store/ Configuration Files
Table 9-2	Locations of the Installed Bootscript
Table 9-3	/usr/local/md/ Executable Support Files
Table 9-4	/var/md/store/ Runtime Data Files
Table 9-5	M-Store Database Files
Table 9-6	M-Store Binary Mailbox Files
Table 10-1	ms.conf Required Options
Table 10-2	SASL Plugin Options
Table 10-3	SASL Plugin Option Examples

Table 10-4	Recommended M-Store Configuration Options
Table 10-5	Optional ms.conf Entries
Table 10-6	authproxyd Options
Table 10-7	rc.m-store Parameters
Table 10-8	storemgr Options
Table 10-9	M-Store Message Tables
Table 11-1	authproxyd Options
Table 11-2	authproxyd Configuration Options
Table 11-3	authproxy-authmech Configuration Variables 101
Table 11-4	imapd Options
Table 11-5	lmtpd Options
Table 11-6	pop3 Options
Table 12-1	msadm_tclsh Options
Table 12-2	msadm_tclsh Generic Commands
Table 12-3	<pre>msadm_tclsh Site Administration Commands 115</pre>
Table 12-4	msadm_tclsh Domain Management Commands 116
Table 12-5	msadm_tclsh Account Management Commands
Table 12-6	<pre>msadm_tclsh Account Mapping (alias) Commands 120</pre>
Table 12-7	User Mailbox Management Commands
Table 12-8	User Mailbox Management Commands
Table 12-9	msadm_bulkadd Options
Table 12-10	msadm_bulkdel Options
Table 12-11	msdb_archive Options
Table 12-12	Default Directory Structure of a Backup
Table 12-13	msdb_checkpoint Options
Table 12-14	msdb_recover Options
Table 12-15	msdb_test Options
Table 12-16	reconstruct Options
Table 12-17	reconstruct Examples
Table 12-18	msdb_upgrade Options
Table 13-1	deliver Options (required)

007-3878-001

About This Guide

This guide is a comprehensive overview and administration reference for administrators of M-Store, the messaging software product from MessagingDirect, Ltd., running on the SGI 1200 Internet server.

Summary of Contents

This guide is comprised of four tabbed parts:

1. Installation

Provides installation procedures for M-Store, including initial installations and upgrade installations.

2. Administration

Provides general M-Store administration information and procedures.

3. Web Administration

Provides general M-Store Internet administration information and procedures.

4. Reference

Provides information on all utilities, tools, and files found in M-Store.

This document does not provide for the integration of M-Store with other MessagingDirect products, third-party products or specific specialized environments.

Note: This guide refers to the following RFCs: 882, 1734, 1939, 2060, 2086, 2087, 2088, 2342, and 2359. See http://www.ietf.org/rfc.html for these RFC documents.

Audience

This guide is written for experienced system administrators who administer M-Store or delegate its administration duties to others.

Typographical Conventions

The following typographical conventions are used in this guide:

Table i	Typographical Conventions
Bold	emphasis, GUI field names
Italics	command variable or directory variable
Courier	commands, command arguments, sample code, file names, directory paths, program names, screen text
Courier Bold	a user input entered from the keyboard
[]	command option (except where noted)

For clarity, administration tools and utilities are presented in a consistent format as follows:

- Tool or utility title
- Syntax synopsis and/or written synopsis
- Explanation / additional notes
- Options (if any)
- Example (if any)
- Files (if any)
- See also (if any)

PART ONE

Installation

Chapter 1, "Installation Planning"

Chapter 1

Installation Planning

Capacity Planning

The following section is meant to aid in the research, design, and implementation of the messaging system.

Server Performance Considerations

The size of the server(s) is dependent on the user populations assigned to them. There are no absolute rules to apply here. The best approach is to apply some general guidelines in calculating the expected load on the server. It is recommended that one errs on the side of caution by estimating one's load, plus a healthy percentage above that. Use of the facility beyond its capabilities will result in degraded performance. It will never result in denial of service, except at the explicit request of the System Administrator. If the host facility is running, there is nothing in the M-Store software that would result in the denial of service without notification. It is up to each site to determine what level of performance is acceptable and scale their facilities appropriately.

The following is a guideline for scaling the server facilities. The values presented in the guidelines are averages for an M-Store infrastructure that is less than two years old. An increase in the average amount of resources can be expected over time as users send greater volumes of mail, message complexity increases, and new users are added.

M-Store - Message Service

The resources consumed by the Message Service (MS) are dependent on both the active and the total number of users. Typically, active users are approximately 5% of the total user base, and active users are defined as the number of users continually accessing their mailstore. Active users impact virtual memory and CPU usage. The total number of

users impacts overall disk space usage. Typically, a single user will consume the following resources:

Memory: 1 Mbyte per active user

Disk Space: 5 Mbytes per user

The suggested layout is:

- Database on a separate disk from the mail partitions
- 256 Mbytes minimum to avoid system paging
- Current CPU class Pentium

Mailstore performance is most greatly effected by I/O, not the CPU. The only major effect on the CPU is the concurrent number of users creating I/O such as checking, retrieving and sending mail. Additionally, the CPU is taxed in such a case by worker threads. Generally speaking, 10,000 users/CPU will be adequate for maximum performance.

Sendmail Mail Transfer Agent (MTA)

The M-Store mail transfer agent (MTA) is an enhanced version of the public Sendmail 8.9.3 release. It has been tailored for sites running the IMAP4/POP3 enabled M-Store. The amount of resources required depends on the average number of mail messages being delivered and the peak load level, in other words, enough memory and spool disk space to handle average loads and peaks in message traffic. The average site needs an additional 20 Mbytes of memory for the MTA and 500 Mbytes of disk space for the MTA spool/queue. 500 Mbytes gives enough room for peak loads and to handle any large queues because of outages.

M-Store - Server Component Requirements

A mail server that contains the Sendmail MTA, M-Store and an MSS (Multiprotocol Switching Service) component, with 400 permanent users of which 150 are active at any given time, would resemble the following configuration:

Memory:256 Mbytes Physical, 512 Mbytes SwapDisk Space:3 GbytesCPU:Recent 32-bit class CPU

007-3878-001

This configuration can adequately handle peak loads and also includes room for future growth.

Capacity Planning Summary

- One file per message (similar to traditional usenet news storage)
- IMAP Mail data kept on a server has a potential to grow, and is constantly changing (unlike POP-based Mail Servers)
- Numerous relatively inactive concurrent¹ processes
- Mission critical data backup and protection

Hardware Requirements

This section is an overview of the minimum hardware requirements for the efficient operation of M-Store.

- A server dedicated to Mail or Directory services.
- Numerous small disks with data striped across disks utilizing RAID level 5 striping and failed disk recovery.
- Multiple SCSI controllers to spread I/O across channels.
- Multiple CPUs typically perform better than a single more powerful CPU, especially if the load of multiple concurrent processes is being run in parallel across the multiple CPUs. M-Store runs with many independent processes, which is ideal for multiple CPUs setups. (Note that this is dependent on the OS being used.)
- Large mail spool area for mail data (that is, 5 10 Mbytes per user).
- Multiple swap partitions on separate disks.
- *Real memory* large enough to hold all active processes² in memory.
- Network throughput to support average mail usage. For example, to support 100,000 users delivering an average of 25 messages (each 10 Kbytes) per 8 hour day,

¹ Concurrent processes are defined as processes that is running and can be swapped-out. For example, the IMAP process for a person's inbox when the person is not reading mail is typically the state of most processes on a IMAP mail server.

one would require an average network throughput of 6.78 Mbytes. The throughput figure was obtained using the following assumptions and formulae:

Table 1-1	Messaging Usage for Minimum Hardware Requirements						
Assumptions							
25 messages	25 messages sent or received offsite per user (msr) 100 000 (users)						
10 KB per m	essage sent or received (msize)	8 hours per day (hrs)					
3600 seconds per hour (shr)1024 KB per byte (Kbytes)							

- . .

Throughput = (users x msr x msize x bytes)/(Kbytes x hrs x shr) Throughput = $(100000 \times 25 \times 10 \times 8)/(1024 \times 8 \times 3600) = 6.7$ MBperSec

Key Server Components

The most important features of a server are:

- amount of physical memory
- amount of swap space
- amount of disk space
- I/O performance

8 bits per Byte (bytes)

When planning server capacity, one must take into account the total number of concurrent connections and the total amount of disk space required. The disk usage can

² Active processes are defined as processes that are currently in a processing state. For example, the IMAP process for a person's inbox while reading and processing mail or an IMSP process when a person is searching in an address book.

be controlled by setting the domain quota and the user quotas, which will limit the amount of space that users are allowed to use for their mail.

Table 1-2Hard Drive Space Requirements by OS Platform

Platform	/usr/local/md
IRIX 6.5	20 Mbytes
Red Hat Linux 6.0	13 Mbytes

You should allow for at least 100 Mbytes for the mailstore alone; 1 Gbyte is recommended depending on user numbers and the expected number of stored messages per user.

Table 1-3 Important File Locations			
File Path	Description		
/etc/md/store	Contains the configuration file and the sample boot script; requires 20 Kbytes.		
/var/md/store	Contains all data for the message store, and its size depends on the size of the site and the number of users and messages. 100 Mbytes is a typical minimum size.		

Network Requirements

M-Store requires only a network connection and a TCP stack.

Linux Platform System Parameters

The Linux platform requires a change to the system parameters. The default Linux OS configuration disables synchronous meta-data updates in the ext2fs filesystem. This is a serious design flaw that can make it impossible for fsck to recover filesystem data after a system crash. We strongly recommend that Linux sites add the sync option to all ext2fs entries in /etc/fstab. (Reboot the server for this change to take effect.)

Preparation for Installation Work Sheet

The following work sheet summarizes the various settings for the M-Store installation process. Except for the "example only" settings, the default values of all other settings are **strongly recommended**.

Data Type Description	Default Setting	Planned Setting
Install Directory	/usr/local/md	
Owner	sms (example only)	
Group	sms (example only)	
Base Path	/var/md/store	
Mailstore Partition (This should be on a separate partition from the other ore files.)	/var/md/store/ mailstore	
Number of Users	10000	
Directories in the first level (This is available to set during installation only if the number of users entered is 10000 or greater.)	20	
Directories in the second level (This is available to set during installation only if the number of users entered 10000 or greater.)	200	
Use Internal Authentication	ON	
CRAM-MD5	ON	
DIGEST	ON	
PLAIN	OFF	
KERBEROS_V4	OFF	
GSSAPI	ODD	
Disable Cleartext Login	OFF	
IMAP Port (Internet Standard)	143	

Table 1-4List of Installation Settings

Table 1-4	(continued)	List of Installation Settings		
Data Type Description		Default Setting Planned Setting		
POP Port (In	ternet Standard)		110	
httpd Port (Internet Standard) (This is available to set during installation only if it was selected as an install package.)		80		

PART TWO

Administration

Chapter 2, "Messaging System Overview"

Chapter 3, "Managing the Store"

Chapter 4, "Tuning the Store"

Chapter 5, "Troubleshooting"

Chapter 2

Messaging System Overview

Introduction

An electronic mail infrastructure consists of a number of different components that are chosen and combined in different ways depending on your organization's needs. This section provides an overview of the different components that comprise an M-Store-based electronic mail infrastructure, and describes the role of each within the entire system. Later sections aid in deciding how these components can best be deployed for your organization.

The figure below provides a conceptual look at the different types of mail components and how they interrelate.



Overview of Mail Components

Figure 2-1 M-Store Mail Component Overview

Store Component Overview

This section introduces the core components of M-Store. Please note the additional references for more detailed information.

More detailed information is available from the system prompt via the man command. (man pages are located in /usr/local/md/man/catn/filename) Or please refer to the table of contents or index in this document. Furthermore, all M-Store print manuals are located in /usr/local/md/doc/ in PostScript (.ps) and Adobe Acrobat format (.pdf).

The following diagram details the M-Store Component Architecture.



Figure 2-2 M-Store Component Architecture

Servers				
	Please see Chapter 11, "Server Commands" for further details on the usage of the following servers.			
imapd				
	M-Store is an IMAP4 revision 1 (RFC2060) compliant mailbox server. The SASL authentication mechanisms PLAIN and CRAM-MD5 are built in, and other available mechanisms can be made available by placing the appropriate plugin into the M-Store plugin directory.			
lmtpd				
	This daemon process provides a LMPT message injection interface to the MessagingDirect message store. It provides numerous benefits over deliver and is the preferred delivery interface between the MTA and the message store.			
pop3d				
	This daemon process is a front-end to the M-Store message store providing support for the pop3 protocol. An experimental implementation of the CAPA command is provided; please see "POP3 Message Service (pop3d)" on page 110.			
authproxyd Server				
	This daemon process provides authentication services to the M-Store imapd and pop3d servers. This server fulfills two roles: to isolate all code requiring superuser privileges into a single process, and to provide proxy authentication services to clients that do not understand SASL-based authentication.			
M-Store Command Line Interface				
	<pre>msadm_tclsh is a powerful and flexible command line interface that provides many tools needed for mailstore administration. It is built with the Tcl/Tk shell scripting language. See "IM-Store Administration Command Interpreter (msadm_tclsh)" in Chapter 12 for</pre>			

more information.

Database Organization

The following is the M-Store database layout:

/var/md/store/	database/	db_lock.share	Shared memory segments.
		db_mpool.share	
		db_txn.share	
		/data	
			acl.db
			administrators.db
			authmap.db
			domain.db
			identifiers.db
			mailboxaccess.db
			mailboxbyid.db
			mailboxbyname.db
			quota.db
			sec.deb
			subscription.db
			userbyid.db
			userbyname.db
		/transaction_log	
			db_log.share
			log.0000000001

007-3878-001

Mailbox Organization

The M-Store mailbox directory is laid out as follows (additional details can be found in Chapter 9, "File and Directory Layouts".).

/var/md/store/	mailstore/	XX/		Hexnamedhashdirectory. (min 5, max 500, default 5 directories at this level)
		YY/		Hexnamedhashdirectory. (min 5, max 500, default 20 directories at this level)
		ZZ/	fdb.cache	Pre-parsed envelope and body data for each message.
			fdb.header	General mailbox specific information.
			fdb.index	Mailbox and message information.
			fdb.seen	Tracks seen and recent flags on a per message per user basis
			1.	Stored messages. (RFC 822 compliant)
			2.	
	ipc/			The UNIX domain socket files for authproxyd and lmtpd communications.
	tmp/			The directory for store temporary when new messages are injected into the store.
	etc/	nologin/		Path of the imapd and pop3 shutdown file.

run/

Location of the lock files containing the process id of each running daemon process. These files ensure that only one instance of a daemon runs for any given message store. Multiple instances of an M-Store daemon must use different configuration files each with a different ms-path value.

Store Concepts

The following concepts provide a basis for understanding the proper administration of the message store.

Partitions

Partitions, or mailstores, are directories on a hard disk that contain mailboxes and stored mail messages. Upon creation, mailboxes are assigned a specific partition according to rules defined in the configuration file.

Domains

M-Store fully supports the use of multiple domains in the message store. Domains are used to group sets of users in a logical or logistic manner. For example, a web hosting company hosts separate companies Foo and Bar, using the domains foo.com and bar.com to separate email addresses belonging to the companies. Or a company may wish to distinguish between offices in different cities and would then use the sub-domains city1.company.com and city2.company.com to partition the employee email addresses. Domains can be administered through the web-based administration interface or through msadm_tclsh (See "IM-Store Administration Command Interpreter (msadm_tclsh)" in Chapter 12.).

007-3878-001

Mailbox Hierarchy

The mailbox hierarchy refers to the collection of visible folders for a particular user. For example, Joe's mailbox hierarchy may include:

- Inbox (Joe's incoming mail folder)
- drafts
- sentmail/1999
- sentmail/2000
- Important (Joe's personal folders)
- Other Users/jane/memo
- Shared Folders/admin
- Shared Folders/staff (Folders within the domain that are shared between all users.)

To create a new mailbox called foobar the client just needs to send:

0 create foobar

Note: This command is only for IMAP.

This has improved the administration interface because users can now see the mailbox hierarchy in which they are working.

Quotas

Quotas are used to restrict the size of mailboxes and effect all sub-mailboxes. The mailbox that has a quota directly applied to it is called a 'quotaroot'. For example, we apply a quota of 2000 Kbytes to the quota root user/joe. Now user/joe and all of his sub-mailboxes can contain at most 2 Mbytes of mail. After filling the quota, no more mail can be delivered into the quotaroot or its sub-mailboxes. Quotas can also be applied to domains to restrict disk usage.

Mailbox Access Control

Mailbox access control refers to a set of controls used to restrict the types of access to the mailbox of individual users. The controls include, but are not restricted to, read, write, create, delete, and administration rights. These rights are assigned on a per user basis. A user may be assigned positive or negative rights to a particular mailbox to allow or disallow a particular type of access. M-Store uses access control lists or ACLs to restrict access to mailboxes. ACLs may be modified through the IMAP protocol (RFC2086) or through the included Web-based administration interface (See Chapter 6, "Site Administration".)

User Accounts

M-Store separates the concepts of users, authentication identifiers (the string used to login), and mailboxes for architectural reasons. A mailbox and authentication identifier cannot exist without a user, but a user can exist without a mailbox or without an authentication identifier. Hence, to create a typical user, the following multiple steps are required:

- 1. Create a user in an existing domain.
- 2. Create a mailbox for the user.
- 3. Create an authentication account for the user.

Note that even though steps 2 and 3 are optional, all three steps are the typical procedure. Steps 1 and 2 are usually combined in the administration tools to create both a user and inbox for incoming mail. Step 3 allows the user to authenticate to the IMAP or POP server if M-Store will not be holding the authentication accounts. For example, this is used if your site uses an external authentication mechanism like kerberos4 or the /etc/passwd file.
Chapter 3

Managing the Store

Application Runtime Control

Log in as the superuser to start and stop M-Store. The command path varies slightly by platform. Refer to Chapter 12, "Administration Commands" for specific details regarding the location and usage of the rc.m-store script on specific platforms.

Starting

Example

To start M-Store: /etc/init.d/rc.m-store start

Stopping

Example

To stop M-Store: /etc/init.d/rc.m-store stop

007-3878-001

Database Administration

The following is an outline of the tools necessary to administer the M-Store database. This section is organized into specific duties and the files needed to perform these duties.

Validation

msdb_test quickly opens and closes the message store database, creating or recovering any files if necessary. Any errors are written to standard error. msdb_test must be invoked as the superuser or the runtime-user (that is, sms) as defined in the configuration file.

Certain deadlock conditions may cause msdb_test to hang while opening the databases. In such cases, terminate msdb_test with Ctrl-c and rerun msdb_test with the -r flag.

msdb_test exits 0 on success, and 1 if an error occurs

msdb_test will not run if any database files are missing. In such a case, a backup containing all database files must be restored.

Option	Description	
-f config	Specify the path of an alternative message store configuration file.	
-1	Test for deadlocks after opening the database.	
-r	Recover the databases before testing. This should be used if starting M-Store from a boot script to clean up the database in case it was not cleanly shut down. This flag is equivalent to executing msdb_recover and is only be given by the M-Store runtime user. Please see msdb_recover, "Database Recovery Tool (msdb_recover)" on page 136, for possible risks associated with this flag.	
- V	Verbosely display the state of the database upon exiting.	

Table 3-1msdbtestOptions

Example		
	msdb_test -v	
	Test the database and display a message regarding its state. If there are any problems with the database they will be echoed to standard error.	
	msdb_test -r	
	Verbosely test the database. This is performed at startup by the rc.m-store boot script to ensure the consistency of the database before starting imapd or any other M-Store applications. This command is equivalent to msdb_recover -v.	
	msdb_test -lv	
	Verbosely test the database and check for an	ny deadlocks.
Files		
	/etc/md/store/ms.conf	The default M-Store configuration file.
	<i>ms-path</i> /database/	Default database home, where <i>ms-path</i> is defined in the ms.conf file.
	<i>ms-path</i> defaults to /var/md/store.	
See Also		
	ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10	
	msdb_recover, "Database Recovery Tool (msdb_recover)" in Chapter 12	
	Chapter 9, "File and Directory Layouts"	

Backups

It is strongly recommended that backups be performed on a regular basis. While M-Store has the ability to recover its mailstore from a system fault, all pending transactions (new accounts, mailboxes, etc.) will be lost. The physical mail will not be directly affected by a database crash.

msdb_backup provides a sample shell script that may be used to create live backups of the M-Store database. msdb_restore may be used to restore this backup in the event of a catastrophic failure.

msdb_backup will make a backup of the current database tables and logs in a subdirectory of /var/md/store/backup named by date and time. The default directory structure of a backup is:

Path	File Name
/var/md/store/backup/MSDB_Backup_ <i>timestamp</i>	table.db
	log.log_number

Upon successful termination, the directory should be moved to backup media for archival purposes.

The msdb_backup script is only a sample backup script that can be used as a base for administrators to write their own customized backup scripts. A successful backup must include the following sequence of events:

- 1. Force a checkpoint with msdb_checkpoint (recommended for non-live backups; this will not affect live backups).
- 2. Backup all database table files.
- 3. Use msdb_archive to determine which log files need to be backed up.
- 4. Backup the required log files.

msdb_backup defines a number of paths in the PUBLIC DEPENDENCIES section of the script which may need to be changed to reflect any changes made from the default M-Store installation. The ms.conf file will contain any changed values.

	After copying the transaction log files, m in active transactions.	nsdb_backup deletes those that are not involved	
Example			
	msdb_backup		
Files			
	/etc/md/store/ms.conf	The default M-Store configuration file.	
	/var/md/store/backup	The default M-Store database backup directory.	
See Also			
	ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10		
	<pre>msdb_archive, "Database Archive Tool (msdb_archive)" in Chapter 12</pre>		
	<pre>msdb_checkpoint, "Database Checkpoint Tool (msdb_checkpoint)" in Chapter 12</pre>		
	msdb_restore, "Database Restore-From-Backup Tool (msdb_restore)" in Chapter 12		
	Chapter 9, "File and Directory Layouts"		

Restore

msdb_restore provides a sample shell script that can be used to restore backups of M-Store's database that were created with msdb backup.

msdb_restore takes a single argument *backup_path* which must refer to the directory containing the archived database tables and transaction logs.

msdb_restore is only a sample restore script that can be used as a base for administrators to write their own customized backup restore scripts. The minimum sequence of events for restores are:

- 1. Shutdown all M-Store database related applications. This may entail any or all of the following: an imapd/pop3d shutdown file, ensuring no administration tools are currently running, and stopping the rc.mdstore script.
- 2. Empty, or backup, the M-Store transaction_log and data directories.
- 3. Copy all archived data files (*.db) into the data directory. Copy all archived log files (log.*) into the transaction_log directory.
- 4. Enter **msdb_recover** -c to finish restoring the database.

Any existing database directories are renamed to:

dirname.asoftoday's date.

msdb_restore defines a number of paths in the PUBLIC DEPENDENCIES section of the script which may need to be changed to reflect any changes made from the default M-Store installation. The ms.conf file will contain any changed values.

Example

msdb_recover -v

Verbosely recover the database. This is performed at startup by the rc.m-store boot script to ensure the consistency of the database before starting imapd or any other M-Store applications. The command is equivalent to msdb_test -r.

	msdb_recover -c		
	Verbosely recover the database after a catastrophic fa the database. This is performed by msdb_restore as previously archived database.	ilure and subsequent restoration of the final step in restoring a	
Files			
	/etc/md/store/ms.conf	The default configuration file.	
	/var/md/store/database/data	The default database data directory.	
	/var/md/store/database/transaction_log	The default database log directory.	
See Also			
	ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10		
	msdb_archive, "Database Archive Tool (msdb_archive)" in Chapter 12		
	msdb_checkpoint, "Database Checkpoint Tool (msdb_checkpoint)" in Chapter 12		
	msdb_recover, "Database Recovery Tool (msdb_recover)" in Chapter 12		
	msdb_restore, "Database Restore-From-Backup Tool	(msdb_restore)" in Chapter 12	
	Chapter 9, "File and Directory Layouts"		

Recovery

msdb_recover must be executed after an unexpected application, database, or system failure to restore the database to a consistent state. All committed transactions are guaranteed to appear after msdb_recover has run, and all uncommitted transactions will be completely undone. msdb_recover must be invoked as the superuser or the runtime-user as defined in the configuration file.

In the case of catastrophic failure, an archival copy or snapshot of all database files must be restored along with all of the log files written since the database file snapshot was made. (If disk space is a problem, log files may be referenced by symbolic links). For further information on creating a database snapshot, see msdb_backup, "Database Backup Tool (msdb_backup)" in Chapter 12. For further information on performing a recovery, see msdb_restore, "Database Restore-From-Backup Tool (msdb_restore)" in Chapter 12.

msdb_recover exits 0 on success, and >0 if an error occurs.

If the failure was not catastrophic, the files present on the system at the time of failure are sufficient to perform recovery.

If log files are missing, msdb_recover will identify the missing log file(s) and exit on fail, in which case, the missing log files need to be restored and recovery performed again.

The msdb_recover utility attaches to one or more of the Berkeley DB shared memory regions. In order to avoid region corruption, it should always be given the chance to detach and exit gracefully. To cause msdb_recover to clean up after itself and exit, send it an interrupt signal (SIGINT).

If there are many existing transaction log files, msdb_recover may take a great deal of time to execute. This may give the appearance of being hung-up, even though it is continuing to function properly. This is common after doing bulk additions or deletions of users. msdb_archive may be used to list log files that may backed up and deleted.

Rarely, the transaction logs may become corrupted and cause all applications to hang at startup, and msdb_recover crashes due to a segfault. This is a database bug. The

	Table 3-3 msdb_recover Options		
	Option	Description	
	- C	Failure was catastrophic	2.
	-f config	Specify the path of an a	lternative message store configuration file.
	-v	Run in verbose mode.	
Example			
	msdb_recover	[-cv] [-f config]	
Files			
	/etc/md/sto	re/ms.conf	The default M-Store configuration file.
	<i>ms-path</i> /datab	ase	The default database home, where <i>ms-path</i> is defined in the ms.conf file.
	<i>ms-path</i> defaults to /var/md/store		
See Also			
	ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10		
	msdb_archive, "Database Archive Tool (msdb_archive)" in Chapter 12		
	msdb_backup,"Database Backup Tool (msdb_backup)" in Chapter 12		
	msdb_checkpoint, "Database Checkpoint Tool (msdb_checkpoint)" in Chapter 12		
	<pre>msdb_restore, "Database Restore-From-Backup Tool (msdb_restore)" in Chapter 12</pre>		
	msdb_test,"I	Database Test Tool (msdb	_test)" in Chapter 12
	Chapter 9, "File and Directory Layouts"		

work-around is to delete all transaction log files and run msdb_test. Never attempt to do so on a live system.

007-3878-001

Chapter 4

Tuning the Store

Store Configuration

ms.conf is used to configure the mailstore at invocation. The options that can be listed in the ms.conf file are organized into Required Configuration, Recommended Configuration, Option Configuration and authproxyd. Each line of the file has the form:

option value ...

where *option* is the name of the configuration option being set and *value* is the value the configuration option is being set to. Blank lines and lines beginning with "#" are ignored. Options take either a boolean, numerical, or (multiple) string argument.

Note: If an option is not present in the file, its default is assumed. Default values appear in square brackets at the head of the description text, that is, [<default>]. Some options have no default value; these are listed with <no default>. Options that default to an empty string are listed with <none>.

For boolean options, the values yes, on, t, and 1 (one) turn the option **on**, and the values no, off, f, and 0 (zero) turn the option **off**.

Required Configuration

The following options are required for the operation of M-Store (see NOTE in "Store Configuration" on page 31):

Option	Description
admin_domain [<no default="">]</no>	All users of the specified domain are assumed to have site administration privileges. This option is necessary to perform Web-based site administration.
cleartext-login-enable [on]	Enables the IMAP4 LOGIN command and the POP3 USER and PASS commands. At least one of cleartext-login-enable or sasl-enable- <mech> must be enabled for users to authenticate. By default, all SASL CRAM-MD5 and DIGEST-MD5 authentication mechanisms are also enabled.</mech>
default-domain name [<no default>]</no 	The default domain name if single-domain is enabled.
mailstore name path [<no default>]</no 	Declare path as a mailstore with the symbolic name name. There must be at least one mailstore declared.
<pre>ms-assignment-policy rule [glob] mailstore [<no default="">]</no></pre>	Determine the mailstore (with symbolic name mailstore) on which a newly created mailbox resides. There must be at least one assignment policy defined as each acts as a filter executed in order of appearance in the ms.conf file.

Table 4-1ms.conf Required Options

There are three available ms-assignment-policy rules:

user-rule	The mailbox resides on the mailstore for which the user matches the glob pattern. This rule takes both a glob pattern and a single mailstore name.
domain-rule	The mailbox resides on the mailstore for which the domain matches the glob pattern. This rule takes both a glob pattern and a single mailstore name.

```
bytes-free The mailbox resides on the mailstore with the most free
space. This rule does not require a glob pattern, but does
take a list of mailstore names. It is recommended to end
with a bytes-free rule or a glob rule with a glob pattern of
"*" to ensure a default mailstore exists for newly created
mailboxes.
```

Table 4-2SASL Plugin Options

Option	Description
sasl-enable-cram-md5 [on]	Enable the built-in SASL CRAM-MD5 authentication mechanism.
<pre>sasl-enable-digest-md5 [on]</pre>	Enable the built-in SASL DIGEST-MD5 authentication mechanism.
sasl-enable-plain [off]	Enable the built-in SASL PLAIN authentication mechanism.
sasl-enable- <mech> [off]</mech>	Enable the SASL <mech> authentication mechanism plugin. The <mech> plugin must also be installed in <i>executable_base_path</i>/lib/plugins/</mech></mech>

Example

Table 4-3	SASL Plugin Examples	3
Example Comm	hand	Description
sasl-enable	-kerberos_v4	Enable the SASL KERBEROS_V4 plugin.
sasl-enable	-gssapi on	Enable the SASL GSSAPI plugin.

Recommended Configuration

The following options are recommended for proper operation of M-Store (see NOTE in "Store Configuration" on page 31):

Option	Description
hash-level-1 [20]	The number of hash directories in the first level of the mailstore. The minimum value allowed is 5 and the maximum is 500. (See NOTE in hash-level-2 Description)
hash-level-2 [200]	The number of hash directories in the second level of the mailstore. The minimum value allowed is 5 and the maximum is 500. NOTE: Under each of the defined mailstores exist a number of first-level hash directories. Each of which contains a number of second level hash directories. Mailboxes physically reside under the second-level hash directories.
quotawarn [90]	The percentage of quota utilization above which the IMAP server generates warnings.
transaction-log-directory [transaction_log]	The directory path where the database log files are stored. If the argument is a relative path, the logs are stored in ms-path/database/ \ transaction_log_directory/. NOTE: Log files should be stored and backed up on a separate disk from the database tables. See msdb_backup, "Database Backup Tool (msdb_backup)" in Chapter 12, for more information.

 Table 4-4
 Recommended M-Store Configuration Options

007-3878-001

Optional Configuration

The following are optional for M-Store configuration file (see NOTE in "Store Configuration" on page 31):

Table 4-5Optional ms.conf Entries

Option	Description
admin-append-domain-auth [on]	When enabled, append the current domain to the identifier when creating authentication accounts with the administration tools. For example, creating an authentication account for user foo implicitly creates the account for foo@mydomain.bar instead.
allow-one-message-overquota [off]	Allow a user to receive one message that would put them over quota. Note that if a user is already over quota then no messages can be received.
allowanonymouslogin [off]	Permit logins by the user anonymous using any password (this feature is not supported by all authentication mechanisms).
auto-create-inbox [off]	If the authenticated user does not already have an IMAP INBOX, create one automatically when they authenticate.
auto-create-inbox-quota [0]	If auto-create-inbox is enabled, the newly created INBOX is assigned a quota root with the specified value (in bytes). If the value is less than or equal to zero, no quota root is assigned.
defaultacl [anyone lrs]	The default acl (access control list) for newly created mailboxes.
executable-base-path [/usr/local/md]	The base path for M-Store binaries and documentation.
imap-port [143]	Specify the port used by imapd.
license-file-path [/etc/md/store/license.dat]	Specify the absolute path of the license file license.dat.

Option	Description
lmtp-enable-overquota-delivery [off]	When enabled, Imtpd will also listen to the named socket <i>ms-path</i> /ipc/lmtpd-oq. All mail delivered through this socket is delivered regardless of a user's quota. The behavior of the default socket is unchanged.
lmtp-shared-name [shared]	Specify the local name used by lmtpd to denote shared folders during Plus-Addressing delivery.
max-overquota-kb [0]	If we have allow-one-message-overquota set [on], this option limits the size of a message that can be delivered over quota. If this is set to 0 or undefined, there is no limit.
messagestore-deliver-eat-nuls [off]	Enable the removal of NUL characters in messages. The default behavior is to reject such messages. Note that removing such characters may render parts of the message unreadable. NUL characters are illegal in messages according to RFC2060; this option is provided to allow sites to work around non-compliant (broken) mail clients.
messagestore-deliver-overquota -bounce [off]	If enabled, causes deliver and lmtpd to return a permanent delivery failure for any message delivery that would put the target mailbox over its quota limit. Normally these programs return a temporary failure, allowing the message transport agent (MTA) to requeue the delivery attempt. Enabling this option forces the MTA to immediately bounce the message.
ms-path [/var/md/store]	The base path of the message store data.
plaintextloginpause [0]	Number of seconds to pause after a successful plaintext login. For systems that support strong authentication, this permits users to perceive a cost in using plaintext passwords.
pop-port [110]	Specify the port used by pop3d.
popminpoll [0]	Set the minimum amount of time, in minutes, the server forces users to wait between successive POP3 logins.

Table 4-5 (continued)	Optional ms.conf Entries
-----------------------	--------------------------

007-3878-001

Option	Description
poptimeout [10]	Set the length of the POP3 server inactivity for the autologout timer, in minutes. The minimum value is 10 minutes.
runtime-user [sms]	The login name of the UNIX account under which the server runs.
timeout [30]	The length of the IMAP server inactivity for the autologout timer, in minutes. The minimum value is 30 minutes.
umask [077]	The default umask value used by the server programs.

Table 4-5 (continued)Optional ms.conf Entries

authproxyd Configuration

The following options are used by authproxyd, the M-Store authentication server (see NOTE in "Store Configuration" on page 31):

Table 4-6authproxyd Options

Option	Description
authproxy-authmech [authdb]	Specify the mechanism used to authenticate plaintext logins.
authproxy-legacy-authmech [<no default>]</no 	If authentication using authmech fails, authenticate using the legacy-authmech. If the latter succeeds, automatically build an account in the authmech authentication environment using the username and password information supplied in the authentication request. Future authentications with the same username and password will succeed with the original authmech.

	Option	Description
	authproxy-rimap-host [<no default>]</no 	The remote host to be contacted by the rimap authentication mechanism. The argument can be a hostname (imap.foo.bar) or a dotted-quad IP address (192.168.0.1). The latter is useful if the remote server is multi-homed and has network interfaces that are unreachable from the local IMAP server. The remote host is contacted on the imap service port. A nondefault port can be specified by appending a forward slash and the port name or number to the host argument.
	authproxy-pam-service [authproxyd]	The service name for PAM authentication. Setting this value to a predefined PAM service allows IMAP and POP users to authenticate with the same credentials used to authenticate via the defined service, i.e., login allows users who can physically log into the machine to be authenticated via authproxyd.
Files		
	/etc/md/store/ms.conf	The default location for the message store configuration file.
	/etc/md/store/ms.sample	The sample M-Store boot script.
See Also		
	authproxyd, "Authentication Server (authproxyd)" in Chapter 11	
	impad, "M-Store Message Server (imapd)" in Chapter 11	
	<pre>lmtpd, "LMTP Delivery Server (lmtpd)" in Chapter 11</pre>	
	pop3d, "POP3 Message Service (pop3d)" in Chapter 11	
	Chapter 9, "File and Directory Layouts"	

Table 4-6	(continued)	authproxyd Options

007-3878-001

Store Manager

Synopsis

storemgr [-f config_file]

storemgr is a daemon process that manages the collection of protocol, authentication and database management server processes that make up the message store. It is the primary control daemon for the store, managing starting, restarting and shutting down the entire message store. Running storemgr starts the store manager, which subsequently starts all of the other store processes. Once started, store processes are monitored and restarted in the event that one of them terminates outside of storemgr control.

storemgr must be run as the superuser and is normally invoked from the rc.m-store boot script. The rc.m-store should be used as the command line interface for performing control operations for the store, rather than using the signal-based control support provided by the store manager.

Table 4-7storemgr Options

Option	Description
-f config_file	Specify an alternate location for the M-Store configuration file.

SIGTERM stops the store. This causes all managed processes to be terminated.

SIGHUP restarts the store. This causes all managed server processes to be stopped and then re-started.

See Also

authproxyd, "Authentication Server (authproxyd)" in Chapter 11

imapd, "M-Store Message Server (imapd)" in Chapter 11

lmtpd, "LMTP Delivery Server (lmtpd)" in Chapter 11

ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10

msdb_checkpoint, "Database Checkpoint Tool (msdb_checkpoint)" in Chapter 12
msdb_test, "Database Test Tool (msdb_test)" in Chapter 12
pop3d, "POP3 Message Service (pop3d)" in Chapter 11
rc.m-store, "Message Store Configuration (ms.conf)" in Chapter 10
Chapter 9, "File and Directory Layouts"

Filesystem Parameters

Generally, filesystem parameters are system specific. However, M-Store is designed to run without any difficulty using the default system settings of any standard installation.

Inode counts

In deciding the number of inodes for a given partition, it is generally assumed that there should be eight (8) inodes per mailbox. Additionally, one (1) inode should be assumed for each message. With these assumptions, the administrator can determine an adequate level of inodes for optimum performance.

Adding New Partitions

When an existing partition is running low on free space or the need for additional partitions occurs, perform the following:

- Install a new hard disk drive and mount the new filesystem. See your system documentation for assistance in this area. Let's assume the file system is mounted at /d/d2.
- 2. Enter the following commands:

mkdir /d/d2/mailstore
chown sms:sms /d/d2/mailstore

3. vi /etc/md/store/ms.conf

Add the mailstore name/path and a rule so the new partition is used. For example: mailstore ms2 /d/d2/mailstore ms_assignment_policy bytes_free ms1 ms2

4. HUP the server to reread the ms.conf file as follows:
kill -1 'cat /var/md/store/run/imapd.lock'

Operating System Parameters

Only the Linux platform requires a change to the system parameters. The default Linux OS configuration disables synchronous meta-data updates in the ext2fs filesystem. This is a serious design flaw that can make it impossible for fsck to recover filesystem data after a system crash. We strongly recommend that Linux sites add the sync option to all ext2fs entries in /etc/fstab.

Reboot the server for this change to take effect.

Chapter 5

Troubleshooting

Correcting File Permissions

The store runs as the runtime user and needs to able to read and write to the mail partitions, databases, ms.conf, and *ms-path*. The signs of permission problems are i/o error messages, being unable to open databases and being unable to read the configuration file. Several common causes of permission problems are running reconstruct and msdb_* commands as root (superuser), creating new partitions and not doing the chown sms:sms step.

To repair permission problems do the following at the system command prompt:

chown -R sms:sms /var/md/store /d/d2/mailstore

Mailbox Cache Recovery

reconstruct rebuilds one or more IMAP message store mailbox cache files within a given domain. It can be used to recover from almost any sort of data corruption. Since reconstruct can create new cache files it should be run as the M-Store runtime user.

When reconstruct finds existing header and index files, it attempts to preserve any data in them that is not derivable from the message files themselves. The state that reconstruct attempts to preserve includes: the flag name, flag state, and internal date. reconstruct derives all other information from the message files.

The mailbox arguments must be fully qualified IMAP mailbox names and may need to be quoted on the command line if the name contains shell-specific characters.

Table 5-1 reconstruct Options	
Option	Description
-f config_file	Specify an alternate location for M-Store's configuration file.
-r	Recursively reconstruct all sub-mailboxes of the mailboxes or mailbox-prefixes given as arguments. If no mailbox arguments are given, all mailboxes within the specified domain will be reconstructed.
-u	Reconstruct a specific user's mailbox or mailboxes.
-v	Display program version information on standard error, then exit.

Example

This command recursively reconstructs all cache files for the personal hierarchy of user foobar@esys.ca

reconstruct -r esys.ca "user/foobar"

Table 5-2reconstruct Examples

Command Example	Description
reconstruct -r example.com	Reconstruct all mailboxes in the example.com domain.
reconstruct -r -u joe example.com	Reconstruct all of joe@example.com's mailboxes.
reconstruct -u joe example.com INBOX	Reconstruct only joe@example.com's mailbox.
reconstruct -r -u joe example.com pub	Reconstruct joe@example.com's pub folder and all sub-folders.

Table 5-2 (continued) reconstruct	Examples
reconstruct foo.com admin	Reconstruct the shared folder admin in the foo.com domain.
reconstruct -r example.com admin	Reconstruct the shared folder admin and all sub-folders in the example.com domain.

Files

/etc/md/store/ms.conf	The default M-Store configuration file.
mailboxpath/fdb.*	Mailbox cache files.

See Also

ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10

Chapter 9, "File and Directory Layouts"

Database Corruption

Database corruption is a very rare event, and may never happen. The possible causes are filesystem corruption, a system crash, and disk failure. To recover a database, run msdb_recover first. If that fails, run msdb_backup, delete the transaction logs and run msdb_recover. If the above fails, one must restore the last good backup.

Files		
	/etc/md/store/ms.conf	The default M-Store configuration file.
	ms-path/database	The default database home, where <i>ms-path</i> is defined in the ms.conf file.
	<i>ms-path</i> defaults to /var/md/store on all systems.	
See Also		
	ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10	
	<pre>msdb_test, "Database Test Tool (msdb_test)" in Chapter 12</pre>	
	Chapter 9, "File and Directory Layouts"	
Transaction Logs		
		1 1, 1 1 .1

Transaction logs are support files for the database and are used to help recover the databases on an error. The logs are part of the reason why database corruption is so rare. They can become corrupted, but is a truly rare occurrence. To avoid problems, the system administrator should run msdb_backup at least once a day. The most convenient method is to add a cron job to run msdb_backup at a specified daily time.

PART THREE

Web Administration

Chapter 6, "Site Administration" Chapter 7, "Domain Administration" Chapter 8, "Account Management"

Chapter 6

Site Administration

Accessing Site Administration

The Web Administration Interface is designed to provide a convenient means of administering M-Store remotely. The administrative functions include managing domains, users, and mailboxes. They are, in essence, a web-based implementation of the command line administration utility (msadm_tclsh).

To access the interface, use a standards-based Java Script enabled web browser and means of connecting to the M-Store domain. The administration tools URL is determined by the location where the httpd server was installed. To access the interface, simply provide a URL that points to this domain. For example:

httpd was installed on

www.yoursite.com

means the URL for the Administration Interface is https://www.yoursite.com/msadm/

To ensure a secure session, please use https://... in your URL. Failure to do so may result in an insecure session.

Once at the Administration site, the following is displayed:



Figure 6-1Web Administration Tools Welcome Page

Please choose the Site Administration link.

Each administration task has a predefined permission level. Only the Site Administrator has access to all other permission levels, while users can only change their own passwords.

 Table 6-1
 Administration Permission Levels

Administration Task	Permission Level
Site Administration	Site Administrator, Domain Administrator, User
Domain Administration	Domain Administrator, User
Change User Password	User

After logging in, it is not possible to leave the secure administration area without either logging out or causing the secure session to be terminated. The login **cookie** is deleted automatically on logout as a security measure against unauthorized access. When finished, please logout using the Logout link in the navigation area. Even though the login cookie is destroyed by default when the browser is closed, it may persist under certain unforeseen conditions such as an application crash. So it is strongly recommended that the Logout link be used every time to log out of a session.

The web administration defaults file, which specifies all the configuration options for all tools, is found in:

/usr/local/md/libdata/httpd/htdocs/msadm/config/defaults.php3

For convenience, a URL may be bookmarked to provide direct access to the required administration level. The following table provides the default URL to each administration level.

Default Administration URLs

https://yourhostname/msadm/site
https://yourhostname/msadm/domain
https://yourhostname/msadm/user/change password.php3

Site Administration

The Site Administration page allows an administrator to alter the Domain Management settings, and modify lower level administrators and their passwords. Navigation is performed via the navigation area on the left side of the page.

The following steps need to have taken place in order to use this tool. (If one of the included setup wizards was used, it is unlikely that this list of steps will be need to be reviewed. If installation was completed without a wizard then the following steps need to be completed with the msadm_tclsh command line interpreter):

- 1. An administrative domain was created.
- 2. The name of the administrative domain is specified in the ms.conf file.
- 3. The Site Administrator was added to the administrative domain. This is accomplished by adding a user, then adding that user as a site administrator.
- 4. An authentication account was added for the Site Administrator.



Figure 6-2 Site Administration Login Page

Enter your **Auth ID** (Site Administrator Username) and **Password** (Site Administrator Password). If authentication is successful, a secure session is established. Please use Logout when your session is complete (see Logout, "Accessing Site Administration").

Domain Management

This page is reached via the Domain Management link (located in the navigation area on the left side of the page) on the Site Administration page. Here, one can add, delete and change quotas for all the listed domains. A checklist of existing domains is provided including the Quota Usage (MB) and Quota Limit (MB). The number of Domains listed per page can be set in the defaults.php3 file.

Navigation between domain pages is accomplished with the navigation arrows in the upper right hand portion of the page. If one wishes to jump to a particular domain list page, one can enter the page number in the area between the navigation arrows and hit the Enter key (Figure 1).

Figure 1. Figure 2.



One can also filter the domain names listed by entering a search pattern in the **Apply Filter** field (Figure 2 above). The filter uses standard simple pattern matching. For example: ***c*** matches north.ca and messagingdirect.com, but not noseehere.net.

The sort order of the domains listed can be reversed by clicking on the Sort Order Icon next to the **Domain List** column.

Ć	i.	Domain List	Quota Usage (MB)	Quota Limit (MB)
	P	m1.net1.com	N/A	None
		m2.net2.com	N/A	None

Figure 6-3 Sort Order Icon (Domain Management)

Adding Domains

Click on the Add Domain button to view the Add Domain dialogue. Enable Domain is selected by default. The domain name is the name of the domain to be to added. For example: mail2.foo.com. If you wish to create, but not enable the domain at this time, deselect Enable Domain. If Allow Anonymous Login is selected, any user can log into the domain using anonymous as a login name. The Quota Size can also be set at this time. Until a quota is set, no mail can be received under normal conditions.

Domain Name	
🔽 Enable Domain	
🗖 Allow Anonymous Lo	gin
Quota Information	
Quota Size (in MB)	



Deleting Domains

To delete a domain, first select the target domain from the provided list by clicking in the checkbox next to the named domain. Then, click on the **Delete Domains** button. Click on **OK** to delete the selected domain. Note that this cannot be undone. All M-Store related data is deleted in the selected domain.

Changing Quotas

To modify a domain, click on the name of the domain in the domain selection table. A dialog is presented where the desired changes can be made. Click on **OK** when finished. The Domain Name must be a valid RFC822 domain name. If a quota limit exists, the current quota is shown. To remove an existing quota, delete all the text in the **Quota Size** (in **MB**) field and leave it blank.

Modify Domain - Mi	crosoft Internet Explorer 💶 🗙			
Basic Information				
Domain Name	m1.net.com			
🔽 Enable Domain				
🗖 Allow Anony	🗖 Allow Anonymous Login			
Quota Inform Quota Size (in M	B)			
ок	Cancel			

Figure 6-5 Modify Domain Dialog

Site Administrators

This page is reached by clicking on **Site Administrators** link in the navigation area. With this page administrators are added, deleted, or modified.

Adding Site Administrators

To add a Site Administrator, click on the **Add Administrator** button. A dialogue is displayed asking for the User Name of the new administrator. The user name must be a user in the administrative domain specified in the ms.conf file. Note that this process does not create an authentication account for the new user. Therefore, if an auth account does not exist, the user will not be able to log into Site Administration. A new authentication account must be created using **Domain Administration**.

- 1. Login into Site Administration using your Authentication ID and Password.
- Specify the Domain for which you wish to add an Administrator (new user) in the Navigation portion of the page. This actions takes you to the Domain Administration page.
- 3. Add a new Administrator (Add User).
- 4. Set the new user as an Administrator and choose their password.
- 5. Return to Site Administration using the Site Admin link in the Navigation area.

- 6. Click on the Site Administrators link.
- 7. Add User and provide the same user name as in Step 3.
- 8. The new Administrator will now appear in the Site Administrators list.

The new Administrator can now login as a Site Administrator. See Chapter 7, "Domain Administration" for further information.

Deleting Site Administrators

To delete an administrator, select the user name via the checkbox in the **Site Administrator List** table. Then click on the **Delete Administrator** button. A warning dialogue is presented; choose **OK** to accept the deletion. Choose **Cancel** to exit the dialogue. Deleting the administrator removes only the site administrative rights of the user; all other aspects of the user's account will continue to exist.
Chapter 7

Domain Administration

Accessing Domain Administration

The Web Administration Interface is designed to provide a convenient means of administering M-Store remotely. The administrative functions include managing domains, users, and mailboxes. They are, in essence, a web-based implementation of the command line administration utility (msadm_tclsh).

To access the interface, use a standards-based Java Script enabled Web browser and means of connecting to the M-Store domain. The administration tools URL is determined by the location where the httpd server was installed. To access the interface, simply provide an URL that points to this domain. For example:

httpd was installed on:

www.yoursite.com

means the URL for the Administration Interface is http://www.yoursite.com/msadm/

Once one is at the Administration site, the following displays:



Figure 7-1 M-Store Web Administration Tools Welcome Page

Select the Domain Administration link.

Please see Chapter 6, "Site Administration" for details regarding Administration Permission levels.

Domain Administration

A domain can be administered by both site administrators and domain administrators. The first domain administrator for a domain is added using msadm_tclsh or by logging into the domain as a site administrator and creating a user with administration rights.

	When presented with the login page, the Auth ID for domain administrators is their username. The target domain is selected from the drop-down list of domains at the bottom of the domain administration login page. The target domain is the domain they have been assigned to administer. If authentication is successful, a secure session is established.
	In contrast, for Site Administrators, if the target domain is different from the admin-domain specified in ms.conf, the Auth ID must be in the form of <i>username@target_domain</i> . The Domain Administration page is accessed by selecting the target domain from the Administer Domain drop-list, which is located in the navigation area of any Site Administration page.
	The main tools that are available on the Domain Administration page are User Accounts and Shared Mailbox Management .
User Accounts	
	Click on User Accounts to reach the User Accounts page. Use this page to add, delete and modify user accounts.
Add Users	
	Click on the Add New User button and fill out the resulting dialog. By default, Create Personal Folder Space, Create Internal Authentication Account, and Enable Internal Authentication Account are selected. The User Name must not contain the "@" character. If the Administrator option is selected, the new user is added as an administrator to the current domain. The new user now has access to the Domain Administration pages.

🛣 Add User - Netscape	_ <u> </u>
Basic Informat	ion
User Name	
Administrator	
Folder Informa	ntion
🔽 Create Person	ial Folder Space
Quota Size (in MB	
Authentication	Information
🗹 Create Interna	l Authentication Account
🗷 Enable Interna	l Authentication Account
Password	
Verify Password	
ок	Cancel

Figure 7-2 Add New User Dialog

The **Create Personal Folder Space** selection generates a namespace, including an INBOX, for the user allowing for the creation of additional folders that allow them to receive and organize mail. The **Quota Size** field is blank by default; a quota of 2 Mbytes is a typical setting. A default quota setting can be specified in the defaults.php3 file.

Enabling the **Create Internal Authentication Account** option creates an authentication ID of *username@domain_name* if the multi-domain mode was set during M-Store installation. If in single-domain mode, the authentication ID is *username* only. If **Create Internal Authentication Account** is checked, a password must be provided. If the **Enable Internal Authentication Account** is checked, the user can use the provided **Auth ID** and **Password** to authenticate themselves to the mailstore, otherwise they will be unable to login. Click on **OK** when finished.

Delete Users

To delete users, select the checkbox next to the users to be deleted. Click on the **Delete Users** button; a warning dialog then appears. Click on **OK** to delete the user(s), or click on **Cancel** to abort the deletion.

Change Quotas

Click on the user name in the **User List** of the user to be created, deleted, or modified. In the resulting dialog **Modify User** (see Figure 7-3), the **Folder Information** section has a field named **Quota Size (in MB)**. Here, enter the user's mail quota size in megabytes. For example, an entry of '2' means the quota is now set to 2 Mbytes. To change the quota simply highlight the current setting with the mouse pointer and enter the new setting. If you set the quota to zero or delete the current value (that is, leave the **Quota Size** field blank), you will prevent any more mail from being delivered to the user's mailbox:

Hodify User - Netsca	ape 📕
Basic Informa	tion
User Name	sms
Administrator	
Folder Inform	ation
A personal folder sp	pace has been created for this user.
Ouata Siza (in MB	
Quota Size (ili ivit	5)
Authentication	Information Authentication Account
Authentication Delete Interna F Internal Authe	al Authentication Account entication Account Enabled
Authentication Delete Interns Internal Authe Password	Information Authentication Account entication Account Enabled
Authentication Delete Interna I Delete Internal Authe Password Verify Password	a Information al Authentication Account entication Account Enabled
Authentication Delete Interns Internal Auther Password Verify Password 	Information Authentication Account Entication Account Enabled

Figure 7-3 Modify User Dialog

Click on **OK** when finished.

Change Passwords

Click on the user name in the **User List** for whom a password is to be created, deleted, or changed. In the resulting dialog, the section entitled **Authentication Information** allows one to delete an internal authentication account, and enable an internal authentication account as well as change the password. Please see the above section **Adding Users** ("Add Users" on page 59) for details on these settings. To change the password, enter the new password in both the **Password** and **Verify Password** fields. The old password, if one existed, is overwritten. Click on **OK** when finished.

Provide Domain Administrative Rights

By selecting the **Administrator** check-box, a user can be designated as an administrator for the given domain. The designated user can add, modify, or delete users, mailboxes, and perform other domain administration duties. However, they cannot perform site administration duties such as adding domains. Once a user has been added, the domain rights can be set or edited. Click on **OK** when finished or **Cancel** to return to the previous page.

Shared Mailbox Management

With the Shared Mailbox Management page, one can add, delete and modify mailboxes.

				Shared Ma	ilboxes
Domain Administration	Add Mailbox [Delete Mailboxes	Apply Fi	lter 🕄 🏹 🗍 1	of 1 🗅 💭
User Accounts	1	Shared Mailbox List	Quota Usage (MB)	Quota Limit (MB)	
Shared Mailboxes		hold	0	1	
Logout		(Use checkbox	es to tag mailboxes for d	leletion)	
<u>Logout</u>		(Use checkbox	es to tag mailboxes for d	leletion)	



Add Shared Mailboxes

To add a new mailbox, one must either have an existing user or first create a new user. Please see above, Domain Administration: Add Users ("Add Users" on page 59). To modify an existing mailbox, click on the target mailbox in the Mailbox List.

Add a new mailbox by clicking on the **Add Mailbox** button. If modifying an existing mailbox, click on the target mailbox in **Shared Mailbox** list. The **New Shared Mailbox** dialog is divided into **Basic Information**, **Mailbox Rights** and **Quota Information**. For **Basic Information: Shared Mailbox**, just enter the new mailbox name. The **Quota Size** is blank by default; a typical setting is 2 Mbytes. Click on **OK** to return to **Shared Mailboxes**.

Basic Information	
Change of D Callbarry	1
Shared Mailoox	
Mailbox Rights	
Add	4
Modify	
	*
Quota Information	1
Quota Size (in MB)	
ок	Cancel

Figure 7-5 New Shared Mailbox Dialog

Mailbox Hierarchy

If, for example, the shared mailbox public were added, we would need to provide the username of the shared mailbox administrator. Essentially, this is the owner of the mailbox who gives other users rights as they see fit. At this stage, we can also give other users their rights on the new mailbox, but it need not be done at this time. After a new mailbox has been created, any new sub-folder of that new mailbox inherits the rights of the parent mailbox. For example, if we were to add public/things, then the sub-folder

things would inherit all rights from public. However, if one chooses, the rights of the sub-folder things can be edited by first selecting the mailbox path from the picklist and then clicking on the **Add** or **Modify** button.

涨 Add Rights	: - Netscape	<u>_ ×</u>
User Name	sms	
	 C Read C Read/Write C Administrator 	
ок		Cancel

Figure 7-6 Add Rights Dialog

In the Add Rights dialog, enter the username *username* and select the rights level from one of **Read**, **Read**/Write, and **Administrator**. The **Modify Rights** dialog operates in the same manner, with the exception of the username *username* which is not required.

Users can modify, add, or delete their own mailbox, folder and sub-folder rights via their own mail client.

Delete Shared Mailboxes

To delete a shared mailbox, select the checkboxes next to the mailboxes to be deleted. Click on the **Delete Mailboxes** button; a warning dialog appears. Click on **OK** to delete the mailbox(es), or click on **Cancel** to abort the deletion.

Change Mailbox Quota

To change a mailbox quota, click on the mailbox name in the **Shared Mailbox** list. The **Modify Shared Mailbox** dialog is then presented (see "Change Access Rights" on page 65). If there is an existing mailbox quota, highlight the existing quota and then enter the new quota. To effectively set the quota to zero, or no quota, leave the **Quota Size** field blank. Click on **OK** when finished.

Change Access Rights

To change access rights, click on the target mailbox in the **Shared Mailbox List**. The **Modify Shared Mailbox** dialog appears.

Shared Mailbox	hold	
Mailbox Rights		
Add	sms (admin)	*
Modify		
Remove		v
Juota Informa	tion	
Quota Usage		0
Ouota Size (in MB) 1	

Figure 7-7 Modify Shared Mailbox Dialog

When the existing shared mailbox settings are displayed, click on the user name in the **Mailbox Rights** field. Then click on the **Modify** button. Another dialog is displayed; click on the level of rights required. To delete mailbox rights, select the user name and click on the **Remove** button.

茶 Modify Ri	ghts - Netscape	<u> </u>
	User Name: sms	
	C Read	
	C Read/Write	
	 Administrator 	
ок		Cancel

Figure 7-8 Modify Rights Dialog

Click on **OK** when finished.

Chapter 8

Account Management

User Passwords

The end-user has access to his or her own password only. This is the only end-user accessible administration command using the Web administration interface.

Change User Password Page

This page is the only administration tool available to end-users. It allows users to independently change their own password without interaction from the administrator. As with all security measures of the password-based type, it is strongly recommended that users be advised to change their passwords on a regular basis and to use a nonsensical combination of letters and numbers. To change a password, the user must provide their **Authentication ID** (login name), their **Old Password** and their **New Password**.

Note: The user must enter the new password twice for verification, then click on the **Change Password** button to complete the change.

Change U	ser Password
Auth ID	
Old Password	
New Password	
Verify New Password	
Change Pass	word Back



PART FOUR

Reference

 \mathbf{IV}

Chapter 9, "File and Directory Layouts"

Chapter 10, "File Descriptions"

Chapter 11, "Server Commands"

Chapter 12, "Administration Commands"

Chapter 13, "Mail Delivery to M-Store Mailbox Tool (deliver)"

Chapter 9

File and Directory Layouts

The following chapter is a detailed description of the M-Store filesystem. It is meant to be used as a quick reference for determining the files and directories used in M-Store. All files are located in three default directory paths:

Configuration Files	/etc/md/store/
Executable Support Files	/usr/local/md/
Run Time Data	/var/md/store/

The subdirectories and expected files at each location are organized into quick reference tables. A short description details the files found in each subdirectory.

Configuration Files

The configuration files are static files used to configure the M-Store runtime environment. These files are usually edited once when the software package is first installed, then remain static until the system administrator decides to change the configuration of the software.

Table 9-1/etc/md/store/ Configuration Files

Extended Path	File Name	Description
	ms.conf	The default message store configuration file. See Chapter 10, "File Descriptions" for a complete list of options.
	ms.conf.sample	Sample configuration file.

Table 9-1	(continued) /e	etc/md/store/ Configuration Files
Extended Path	File Name	Description
	rc.m-store.sam ple	Sample boot/shutdown script
	license.dat	The default message store license file that enables operation and determines the number of users that can be created. The path of the license file may be changed in the ms.conf configuration file.

Runtime Control

The runtime control of the message store is managed by the rc.m-store bootscript. See "Message Store Configuration (ms.conf)" in Chapter 10 for further details.

The following is the platform specific locations of the installed bootscript:

Table 9-2	Locations of the Installed Bootscript	
Platform	Bootscript Location	
IRIX	/etc/init.d/rc.m-store	
Linux	/etc/rc.d/init.d/rc.m-store	

Executable Support Files

These files are runtime files that make up the M-Store package, along with the online manpages and server documentation. This root is defined as the configuration option *executable-base-path*.

Extended Path	File Name	Description
doc/	m-store_manpages.ps	Collection of all man pages in PostScript form.
	m-store_ <i>name</i> .pdf	All M-Store manuals in Adobe Acrobat format.
lib/msg_tab/	adminmsg	Default message files for store sub-systems.
	plugmsg	
	saslmsg	
	storemsg	
lib/plugins/		Location of dynamically loadable SASL mechanism plugins. See impad "M-Store Message Server (imapd)" in Chapter 11 for further details.
lib/store/plugins/		Future alternate location of dynamically loadable SASL mechanism plugins.
lib/tcl8.2/ lib/tk8.2/	history.tcl	Installations of TCL 8.2 and TK 8.2 for use with the setup wizard and msadm_tclsh utilities. Additional sub-directories and files relating to the tcl/tk utilities are also found here.
lib/tkwizard/		Data files for the M-Store setup wizard.
man/cat5/		man pages for M-Store configuration and file locations.
man/cat8/		man pages for M-Store tools and utilities.
sbin/		M-Store runtime files.

 Table 9-3
 /usr/local/md/ Executable Support Files

Table 9-3	(continued) /usr/local/	/md/ Executable Support Files
Extended Path	File Name	Description
	authproxyd	Authentication Proxy Server.
	deliver	Utility to deliver mail into M-Store.
	imapd	IMAP daemon.
	lmtpd	LMTP daemon delivery server.
	lmtpd-oq	LMTP daemon for over quota delivery.
	msadm_bulkadd	Utility to add and create accounts for multiple users.
	msadm_bulkdel	Utility to delete accounts for multiple users.
	msadm_tclsh	Administration Command Interpreter.
	msdb_archive	Utility to list the transaction files that are no longer involved in active transactions and can be deleted to save disk space.
	msdb_backup	Utility to create live backups of M-Store.
	msdb_checkpoint	Utility to checkpoint the M-Store transaction logs.
	msdb_deadlock	Utility to detect and abort deadlocked transactions.
	msdb_recover	Utility to recover the M-Store database from corruption or failure.
	msdb_restore	Utility to restore the database from a previous msdb_backup created backup.
	msdb_test	Utility to test, initialize, or recover M-Store database files. Use it often to ensure database integrity.
	pop3d	POP3 front-end daemon.
	reconstruct	Utility to recover from mailbox cache file corruption.

Table 9-3	(continued)	/usr/local	1/md/ Executable Support Files	
Extended Path	File Na	ame	Description	_
	stor	emgr	Manages the store processes.	
	stor	e_setup	Utility to setup M-Store.	

Runtime Data Files

These files contain the dynamically changing information maintained by the M-Store package. As a rule, the files in this part of the filesystem are controlled and updated by the M-Store software itself, and are not accessed directly by an administrator or end-user. Users should never, and never need to, directly modify any files in the directories listed here with the exception of the /var/md/store/etc/nologin file and the /var/md/store/backup directory. Back up all of the files listed here on a regular basis, as they contain all of the critical user data (for example, e-mail message data).

The following files are rooted in /var/md/store. This root is defined as the configuration option ms-path.

Extended Path	File Name	Description
backup/	MSDB_Backup_ <mm>-<dd> -<yyyy>_<hr-mn></hr-mn></yyyy></dd></mm>	Default location of database backups created with msdb_backup.
database/	db_lock.share	Shared memory segments
	db_mpool.share	used by the database.
	db_txn.share	
	db.001	
database/data/	acl.db	Individual database tables
	administrators.db	in more detail below.
	authmap.db	

Table 9-4/var/md/store/Runtime Data Files

Table 9-4 (continued)) /var/md/store/ Runtime Data Files		
Extended Path	File Name	Description	
	domain.db	See above, M-Store Database Tools.	
	identifiers.db	See above, M-Store Database Tools.	
	mailboxaccess.db	See above, M-Store Database Tools.	
	mailboxbyid.db	See above, M-Store Database Tools.	
	mailboxbyname.db	See above, M-Store Database Tools.	
	quota.db		
	sec.db		
	subscription.db		
	userbyid.db		
	userbyname.db		
database/transaction_log,	/db_log.share	Shared memory segments shared between processes (db_*.share), database tables (data/*.db), and the transaction log files (transaction_log/log\. *). The path of the transaction log directory is defined by the transaction-log- \directory configuration option and defaults to the location presented here.	
	log.000000001	Default location of various database log files.	
etc/nologin/		Location of the imapd and pop3d shutdown file.	

Table 9-4	(continued)	/var/md/store/ Runtime Data Files		
Extended Path	ı	File Name	Description	
ipc/		authproxyd lmtpd	UNIX domain socket files for authproxyd and lmtpd communications.	
ipc/.tf/		user	Holds ticket files for the kerberos4 authproxyd authentication mechanism. This directory only exists if the kerberos4 authproxyd mechanism is used.	
lock/mbox/		db.001	This directory contains shared memory segments used by the locking sub-system throughout the mailstore.	
lock/pop/		db.001	This directory contains shared memory segments used by the locking sub-system throughout the mailstore.	
log/			This directory is reserved for future telemetry logging.	
mailstore/			Recommended location for the physical message store.	
mailstore/X	X/YY/ZZ/	fdb.cache	Contains pre-parsed envelope and body information for each message.	
		fdb.header	Contains general information about the mailbox itself.	
		fdb.index	Contains various mailbox and per message information.	
		fdb.seen	Tracks the seen and recent flags on a per message per user basis.	
		1.	Stored messages in RFC822 format.	

Table 9-4	(continued)	/var/md/store/ Runtime Data Files	
Extended Pa	ıth	File Name	Description
		2.	Stored messages in RFC822 format.
run/		authproxyd.lock	Lock file containing the process ID of each running daemon process. File ensures that only one instance of the daemon is running for a given message store. Multiple instances of an M-Store daemon must use different configuration files with each ms-path value.
		imapd.lock	Lock file containing the process ID of each running daemon process. File ensures that only one instance of the daemon is running for a given message store. Multiple instances of an M-Store daemon must use different configuration files with each ms-path value.
		lmtpd.lock	Lock file containing the process ID of each running daemon process. File ensures that only one instance of the daemon is running for a given message store. Multiple instances of an M-Store daemon must use different configuration files with each ms-path value.

Table 9-4 (continued)		/var/md/store/ Runtime Data Files		
Extended Pat	h	File Name	Description	
		msdb_checkpoint.lock	Lock file containing the process ID of each running daemon process. File ensures that only one instance of the daemon is running for a given message store. Multiple instances of an M-Store daemon must use different configuration files with each ms-path value.	
		msdb_deadlock.lock	Lock file containing the process ID of each running daemon process. File ensures that only one instance of the daemon is running for a given message store. Multiple instances of an M-Store daemon must use different configuration files with each ms-path value.	
		pop3d.lock	Lock file containing the process ID of each running daemon process. File ensures that only one instance of the daemon is running for a given message store. Multiple instances of an M-Store daemon must use different configuration files with each ms-path value.	
		storemgr.lock		
tmp/			The location for all temporary M-Store processes.	

M-Store Database Files

The following files are used for the database administration functions:

Table 9-5M-Store Database Files

Database Tool	Description
msdb_archive	Lists the transaction log files that are no longer involved in active transactions and can be archived or deleted to decrease disk space.
msdb_backup	Runs a live backup of the database.
msdb_checkpoint	Checkpoints the transaction logs.
msdb_recover	Recovers the database after corruption or failure.
msdb_restore	Restores the database from a previous backup
msdb_test	Tests the database for usability. Use it often to ensure database integrity, as it can detect and repair most database problems.
msdb_upgrade	Creates and initializes a new database or upgrades an existing one. This should only be run once after an install.

M-Store uses a Sleepycat database to store mailstore meta-data. Database tables containing information regarding domains, users, and mailboxes are stored in the /var/md/store/database/data directory. Modifications to the database tables are executed as atomic transactions to prevent race conditions and keep the data consistent. The /var/md/store/database/transaction_log directory contains log files of the transaction data. In the case of corruption or system failure, the transaction logs can be used to recover the database data. The database is integral to the message store and should only be operated upon by the msdb_* applications.

If any database files are missing, the message store becomes unusable. In such a case, a backup containing all database files must be restored. So it is strongly recommended that backups are completed on a regular basis. Failure to recover or restore a missing database file is a irrecoverable error and cannot be repaired. The recreation of all database files will be necessary.

M-Store Physical Mailbox Files

The path to physical mailboxes is hashed to balance the mailbox distribution throughout one or more disk partitions. Such balancing also keeps the number of subdirectories in any directory small to maintain fast access speed.

Each mailbox has a unique path determined by its partition (or mailstore), two levels of hashing (in hexadecimal), and its unique numerical mailbox identifier. For example the mailbox user/joe/INBOX in the example.com domain may have the path:

/var/md/store/mailstore/0E/C2/16183

where /var/md/store/mailstore is in the mailstore path, OE is the first hash level, C2 is the second hash level, and 16183 is the mailbox id. The path to a particular mailbox can be determined using the msadm_tclsh administration tool (see mbox_get_user_path in "User Mailbox Management Commands".

Table 9-6	M-Store Binary Mailbox Files
fdb.cache	
fdb.header	
fdb.index	
fdb.seen	

Each mailbox contains at least four files. There are four fdb binary files containing cached information regarding the mailbox and each message. The mailbox also contains the messages held within it; each message is stored in a separate file in RFC822 format. The mailbox files should never be, nor ever need to be, edited by hand.

Chapter 10

File Descriptions

The following are detailed descriptions of M-Store's key operating files. These include the files necessary for the startup and shutdown of M-Store.

Message Store Configuration (ms.conf)

ms.conf is used to configure the mailstore at invocation. The options that can be listed in the ms.conf file are organized into Required Configuration, Recommended Configuration, and Optional Configuration. Each line of the file has the form:

option value ...

where *option* is the name of the configuration option being set and *value* is the value the configuration option is being set to. Blank lines and lines beginning with # are ignored. Options take either a boolean, numerical, or (multiple) string argument.

Note: If an option is not present in the file, its default is assumed. Default values in Table 10-1 through Table 10-6 appear in square brackets at the head of the description text, for example, [default]. Some options have no default value; these are listed with <no default>. Options that default to an empty string are listed with <none>.

For boolean options, the values yes, on, t, and 1 (one) turn the option **on**, and the values no, off, f, and 0 (zero) turn the option **off**.

Required Configuration

The following options are required for the operation of M-Store (see Note in "Message Store Configuration (ms.conf)"):

Option	Description
admin_domain [<no default="">]</no>	All users of the specified domain are assumed to have site administration privileges. This option is necessary to perform Web-based site administration.
cleartext-login-enable [on]	Enables the IMAP4 LOGIN command and the POP3 USER and PASS commands. At least one of cleartext-login-enable or sasl-enable- <mech> must be enabled for users to authenticate. By default, all SASL CRAM-MD5 and DIGEST-MD5 authentication mechanisms are also enabled.</mech>
default-domain name [<no default="">]</no>	The default domain name if single-domain is enabled.
mailstore name path [<no default="">]</no>	Declare path as a mailstore with the symbolic name name. There must be at least one mailstore declared.
<pre>ms-assignment-policy rule [glob] mailstore [<no default="">]</no></pre>	Determine the mailstore (with symbolic name mailstore) on which a newly created mailbox resides. There must be at least one assignment policy defined as each acts as a filter executed in order of appearance in the ms.conf file.

Table 10-1ms.conf Required Options

There are three available ms-assignment-policy rules:

user-rule	The mailbox resides on the mailstore for which the user matches the glob pattern. This rule takes both a glob pattern and a single mailstore name.
domain-rule	The mailbox resides on the mailstore for which the domain matches the glob pattern. This rule takes both a glob pattern and a single mailstore name.

bytes-free The mailbox resides on the mailstore with the most free space. This rule does not require a glob pattern, but does take a list of mailstore names. It is recommended to end with a bytes-free rule or a glob rule with a glob pattern of * to ensure a default mailstore exists for newly created mailboxes.

Table 10-2SASL Plugin Options

Option	Description
sasl-enable-cram-md5 [on]	Enable the built-in SASL CRAM-MD5 authentication mechanism.
sasl-enable-digest-md5 [on]	Enable the built-in SASL DIGEST-MD5 authentication mechanism.
sasl-enable-plain [off]	Enable the built-in SASL PLAIN authentication mechanism.
sasl-enable- <mech> [off]</mech>	Enable the SASL <mech> authentication mechanism plugin. The <mech> plugin must also be installed in executable-base-path/lib/plugins/</mech></mech>

Example

Table 10-3SASL Plugin Option Examples

Example Command	Description
sasl-enable-kerberos_v4 on	Enable the SASL Kerberos_V4 plugin.
sasl-enable-gssapi on	Enable the SASL GSSAPI plugin.

Recommended Configuration

The following options are recommended for proper operation of M-Store.

Option	Description
hash-level-1 [20]	The number of hash directories in the first level of the mailstore. The minimum value allowed is 5 and the maximum is 500. (See NOTE in hash-level-2 Description)
hash-level-2 [200]	The number of hash directories in the second level of the mailstore. The minimum value allowed is 5 and the maximum is 500. NOTE: Under each of the defined mailstores exist a number of first-level hash directories. Each of which contains a number of second level hash directories. Mailboxes physically reside under the second-level hash directories.
quotawarn [90]	The percentage of quota utilization above which the IMAP server generates warnings.
transaction-log-directory [transaction_log]	The directory path where the database log files are stored. If the argument is a relative path, the logs are stored in ms-path/database/transaction-log-directory/. NOTE: It is highly recommended that the log files are stored and backed up on a separate disk from the database tables. See msdb_backup ("Database Backup Tool (msdb_backup)" in Chapter 12) for more information.

 Table 10-4
 Recommended
 M-Store Configuration Options

Optional Configuration

The following are optional for M-Store configuration file.

Table 10-5Optional ms.conf Entries

Option	Description
admin-auth-modal [on]	In multi-domain mode, append the current domain to the identifier when creating authentication accounts with the administration tools. i.e. creating an auth account for user foo implicitly creates the account for foo@mydomain.bar. This option has no effect in single-domain mode.
allow8bitheaders [off]	Accept messages with non-ASCII header characters by stripping the high-bit off offending characters. This option affects imapd, lmtpd, and deliver.
allow-one-message-overquota [off]	
	Allow a user to receive one message that would put them over quota. Note that if a user is already over quota then no messages can be received.
allowanonymouslogin [off]	Permit logins by the user anonymous using any password (this feature is not supported by all authentication mechanisms).
auto-create-inbox [off]	If the authenticated user does not already have an IMAP INBOX, create one automatically when they authenticate.
auto-create-inbox-quota [0]	If auto-create-inbox is enabled, the newly created INBOX is assigned a quota root with the specified value (in bytes). If the value is less than or equal to zero, no quota root is assigned.
defaultacl [anyone lrs]	The default acl (access control list) for newly created mailboxes.
executable-base-path [/usr/local/md]	The base path for M-Store binaries and documentation.
imap-port [143]	Specify the port used by imapd.

Option	Description
license-file-path [/etc/md/store/license.dat]	Specify the absolute path of the license file license.dat.
lmtp-shared-name [shared]	Specify the local name used by <pre>lmtpd</pre> to denote shared folders during Plus-Addressing delivery.
<pre>lmtp-stuff-nul [off]</pre>	Enable the conversion of NUL characters in messages to"?". The default behavior is to reject such messages.
	Note that converting such characters may render parts of the message unreadable.
	NUL characters are illegal in messages according to RFC2060. This option is provided to allow sites to work around noncompliant (broken) mail clients.
map-authentication [off]	Enable the translation of authentication identifiers using the internal authmap database. See msadm_tclsh("IM-Store Administration Command Interpreter (msadm_tclsh)" in Chapter 12) for more information on adding authentication mappings.
max-overquota-kb [0]	If we have allow-one-message-overquota set [on], this option limits the size of a message that can be delivered over quota. If this is set to 0 or undefined, there is no limit.
messagestore-deliver-overquota -bounce [off]	If enabled, causes deliver and lmtpd to return a permanent delivery failure for any message delivery that would put the target mailbox over its quota limit. Normally these programs return a temporary failure, allowing the message transport agent (MTA) to requeue the delivery attempt. Enabling this option forces the MTA to immediately bounce the message.
ms-path [/var/md/store]	The base path of the message store data.
plaintextloginpause [0]	Number of seconds to pause after a successful plaintext login. For systems that support strong authentication, this permits users to perceive a cost in using plaintext passwords.
pop-port [110]	Specify the port used by pop3d.

 Table 10-5
 (continued)
 Optional ms.conf Entries

Table 10-5 (continued)	Optional ms.conf Entries
Option	Description
popminpoll [0]	Set the minimum amount of time, in minutes, the server forces users to wait between successive POP3 logins.
poptimeout [10]	Set the length of the POP3 server inactivity for the autologout timer, in minutes. The minimum value is 10 minutes.
runtime-user [sms]	The login name of the UNIX account under which the server runs.
single-domain [off]	If enabled, the server assumes all users are of the domain specified by the default-domain option. Disabling this option allows the server to support multiple domains.
timeout [30]	The length of the IMAP server inactivity for the autologout timer, in minutes. The minimum value is 30 minutes.
umask [077]	The default umask value used by the server programs.

authproxyd Configuration

The following options are used by authproxyd, the M-Store authentication server.

-	
Option	Description
authproxy-authmech [authdb]	Specify the mechanism used to authenticate plaintext logins.
authproxy-legacy-authmech [<no default>]</no 	If authentication using authmech fails, authenticate using the legacy-authmech. If the latter succeeds, automatically build an account in the authmech authentication environment using the username and password information supplied in the authentication request. Future authentications with the same username and password will succeed with the original authmech.
authproxy-rimap-host [<no default>]</no 	The remote host to be contacted by the rimap authentication mechanism. The argument can be a hostname (imap.foo.bar) or a dotted-quad IP address (192.168.0.1). The latter is useful if the remote server is multi-homed and has network interfaces that are unreachable from the local IMAP server. The remote host is contacted on the imap service port. A nondefault port can be specified by appending a forward-slash and the port name or number to the host argument.
authproxy-pam-service [authproxyd]	The service name for PAM authentication. Setting this value to a predefined PAM service allows IMAP and POP users to authenticate with the same credentials used to authenticate via the defined service, i.e., login allows users who can physically log into the machine to be authenticated via authproxyd.

Table 10-6authproxyd Options

Files /etc/md/store/ms.conf The default location for the message store configuration file. /etc/md/store/ms.sample The sample M-Store boot script. See Also authproxyd, "Authentication Server (authproxyd)" in Chapter 11 impad, "M-Store Message Server (imapd)" in Chapter 11 Imtpd, "LMTP Delivery Server (lmtpd)" in Chapter 11 pop3d, "POP3 Message Service (pop3d)" in Chapter 11 Chapter 9, "File and Directory Layouts"

M-Store rc.m-store Script

Synopsis

rc.m-store [start | stop | restart]

rc.m-store is the recommended method of starting and stopping the message store. The sample of this file is found at etc/md/store. It is strongly recommended that your own rc.m-store script is carefully tested before putting the mailstore into production mode.

rc.m-store automatically starts at boot time and stops at shutdown. For proper operation with Sendmail or other MTA, start M-Store before starting the MTA and stop after shutting down the MTA. Please see your Operating System manual for instructions and the locations of the runtime level control mechanisms.

Table 10-7rc.m-store Parameters

Parameter	Description	
start	The following steps are required to start the message store. These steps are performed by the storemgr which is executed by the rc.m-store script:	
	1. Cleanup any files possibly left by the message store in the event of a machine crash.	
	2. Run msdb_test with recovery to ensure the consistency of the message store database.	
	3. Start the server components:	
	authproxyd: Generic Authentication server.	
	lmtpd: Local Message Transfer Protocol message delivery server.	
	pop3d: Post Office Protocol mail server.	
	imapd: Internet Message Access Protocol mail server.	
	msdb_checkpoint: Message store database transaction checkpointing daemon.	
	All server components use the default ms.conf M-Store configuration file.	
stop	Stop running the message store by sending the SIGTERM signal to the running components.	
restart	Stop and start the message store.	
Example		
----------	--	--
	/etc/init.d/rc.m-store start	
	Please see Chapter 12, "Administration Comm	ands".
Files		
	/etc/md/store/ms.conf	The default M-Store configuration file.
	/etc/rc.d/init.d/rc.m-store	The location of the bootscript on Linux.
See Also		
	authproxyd, "Authentication Server (authpro	oxyd)" in Chapter 11
	imapd, "M-Store Message Server (imapd)" in	Chapter 11
	<pre>lmtpd, "LMTP Delivery Server (lmtpd)" in Ch</pre>	napter 11
	ms.conf, "Message Store Configuration (ms.c	conf)" on page 83
	<pre>msdb_checkpoint, "Database Checkpoint To</pre>	ool (msdb_checkpoint)" in Chapter 12
	<pre>msdb_test, "Database Test Tool (msdb_test)"</pre>	in Chapter 12
	pop3d, "POP3 Message Service (pop3d)" in Cl	hapter 11
	storemgr, "Store Manager (stormgr)" on pag	e 93
	Chapter 9, "File and Directory Layouts"	

Store Manager (stormgr)

Synopsis

storemgr [-f config_file]

storemgr is a daemon process that manages the collection of protocol, authentication and database management server processes that make up the message store. It is the

	primary control daemon for the store, managing starting, restarting and shutting down the entire message store. Running storemgr starts the store manager, which subsequently starts all of the other store processes. Once started, store processes are monitored and restarted in the event that one of them terminates outside of storemgr control. storemgr must be run as the superuser and is normally invoked from the rc.m-store boot script. The rc.m-store should be used as the command line interface for performing control operations for the store, rather than using the signal-based control	
	support provided by the store	manager.
	Table 10-8 storemgr Options	
	Option	Description
	-f config_file	Specify an alternate location for the M-Store configuration file.
Logging	storemgr logs it's activities vi	a syslogd using the LOG_MAIL facility.
Signals		
	storemgr stores its process ID <i>ms-path</i> variable is defined in process ID will allow you to c) in the file <i>ms-path</i> /run/storemgr.lock, where the the M-Store configuration file. Sending signals to that ontrol various runtime functions in the store.
	SIGTERM stops the store. This	causes all managed processes to be terminated.
	SIGHUP restarts the store. This then re-started.	causes all managed server processes to be stopped and
See Also		
	authproxyd, "Authentication	n Server (authproxyd)" in Chapter 11
	imapd, "M-Store Message Ser	ver (imapd)" in Chapter 11
	lmtpd, "LMTP Delivery Serve	er (lmtpd)" in Chapter 11

ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10
msdb_checkpoint, "Database Checkpoint Tool (msdb_checkpoint)" in Chapter 12
msdb_test, "Database Test Tool (msdb_test)" in Chapter 12
pop3d, "POP3 Message Service (pop3d)" in Chapter 11
rc.m-store, "M-Store rc.m-store Script" on page 92

Message Tables

M-Store uses locale specific message tables to store error messages for its various subsystems. The following are the M-Store message tables and their location:

 Table 10-9
 M-Store Message Tables

Base Path	Extended Path	Message Table
/usr/local/md/	lib/msg_tab/	adminmsg
		plugmsg
		saslmsg
		storemsg

Shutdown file for imapd/pop3d

If the file *ms-path*/etc/nologin exists, imapd will shutdown the connection. The first line of the file will be sent to the client as an [ALERT] message before the connection is closed. See Chapter 11, "Server Commands" for more details.

Chapter 11 Server Commands

This chapter details the runtime files that provide services for M-Store. All of the files discussed here are usually run as daemon processes. Pay close attention the settings presented here as these daemons are the key operating processes for the mailstore.

Authentication Server (authproxyd)

Synopsis

authproxyd [-v] [-f config_file]

authproxyd is a daemon process that provides authentication services to the M-Store imapd and pop3d servers. Specifically, it processes LOGIN and AUTHENTICATE PLAIN IMAP4 commands, as well as the USER and PASS POP3 commands.

This server fulfills two roles: isolation of all code requiring superuser privileges into a single process, and to provide proxy authentication services to clients that do not understand SASL based authentication.

authproxyd must be run as the superuser and will change to the runtime-user as defined in the configuration file except when running against a protected authentication database (for example, the shadow mechanism). authproxyd is normally invoked from the storemgr daemon process as part of the set of managed server processes that make up a running message store. All stop and restart operations for authproxyd should be performed using the rc.m-store boot script.

authproxyd will not run if any database files are missing, in such a case a backup containing all database files must be restored.

Logging

Signals

Protocol

Table 11-1 authproxyd Options Option Description -f config_file Specify a non-default location for the M-Store configuration file, which in turn determines the path name to the named socket to listen to for connection requests. The socket name is defined as *ms-path*/ipc/authproxyd -v Display version number and available authentication mechanism on standard error, then exit. authproxyd logs its activities via syslogd using the LOG_AUTH facility. authproxyd stores its process ID in the file *ms_path*/run/authproxyd.lock, where the *ms-path* variable is defined in the M-Store configuration file. Sending signals to that process ID will allow you to control various runtime functions in the server. SIGTERM - If authproxyd was run standalone, sending SIGTERM to the server will stop it. If authproxyd was invoked by storemgr then sending SIGTERM will cause storemgr to restart it. authproxyd understands only one client command which must be of the form: AUTHENTICATE login password\r\n authproxyd responds with the following form: OK [text message] or NO [text message] Note that the text message is optional and there are no end-of-line characters on the reply.

the rc.m-store boot script.

If authproxyd was invoked by storemgr, then the server cannot be independently shut down, as storemgr will automatically restart it. To shut down the server, you must use

007-3878-001

Files		
	/etc/md/store/ms.conf	The default location for the message store configuration file.
	/etc/md/store/ms.sample	The sample M-Store boot script.
	<i>ms-path</i> /ipc/authproxyd	The default named socket.
	<i>ms-path</i> /run/authproxyd.lock	The lock file containing the process id of the running authproxyd process.
See Also		
	getpwent(*)	
	getspnam(*)	
	getuserpw(*)	
	<pre>ms.conf, "Message Store Configuration (</pre>	(ms.conf)" in Chapter 10
	msadm_tclsh, "IM-Store Administration Chapter 12	Command Interpreter (msadm_tclsh)" in
	pam(*)	
	passwd(*)	
	<pre>sia_authenticate_user(*)</pre>	
	storemgr, "Store Manager (stormgr)" in	Chapter 10
	Chapter 9, "File and Directory Layouts"	
	*See your system man pages.	
Configuration		

The following options are set in the M-Store configuration file. If an option is not present in the file, its default is assumed.

Note: Default values appear in square brackets at the head of the description text. Some options have no default value; these are listed with <no default>.

Option	Description
authproxy-authmech [authdb]	Specify the mechanism used to authenticate plain text logins.
authproxy-legacy-authmech [no default]	When authentication using authmech fails, authenticate using the legacy-authmech. If the latter succeeds, automatically build an account in the authmech authentication environment using the user name and password information supplied in the authentication request. Future authentications with the same user name and password will succeed with the original authmech. (See "Account Migration" on page 102.)
authproxy-rimap-host [no default]	The remote host to be contacted by the rimap authentication mechanism. The argument is a host name (imap.foo.bar) or a dotted-quad IP address (192.168.0.1). The latter is useful if the remote server is multi-homed and has network interfaces that are unreachable from the local IMAP server. The remote host is contacted on the imap service port. A non-default port can be specified by appending a forward-slash and the port name or number to the host argument.
authproxy-pam-service [imap]	The service name for PAM authentication.

 Table 11-2
 authproxyd Configuration Options

Authentication Mechanisms

Depending on the facilities provided by your underlying operating system, authproxyd supports one or more **authentication mechanisms**. The mechanism is selected by the authproxy-authmech configuration variable where the associated value is one of the following:

Variable	Description
authdb	Authenticate via CRAM-MD5 or DIGEST-MD5 against the internal M-Store password database.
getpwent	Authenticate using the getpwent() library function. Typically this authenticates against the local password file. (See your system's getpwent(3) man page for details.)
kerberos4	Authenticate against the local kerberos4 realm. (See caveats regarding this driver in "Account Migration" on page 102.)
pam (Linux)	Authenticate against the PAM (Pluggable Authentication Module) framework. The module name is given by the authproxy-pam-service configuration option. (See your system's getpwent(3) man page for details.)
rimap	Forward authentication requests to a remote IMAP server. This driver connects to a remote IMAP server, specified by the authproxy-rimap-host configuration option, and attempts to login (via an IMAP LOGIN command) using the credentials supplied to the local server. If the remote authentication succeeds, the local connection is also considered to be authenticated. The remote connection is closed as soon as the tagged response from the LOGIN command is received from the remote server.

 Table 11-3
 authproxy-authmech Configuration Variables

Table 11-3 (continued)	authproxy-authmeen configuration variables	
Variable	Description	
	The value of the authproxy-rimap-host configuration option, hostname, describes the remote server to forward authentication requests to. The hostname can be a hostname (imap.foo.bar) or a dotted-quad IP address (182.168.0.1). The latter is useful if the remote server is multi-homed and has network interfaces that are unreachable from the local IMAP server. The remote host is contacted on the imap service port. A nondefault port is specified by appending a forward slash and the port name or number to the hostname argument.	
	The authproxy-rimap-host configuration option is mandatory when using the rimap mechanism.	
shadow	Authenticate against the local shadow password file. The exact mechanism is system dependent. authproxyd currently understands the getspnam() and getuserpw() library routines.	

Table 11-3 (continued) authproxy-authmech Configuration Variables

Account Migration

authproxyd can be configured to automatically migrate users from an insecure authentication mechanism (that is, plaintext) to a more secure one (that is, CRAM-MD5). The authproxy-legacy-authmech configuration option specifies a fallback authentication mechanism to be used if the account being authenticated does not exist in the authmech authentication environment. If this fallback authentication succeeds, authproxyd creates an account in the authmech authentication environment using the account name and password provided in the authentication request. For example, a site wanting to migrate account information from a local password file to an authdb account database would invoke authproxyd with a configuration file containing the following:

authproxy-authmech authdb authproxy-legacy-authmech getpwent

The first time a given account attempts to authenticate using CRAM-MD5 or DIGEST-MD5 the AUTHENTICATE command fails (since the account does not exist in the internal account database), and the client falls back to using an AUTHENTICATE PLAIN or LOGIN command. If this fallback authentication succeeds, authproxyd creates an account

in the internal account database, using the account name and password provided in the authentication request. The next time that account attempts to log in to the server it will be able to do so using the native SASL CRAM-MD5 or DIGEST mechanism.

legacy_authmech can specify any supported authentication mechanism, however, the
only valid authmech when doing account migration is authdb.

The kerberos4 authentication driver consumes considerable resources. To perform an authentication it must obtain a ticket-granting-ticket from the TGT server on every authentication request. The Kerberos library routines that obtain the TGT also create a local ticket file, on the reasonable assumption that a local ticket file is needed for use by other Kerberos applications. These ticket files are unusable by authproxyd, however, there is no way to prevent their creation. The overhead of accessing these ticket files causes serious performance degradation on busy mail servers. We recommend against using this driver. (Kerberos was never intended to be used in this manner; the best option is to deploy Kerberos-aware clients.)

M-Store Message Server (imapd)

Synopsis

imapd [-f config_file]

M-Store is an IMAP4 revision 1 (RFC2060) compliant protocol server interface to the message store. imapd must be run as the superuser and will change to the runtime-user as defined in the configuration file for normal operation. imapd is normally invoked from the storemgr daemon process as part of the set of managed server processes that make up a running message store. All stop and restart operations for imapd should be performed using the rc.m-store boot script.imapd can use SASL to authenticate users. The SASL authentication mechanisms PLAIN and CRAM-MD5 are built in, and other available mechanisms may also be used by placing the appropriate plugin into the M-Store plugin directory *executable-base-path*/lib/plugins/, where *executable-base-path* is defined in the M-Store configuration file.

Normally, the daemon process is invoked from the rc.m-store boot script.

Logging

Signals

Option	Description
-f config_file	Specify an alternate location for the M-Store configuration file.
1	
imapd logs its a	ctivities via syslogd using the LOG_MAIL facility
imapd logs its ad imapd stores its j variable is define will allow you to	ctivities via syslogd using the LOG_MAIL facility process ID in the file <i>ms-path/</i> run/imapd.lock, where the <i>ms-pat</i> ed in the M-Store configuration file. Sending signals to that proce o control various run time functions in the server.

M-Store's imapd supports the following option:

SIGHUP - Dump runtime processing statistics for the server to the *ms-path*/log/imapd.stats log.

/etc/md/store/ms.conf The default M-Store configuration file. /etc/md/store/rc.m-store.sample The sample M-Store boot script. executable-base-path/lib/plugins/ The default SASL plugin directory. *ms-path*/run/imapd.lock The lock file containing the process id of the running imapd process. *ms-path*/ipc/authproxyd The path of the authproxyd communication socket. *ms-path*/etc/nologin The path of the imapd shutdown file. ms-path/log/imapd.stats The path of the log file containing the statistics generated on SIGHUP. *executable-base-path* defaults to /usr/local/md *ms-path* defaults to /var/md/store See Also

authproxyd, "Authentication Server (authproxyd)" on page 97
ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10
pop3d, "POP3 Message Service (pop3d)" on page 110
rc.m-store, "M-Store rc.m-store Script" in Chapter 10
stormgr, "Store Manager (stormgr)" in Chapter 10
Chapter 9, "File and Directory Layouts"
M. Crispin, Internet Message Access Protocol - Version 4rev1, RFC2060

IMAP4 Standard Extensions

imapd supports the following standards track IMAP4 extensions: ACL (RFC 2086), LITERAL+ (RFC 2088), NAMESPACE (RFC 2342), QUOTA (RFC 2087), and UIDPLUS (RFC 2359).

Files

Access Control Lists

The identifiers in access control lists correspond to IMAP4 user names. The user name anyone is reserved as a wildcard entry matching all IMAP4 users on the server. The user name anonymous is also reserved; the server uses this identifier for all anonymous sessions.

Quota Implementation

imapd allows quotas to be set on the amount of disk storage used on a per-user basis. The SETQUOTA resource limit name is STORAGE, and the resource units are 1024 byte blocks. The GETQUOTA and GETQUOTAROOT commands return the resource usage and limits in units of 1024 byte blocks. The resource value displayed is calculated as int(bytes_used / 1024). Internally, the server uses the exact byte count when determining quota usage. Only server administrators can display and set quotas.

Protocol Extensions

The following non-standard protocol extensions are supported:

Capability

If cleartext-login-enable is set to off in the configuration file, the server will include the string X-LOGIN-COMMAND-DISABLED in the capability list. This indicates clients will not issue a LOGIN command. imapd will not run if any database files are missing, in such a case a backup containing all database files must be restored.

If imapd was invoked by storemgr, then the server cannot be independently shut down, as storemgr will automatically restart it. To shut down the server, you must use the rc.m-store boot script. If the file *ms-path*/etc/nologin exists, imapd will shut down the connection. The first line of the file will be sent to the client as an [ALERT] message before the connection is closed. The *ms-path* parameter is defined in the M-Store configuration file ms.conf.

imapd can use SASL to authenticate users. The SASL authentication mechanisms PLAIN and CRAM-MD5 are built in, and other available mechanisms may also be used by placing the appropriate plugin into the M-Store plugin directory executable-base-path/lib/plugins/, where executable-base-path is defined in the M-Store configuration file. User authentication via the IMAP LOGIN command is done by the external authproxyd authentication server.

LMTP Delivery Server (Imtpd)

Synopsis

lmtpd [-f config_file]

Imtpd is a daemon process that provides a LMTP (RFC2033) message injection interface to the MessagingDirect message store. It provides numerous benefits over deliver, and is the preferred delivery interface between the MTA and the message store.

lmtpd must be run as the superuser and will change to the runtime-user as defined in the configuration file for normal operation. lmtpd is normally invoked from the storemgr daemon process as part of the set of managed server processes that make up a running message store. All stop and restart operations for lmtpd should be performed using the rc.m-store boot script.

By default, lmtpd rejects all messages containing non-ASCII characters in the message headers. To maintain backward compatibility with MUA software that does not properly MIME-encode non-ASCII header data, add the line: allow8bitheaders to the ms.conf file. This line forces lmtpd to accept the message by stripping the high-bit from any non-ASCII characters.

By default, lmtpd delivers to a user's INBOX. To deliver to a specific mailbox, append the mailbox name to the recipient's local name. For example:

rcpt to: joe+important/March2000@foobar.com

will deliver the message to the mailbox:

user/joe/important/March2000

where joe@foobar.com is a valid user in the message store. To deliver to a shared mailbox, append the mailbox name to the lmtp-shared-name name defined in ms.conf.

rcpt to: shared+bugreports@foobar.com

This method of delivery is known as **Plus-Addressing**. Plus-Addressing is not a standard, but it does result in a valid RCF822 address.

Imtpd does not (yet) support the LMTP AUTH command. The access permissions on the directory containing the named socket determine who has access to the LMTP server. Any process capable of connecting to the named socket can inject messages into any INBOX in the message store. Only the server runtime user should have access to the named socket directory.

lmtpd will not run if any database files are missing, in such a case a backup containing all database files must be restored. If lmtpd was invoked by storemgr, then the server cannot be independently shut down, as storemgr will automatically restart it. To shut down the server, you must use the rc.m-store boot script.

Option	Description
-f config_file	Specify a non-default location for the M-Store configuration file, which in turn determines the pathname to the named socket to listen on for connection requests. The socket name is defined as <i>ms-path</i> /ipc/lmtpd.

Logging

lmtpd records its activities via syslogd using the LOG_MAIL facility

Signals

lmtpd stores its process ID in the file ms-path/run/lmtpd.lock, where the ms-path
variable is defined in the M-Store configuration file. Sending signals to that process ID
will allow you to control various runtime functions in the server.

SIGTERM - If 1mtpd was run standalone, sending SIGTERM to the server will stop it. If 1mtpd was invoked by storemgr then sending SIGTERM will cause storemgr to restart it.

SIGHUP - Dump runtime processing statistics for the server to the *ms-path*/log/lmtpd.stats log.

The following Imtpd-specific options are set in the M-Store configuration file. If an option is not present in the file, its default is assumed. Default values appear in square brackets at the head of the description text. lmtp-shared-name [shared] Specify the local name used to denote shared folders during Plus-Addressing delivery. When enabled, lmtpd will also listen to the lmtp-enable-overquota-delivery named socket *ms-path*/ipc/lmtpd-oq. All [off] mail delivered through this socket is delivered regardless of a user's quota. The behavior of the default socket is unchanged. Files /etc/md/store/ms.conf The default M-Store configuration file *ms-path*/ipc/lmtpd The default named socket. *ms-path*/run/lmtpd.lock The lock file containing the process ID of the running 1mtpd process. /etc/md/store/rc.m-store.sample The sample M-Store boot script. *ms-path*/log/lmtpd.stats The path of the log file containing the statistics generated on SIGHUP. executable-base-path defaults to /usr/local/md *ms-path* defaults to /var/md/store on all systems. See Also deliver, "deliver Synopsis" in Chapter 13 imapd, "M-Store Message Server (imapd)" on page 103 ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10 storemgr, "Store Manager (stormgr)" in Chapter 10 Chapter 9, "File and Directory Layouts"

Configuration

POP3 Message Service (pop3d)

Synopsis

pop3d [-f config_file]

pop3d is a POP3 (RFC1939) protocol server interface to the message store. It is a daemon process and is normally invoked from the rc.mdstore boot script. pop3d must be run as the superuser and will change to the runtime-user as defined in the configuration file for normal operation. pop3d is normally invoked from the storemgr daemon process as part of the set of managed server processes that make up a running message store. All stop and restart operations for pop3d should be performed using the rc.m-store boot script.

Table 11-6pop3Options

Option	Description
-f config_file	Use M-Store's configuration file <i>config_file</i> instead of the default.

The POP3 server is only capable of serving the authenticated user's IMAP4 INBOX folder. This is not a bug, it is a restriction of the POP3 protocol. If access to multiple folders are required, use the IMAP4 protocol.

pop3d enforces exclusive access to the user's INBOX folder: a user can have only one POP3 session active at any time. Access to the folder via another POP3 session is denied while the original POP3 session has the maildrop open.

If the file *ms-path*/etc/nologin exists, pop3d will shut down the connection. The first line of the file will be sent to the client as an [ALERT] message before the connection is closed. The *ms-path* parameter is defined in M-Store's configuration file ms.conf.

pop3d can use SASL (via APOP) to authenticate users. The mechanisms PLAIN and CRAM-MD5 are built in, and other mechanisms can be used by placing the appropriate plugin into M-Store's plugin directory:

executable-base-path/lib/plugins/

where *executable-base-path* is defined in M-Store's configuration file.

pop3d will not run if any database files are missing. In such a case, a backup containing all database files must be restored.

	If pop3d was invoke as storemgr will au rc.m-store boot so	d by storemgr , then the server cannot be independently shut down, atomatically restart it. To shut down the server, you must use the cript.
Logging		
	pop3d records its ac	tivities via syslogd using the LOG_MAIL facility.
Signals		
	pop3d stores its process ID in the file <i>ms-path</i> /run/pop3d.lock, where the <i>ms-path</i> variable is defined in the M-Store configuration file. Sending signals to that process ID will allow you to control various runtime functions in the server.	
	SIGTERM - If pop3d was run standalone, sending SIGTERM to the server will stop it. If pop3d was invoked by storemgr then sending SIGTERM will cause storemgr to restart it.	
	SIGHUP - Dump run ms-path/log/pop3d	time processing statistics for the server to the .stats log.
Protocol Extensions		
	The following are the protocols supported by this release of pop3d:	
	САРА	The CAPA command lets clients probe the server to discover which POP3 extensions are supported. The CAPA command is experimental; the implementation is subject to change to ensure conformance with the to-be-released POP3 Extensions RFC.
	EXPIRE	The server does not automatically expire messages; an EXPIRE NEVER response is always sent.
	IMPLEMENTATION	The server name and version number are returned with this response.
	PASS	Enter a password after giving the user command.
	PIPELINING	Clients can issue commands while other commands are outstanding.
	RESP-CODES	The server supports the [IN-USE] and [LOGIN-DELAY] extended response codes.
	SASL	If any SASL mechanisms are enabled in M-Store's configuration file they are listed in this response. A SASL response indicates the AUTH command is available.

TOP	The server supports the TOP command.
UIDL	The server supports the UIDL command.
USER	When cleartext-login-enable is turned on in M-Store's configuration file, the server advertises this capability, and the USER and PASS commands are functional.

Files

/etc/md/store/ms.conf	The default M-Store configuration file.
/etc/md/store/rc.m-store.sample	The sample M-Store boot script.
executable-base-path/lib/plugins/	The default SASL plugin directory.
<i>ms-path</i> /pic/authproxyd	The path of the authproxyd communication socket.
<i>ms-path</i> /run/pop3d.lock	The lock file containing the process ID of the running pop3d process.
ms-path/etc/nologin	The path of the pop3d shutdown file.
<i>ms-path</i> /log/pop3d.stats	The path of the log file containing the statistics generated on SIGHUP.
<i>executable-base-path</i> defaults to /usr/local/md	

ms-path defaults to /var/md/store

See Also

authproxyd, "Authentication Server (authproxyd)" on page 97
imapd, "M-Store Message Server (imapd)" on page 103
ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10
rc.m-store, "M-Store rc.m-store Script" in Chapter 10
storemgr, "Store Manager (stormgr)" in Chapter 10
POP3 Authentication Command, RFC1734.
"Post Office Protocol Version 3", RFC1939.

Chapter 12 Administration Commands

This chapter details the commands used to administer the M-Store. Please note the mode in which each command utility is meant to operate. Also note that many of the utilities presented here can be accessed via the Web Administration Interface. Please see the "Web Administration" section of this document for further details.

Starting and Stopping M-Store

The section provides the specific command paths for operating M-Store. This information is also presented in the *Package Installation Summary* screen if M-Store was installed using an included setup wizard.

Starting

Please log in as the superuser to start and stop M-Store. The command varies slightly by platform. Refer to the following command path appropriate to your platform:

Linux

To start M-Store: /etc/rc.d/init.d/rc.m-store start

All M-Store servers are daemon processes. It is possible that the rc.m-store script may falsely fail to detect the successful startup of a server. This behavior can occur on older slower machines or if the store is started while the machine is under load. To confirm the startup of a server, read the syslog files.

Stopping

As with the start command path, the stop command path varies according to platform. Refer to the following command paths to stop M-Store:

Linux

To stop M-Store: /etc/rc.d/init.d/rc.m-store stop

IM-Store Administration Command Interpreter (msadm_tclsh)

Synopsis

msadm_tclsh [-f config_file] [script...]

msadm_tclsh is a simple TCL-based administrative client for the M-Store server. If given optional scripts on the command line, msadm_tclsh reads TCL commands from the file script and evaluates them. Otherwise, msadm_tclsh runs in interactive mode, reading commands from the standard input and evaluating them. msadm_tclsh runs until the exit or quit command is invoked, or until it reacIMhes end-of-file on its standard input. Any arguments other than those specified here are made available in the TCL variables argc and argv. msadm_tclsh must be run as the run-time user.

msadm_tclsh will not run if any database files are missing, in such a case a backup containing all database files must be restored.

 Table 12-1
 msadm_tclsh Options

Option	Description
-f config_file	Specify an alternate location for the M-Store configuration file.
script	Execute commands from a file script or execute the listed commands when evoked from a script as:
	#!/usr/local/md/sbin/msadm_tclsh\ domain_set esys.ca user_add joe

Generic Commands

The following commands may be used at any time during the session.

 Table 12-2
 msadm_tclsh
 Generic Commands

Command	Description & Example	
help	Get help on commands, for example, help <i>command</i>	
quit	Terminate the session and exit (that is, quit or exit).	

Site Administration Commands

The following commands are used to manage site administrators. They may be used at any time during the session.

Command	Description & Example	
get_admin_domain	Displays the name of the administrative domain as defined by admin-domain in the configuration file, for example, get_admin_domain.	
site_admin_add	Add user as a site administrator in the administrative domain, for example, site_admin_add <i>user</i> .	
site_admin_del	Delete user as a site administrator in the administrative domain, for example, site_admin_del <i>user</i> .	
site_admin_list	List site administrators matching the specified glob pattern, for example, site_admin_list <i>pattern</i> .	

 Table 12-3
 msadm tclsh Site Administration Commands

Domain Management Commands

The following commands are used to manage domains.

Command **Description & Example** Create the specified domain. The users anonymous and anyone domain add are implicitly created by this command, for example, domain add domain Allow anonymous logins for the specified domain. Anonymous domain_allow_anon logins are allowed by default when a domain is created, for example, domain_allow_anon domain. domain del Remove the specified domain and all corresponding users and mailboxes. This command is not reversible. Use it with caution. Example: domain del domain. Remove the asigned quota for the specified domain, for example, domain_del_quota domain_del_quota domain. domain disable Temporarily disables users of the specified domain from accessing the server. This prevents users of the domain from being authenticated, but still allows incoming mail to be delivered, for example, domain disable domain. Disable anonymous logins for the specified domain, for example, domain_disable_anon domain disable anon domain. Allow users of the specified domain to access the server. Domains domain enable created with domain add are enabled by default, for example, domain enable domain. domain get Display the details for the specified domain including whether or not it is enabled and allows anonymous logins, for example, domain_get domain. domain_list List domains matching the specified glob pattern, for example, domain_list pattern. domain rename Rename domain *oldname* to *newname*. Any existing password/authentication accounts for this domain will not be renamed, for example, domain rename *oldname newname*.

 Table 12-4
 msadm_tclsh Domain Management Commands

Table 12-4 (continued)	msadm_tclsh Domain Management Commands
Command	Description & Example
domain_set	Set the administrative domain to domain. All subsequent account and mailbox commands will take place within the specified domain. This function assumes the domain has been created with domain_add, for example, domain_set <i>domain</i> .
domain_set_quota	Set a quota limit of <i>quota_limit</i> kilobytes for the specified domain, for example, domain_set_quota <i>domain quota_limit</i> .

Account Management Commands

The following commands are used to manage domain administator, internal password (authentication), and user accounts. They may only be used after defining the current administrative domain with the domain_set command.

 Table 12-5
 msadm_tclsh Account Management Commands

Command	Description
admin_add	Designate the specified user to be an administrator of the current domain, for example, admin_add <i>user</i> .
admin_del	Remove the administrator privileges for the specified user, for example, admin_del <i>user</i> .
admin_list	List users of the current domain having administration privileges and matching the specified glob pattern, for example, admin_list <i>pattern</i> .
auth_add	Add a password account for the specified authentication identifier with the specified password. The authentication identifier authid is the exact string used as a login name.
	If both the configuration option admin-append-domain-auth is enabled and the currently set administrative domain does not match the default-domain configuration option, the current administrative domain is appended to the authentication identifier making it <i>authid@domain</i> .

Table 12-5 (cont	inued) msadm_tclsh Account Management Commands
Command	Description
auth_del	Delete the password account for user <i>authid</i> . If both the configuration option admin-append-domain-auth is enabled and the currently set administrative domain does not match the
	default-domain configuration option, the current administrative domain is appended to the authentication identifier making it <i>authid@domain</i> .
auth_disable	Disable the password account so that the user <i>authid</i> is denied authentication with the stored password.
	If both the configuration option admin-append-domain-auth is enabled and the currently set administrative domain does not match the default-domain configuration option, the current administrative domain is appended to the authentication identifier making it <i>authid@domain</i> .
auth_enable	Enable the password account so that the user <i>authid</i> may be authenticated with the stored password. All the passwords accounts created with auth_add are enabled by default.
	If both the configuration option admin-append-domain-auth is enabled and the currently set administrative domain does not match the default-domain configuration option, the current administrative domain is appended to the authentication identifier making it <i>authid@domain</i> .
auth_get	Display the password account details for user <i>authid</i> . The output consists of three fields:
	authentication identifier: Fully qualified login name.
	password expiration date: If zero (0), the password never expires, otherwise the expiration date is expressed in the form <i>YYYYMMDDHHNNSS</i> , where <i>YYYY</i> is the year, <i>MM</i> is the month, <i>DD</i> is the day, <i>HH</i> is the hour, <i>NN</i> are the minutes, and <i>SS</i> are the seconds.
	account enabled flag: 1 if enabled, 0 if disabled
	If both the configuration option admin-append-domain-auth is enabled and the currently set administrative domain does not match the default-domain configuration option, the current administrative domain is appended to the authentication identifier making it <i>authid@domain</i> .
auth_list	List password accounts matching the specified glob pattern, for example, auth_list <i>pattern</i> .

Command	Description
auth_mod	Modify the password account for the user <i>authid</i> . Currently, this is limited to setting the expiration-date after which the user's password expires. By default, passwords created with auth_add or changed with passwd never expire. If the expiration-date is zero (0), the password never expires, otherwise the date is expressed in the form <i>YYYYMMDDHHNNSS</i> , where <i>YYYY</i> is the year, <i>MM</i> is the month, <i>DD</i> is the day, <i>HH</i> is the hour, <i>NN</i> are the minutes, and <i>SS</i> are the seconds, for example, auth_mod <i>authid expiration-date</i> .
auth_passwd	Set the password stored in the password account for user <i>authid</i> to <i>password</i> . If both the configuration option admin-append-domain-auth is enabled and the currently set administrative domain does not match the default-domain configuration option, the current administrative domain is appended to the authentication identifier making it <i>authid@domain</i> .
auth_rename	Rename the password account for user <i>oldauthid</i> to <i>newauthid</i> . If both the configuration option admin-append-domain-auth is enabled and the currently set administrative domain does not match the default-domain configuration option, the current administrative domain is appended to the authentication identifier making it <i>authid@domain</i> .
user_add	Create the user account for the specified user, for example, user_add <i>user</i> .
user_del	Delete user account for the specified user, for example, user_del user.
user_list	List all user accounts for usernames matching the glob pattern <i>pattern</i> , for example, user_list <i>pattern</i> .
user_rename	Rename the user account for user <i>oldname</i> to <i>newname</i> , for example, user_rename <i>oldname newname</i> .

Table 12-5 (continued) msadm_tclsh Account Management Commands

Example: Create a Login in a Multi-domain Setting

The following example is a typical session to create the traditional login jworker for user joe.worker@example.com in a multi-domain setting. It is assumed that the ms.conf configuration option admin-append-domain-auth is disabled to prevent appending the domain name on authentication account creation.

```
domain_set example.com
mbox_user_add joe.worker
auth_add jworker iMc001
auth_alias_add jworker joe@example.com
quit
```

Note: When creating the user account and mailboxes for joe.worker@example.com, create the authentication account jworker instead of joe.worker@example.com. We create the mapping so that Joe may authenticate as jworker and access his normal joe.worker@example.com account.

Account Mapping (alias) Commands

M-Store provides the ability to explicitly map an authentication account to a particular authorization account. This allows a user to authenticate with a given identifier (authid) and also be authorized with a different identifier (userid).

This is used to provide users with the ability to authenticate using a traditional name such as joe in a multi-domain setting, where Joe's account is actually joe@example.com. Another use is to provide a friendly authentication alias such as joe.user, where Joe's authentication ID is actually his employee number.

Command	Description
auth_alias_add	Add a mapping from the fully-qualified authentication identifier <i>authid</i> to the authorization identifier <i>userid</i> . If the <i>userid</i> is not of the form user@domain, then the <i>userid</i> is assumed to be of the default-domain, for example, auth_alias_add <i>authid alias</i> .
auth_alias_del	Remove the mapping for the fully-qualified authentication identifier, for example, auth_alias_del <i>authid</i> .
auth_alias_mod	Change the mapping for the fully-qualified authentication identifier <i>authid</i> to point to the authorization identifier <i>newuserid</i> . If <i>newuserid</i> is not of the form <i>user@domain</i> , then it is assumed to be of the default-domain.
auth_alias_list	List mapping entries matching the specified glob pattern, for example, auth_alias_list <i>pattern</i> .

 Table 12-6
 msadm_tclsh Account Mapping (alias) Commands

User Mailbox Management Commands

The following commands are used to manage user mailboxes. They may only be used after defining the current administative domain with the domain_set command.

Command **Description & Example** Remove the rights acl for user *identifier* on the mailbox belonging acl_user_del to user, for example, acl_user_del user mailbox identifier acl. Display the access control list for mailbox belonging to user, for acl_user_get example, acl_user_get user mailbox. Add the rights acl for user *identifier* on mailbox belonging to user, acl user set for example, acl user set mailbox identifier acl. Display the path to the mailbox belonging to user, for example, mbox_get_user_path mbox_get_user_path user mailbox. Create a user account and inbox for the specified user, for example, mbox_user_add mbox user add user. mbox_user_del Delete the specified user account and all associated mailboxes, for example, mbox user del user. mbox_user_list List all the mailboxes of the domain that match the specified glob pattern, for example, mbox user list pattern. Rename the oldusername to newusername and each of the associated mbox_user_rename mailboxes, for example, mbox user rename *oldusername* newusername.

 Table 12-7
 User Mailbox Management Commands

Table 12-7 (continued)	User Mailbox Management Commands
Command	Description & Example
mbox_user_to_shared	Convert the mailbox belonging to <i>user</i> to a shared mailbox, for example, mbox_user_to_shared <i>user sharedname</i> Thus mbox_user_to_shared joe graphics would convert user/joe/INBOX user/joe/company_logos user/joe/company_logos/jpeg to shared/graphics/ shared/graphics/company_logos shared/graphics/company_logos/jpeg
mbox_usersub_add	Create the sub-folder mailbox for user, for example, mbox_usersub_add user mailbox.
mbox_usersub_del	Delete the sub-folder mailbox for user, for example, mbox_usersub_del <i>user</i> mailbox.
mbox_usersub_rename	Rename the sub-folder <i>oldboxname</i> to <i>newmboxname</i> , for example, mbox_usersub_rename <i>user oldmboxname newmboxname</i> .
quota_user_del	Remove the quota on a specified user, for example, quota_user_del <i>user</i> .
quota_user_get	Display the current quota limit and usage for the specified user, for example, quota_user_get <i>user</i> .
quota_user_set	Set a quota limit of quota kilobytes for user. The quota applies to all subfolders, for example, quota_user_set <i>user quota</i> .

Shared Mailbox Management Commands

The following commands are used to manage shared mailboxes. They may only be used after defining the current administrative domain with the domain_set command.

Command	Description & Example
acl_shared_del	Remove the rights acl for user identifier on the shared mailbox, for example, acl_shared_del <i>mailbox identifier</i> acl.
acl_shared_get	Display the access control list for the specified shared mailbox, for example, acl_shared_get <i>mailbox</i> .
acl_shared_set	Add the rights acl for user identifier on the shared mailbox, for example, acl_shared_set <i>mailbox identifier</i> acl.
mbox_get_shared_path	Display the path to the specified mailbox, for example, mbox_get_shared_path <i>mailbox</i> .
mbox_shared_add	Create the shared mailbox <i>mailbox</i> owned by owner. The owner is not required if creating a sub-folder of an already owned folder, for example, mbox_shared_add <i>mailbox owner</i> .
mbox_shared_del	Delete the specified shared mailbox, for example, mbox_shared_del <i>mailbox</i> .
mbox_shared_list	List all shared mailboxes matching the specified glob pattern, for example, mbox_shared_list <i>pattern</i> .
mbox_shared_rename	Rename the shared mailbox <i>oldname</i> to <i>newname</i> , for example, mbox_shared_rename <i>oldname newname</i> .
quota_shared_del	Remove the quota on the specified shared mailbox, for example, quota_shared_del <i>mailbox</i> .
quota_shared_get	Display the current quota limit and usage for the specified shared mailbox, for example, quota_user_get mailbox.
quota_shared_set	Set a quota limit of quota kilobytes for shared mailbox. The quota applies to all subfolders, for example, quota_shared_set <i>mailbox quota</i> .

 Table 12-8
 User Mailbox Management Commands

Example: Add a New Site Administrator

The following example adds a new site administrator, where example.mail2.com is set as the Site Administrator domain.

domain_set example.mail2.com
user_add bobadmin
site_admin_add bobadmin
auth add bobadmin passwd

Example: Create a Domain and Add a First User

The following example creates a domain and first user, where the domain example.com and the user joe@example.com with the password IamJoe!4 are created.

domain_add example.com domain_set example.com mbox_user_add joe auth add joe IamJoe!4 mbox_usersub_add joe Sentmail mbox_usersub_add Important mbox_usersub_add joe Important/fun mbox_usersub_add joe Important/work quit

This example also creates the following folders within the example.com domain:

user/joe/INBOX user/joe/Sentmail user/joe/Important user/joe/Important/fun user/joe/Important/work quit

The address joe@example.com is now deliverable and user joe can log on and check his mail.

See Also

ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10
msadm_bulkadd, "Add Users in Bulk to M-Store (msadm_bulkadd)" on page 125
msadm_bulkdel, "Delete Multiple Domains and Users (msadm_bulkdel)" on page 128
Chapter 9, "File and Directory Layouts"

Bulk Administration Tools

This section details the included tools designed to allow for the batch (bulk) administration of M-Store.

Add Users in Bulk to M-Store (msadm_bulkadd)

Synopsis

msadm_bulkadd [-i0] [-f config_file] [-d domain] [-q quota]

msadm_bulkadd reads user information from the given data file and creates an account for each user.

It is highly recommended that msdb_backup be run after bulk adding users to safeguard new data and to clean the database transaction logs. If the transaction logs are not cleaned, there may be very long waits when running database recovery (as is usually done at boot time through the rc.mdstore boot script). At the very least, remove the unused transaction logs with msdb archive.

 Table 12-9
 msadm_bulkadd Options

Option	Description
-d domain	Specify a non-default domain in which the accounts are created. It is not necessary to use the -d flag in single-domain mode.
-f config file	Specify an non-default location for the M-Store configuration file.
-n	Do not create a mailbox for the user. The user's inbox is created by default.
-0	All command line options are used to override the fields in the given data files.
-d	Specify a default quota in kilobytes for all accounts we create. A quota of 0 signifies that no quota is to be assigned.
-v	Display the datafile lines as interpreted.

If -0 is not given, command line option values are used only if the corresponding field is not present in the data files.

If -d is not given, then the domain specified in the configuration as default-domain is assumed.

Data Format

msadm_bulkadd assumes the data files contain lines of the form: <domain>:<user>:<passwd>:<quota>:<inbox>:\n

where:

<domain></domain>	is the domain.
<user></user>	is the username.
<passwd></passwd>	is the user's password.
<quota></quota>	is the user's assigned quota in kilobytes.
<inbox></inbox>	is a flag with values '1' for creating the inbox, '0' for no inbox.

If a field value is not specified, then the default given on the command line is used. If a specified domain does not exist, it will be created. Lines of the form <*domain*>:::<*quota*>:\n will create the specified quota. If the *quota*> field is empty, no quota will be assigned (unless defaulted by the -q flag). If a specified domain does not exist it will be created.

If the configuration option admin-append-domain-auth is enabled and the domain does not match the default-domain configuration option, then the authentication account is of the form *user@domain*. Otherwise the authentication account is just *user*.

Example

Add the users in the given data file. All users not specified with a domain will be added to the default-domain as specified in the configuration file.

msadm bulkadd data

Add the users given in the data file. All users not specified with a domain are assumed to be of the domain example.com. All users not specified with a quota are assigned a quota of two megabytes.

	msadm_bulkadd -d example.com -q 2000 <i>data</i>	
	Add the users given in the data file. All users (with or without a specified domain) are assumed to be of the domain example.com. All users (with or without a specified quota) are assigned a quota of two megabytes.	
	msadm_bulkadd -O -d example.com -q 2000 <i>data</i>	
Files		
	/etc/md/store/ms.conf The default M-Store configuration file.	
See Also		
	ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10	
	msadm_bulkdel, "Delete Multiple Domains and Users (msadm_bulkdel)" on page 128	
	msadm_tclsh, "IM-Store Administration Command Interpreter (msadm_tclsh)" in Chapter 12	
	msdb_backup,"Database Backup Tool (msdb_backup)" on page 131	
	msdb_recover, "Database Recovery Tool (msdb_recover)" on page 136	
	rc.m-store, "M-Store rc.m-store Script" in Chapter 10	

Delete Multiple Domains and Users (msadm_bulkdel)

Synopsis

msadm_bulkdel [-f config_file] datafile

msadm_bulkdel reads user information from a given data file and deletes account and messages for each user (or domain). User and domain deletion is permanent and cannot be reversed; please use with care.

It is highly recommended that msdb_backup be run after bulk deleting users to safeguard new data and to clean the database transaction logs. If the transaction logs are not cleaned, there may be very long waits when running database recovery (as is usually done at boot time through the rc.mdstore boot script). At the very least, remove the unused transaction log files with msdb_archive.

Table 12-10msadm_bulkdel Options

Option	Description
-f config_file	Specify a non-default location for the M-Store configuration.

Data Format

msadm_bulkdel assumes the data files contain lines of the form:
<user>@<domain>

If the *<user>* field is empty, the entire domain will be deleted.

Example

msadm bulkdel data

Remove the users in the *data* file.
Files /etc/md/store/ms.conf The default M-Store configuration file. See Also ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10 msadm_bulkdel, "Delete Multiple Domains and Users (msadm_bulkdel)" on page 128 msadm_tclsh, "IM-Store Administration Command Interpreter (msadm_tclsh)" on page 114 msdb_backup, "Database Backup Tool (msdb_backup)" on page 131 msdb_recover, "Database Recovery Tool (msdb_recover)" on page 136 rc.m-store, "M-Store rc.m-store Script" in Chapter 10

Database Management Utilities

These tools are for the various database activities required to ensure the reliable operation of M-Store.

Database Archive Tool (msdb_archive)

Synopsis

msdb archive [-alsv] [-f config]

msdb_archive writes the pathnames of the log files that are no longer involved in active transactions. These logs, and the tables, may then be copied to backup media in case of corruption or system failures. The log files may be deleted after they are backed up to reclaim disk space. msdb_archive must be invoked as the superuser or the runtime-user as defined in the configuration file.

The msdb_archive utility attaches to one or more of the Berkeley DB shared memory regions. In order to avoid region corruption, it should always be given the chance to

detach and exit gracefully. To cause msdb_archive to clean up after itself and exit, send it an interrupt signal (SIGINT).

The proper procedure for archiving the database is given in msdb_backup. msdb_archive exits 0 on success, and >0 if an error occurs

Option Descriptions Write pathnames as absolute pathnames instead of relative to the database -a home. -f config Specify the path of an alternative M-Store configuration file. Write the pathnames of all database log files, whether or not they are involved -1 in active transactions. Write the pathnames of all database files that need to be archived in order to - S recover the database from catastrophic failure. If any of the database files have not been accessed during the lifetime of the current log files, msdb archive will not include them in the output. Run in verbose mode, listing the checkpoints in the log files as they are -v reviewed.

Table 12-11 msdb_archive Options

Example

List the absolute pathname of all of files not involved in active transactions. These may be deleted to reclaim disk space.

msdb_archive -a

List all of the log files for archive purposes.

msdb archive -1

Verbosely list all the log files not involved in active transactions.

msdb_archive -v

Files		
	/etc/md/store/ms.conf	The default M-Store configuration file.
	<i>ms-path</i> /database	The default database home, where <i>ms-path</i> is defined in the ms.conf file.
	<i>ms-path</i> defaults to /var/md/store	
See Also		
	<pre>ms.conf, "Message Store Configuration (m</pre>	ns.conf)" in Chapter 10
	msdb_backup, "Database Backup Tool (ms	db_backup)″ on page 131
	msdb_checkpoint, "Database Checkpoint	t Tool (msdb_checkpoint)" on page 134
	msdb_recover, "Database Recovery Tool ((msdb_recover)" on page 136
	msdb_restore, "Database Restore-From-E	Backup Tool (msdb_restore)" on page 138
	Chapter 9, "File and Directory Layouts"	

Database Backup Tool (msdb_backup)

Synopsis

msdb_backup

msdb_backup provides a sample shell script that may be used to create live backups of the M-Store database. msdb_restore may be used to restore this backup in the event of a catastrophic failure.

msdb_backup will make a backup of the current database tables and logs in a subdirectory of /var/md/store/backup named by date and time. The default directory structure of a backup is:

Table 12-12 Default Directory Structure of a Backu	ıp
--	----

Path	File Name
/var/md/store/backup/MSDB_Backup_< <i>timestamp</i> >	.db
	log. <log_number></log_number>

Upon successful termination, the directory should be moved to backup media for archival purposes.

The msdb_backup script is only a sample backup script that can be used as a base for administrators to write their own customized backup scripts. A successful backup must include the following sequence of events:

- 1. Force a checkpoint with msdb_checkpoint (recommended for non-live backups; this will not affect live backups).
- 2. Backup all database table files.
- 3. Use msdb_archive to determine which log files need to be backed up.
- 4. Backup the required log files.

msdb_backup defines a number of paths in the PUBLIC DEPENDENCIES section of the script which may need to be changed to reflect any changes made from the default M-Store installation. The ms.conf file will contain any changed values.

After copying the transaction log files, msdb_backup deletes those that are not involved in active transactions.

Example

msdb_backup

Files

/etc/md/store/ms.conf
/var/md/store/backup

The default M-Store configuration file. The default M-Store database backup directory.

See Also

ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10
msdb_archive, "Database Archive Tool (msdb_archive)" on page 129
msdb_checkpoint, "Database Checkpoint Tool (msdb_checkpoint)" on page 134
msdb_restore, "Database Restore-From-Backup Tool (msdb_restore)" on page 138
Chapter 9, "File and Directory Layouts"

Database Checkpoint Tool (msdb_checkpoint)

Synopsis

```
msdb_checkpoint [-1dv] [-f config] [-k kbytes] [-p min]
```

msdb_checkpoint monitors the message store database transaction logs and periodically checkpoints them. msdb_checkpoint may also be invoked as a daemon process. msdb_checkpoint must be invoked as the superuser or the runtime-user as defined in the configuration file.msdb_checkpoint is normally invoked from the storemgr daemon process as part of the set of managed server processes that make up a running message store. All stop and restart operations for msdb_checkpoint should be performed using the rc.m-store boot script.

msdb_checkpoint attaches to one or more of the message store database shared memory regions. In order to avoid region corruption, it should always be given the chance to detach and exit gracefully.

If msdb_checkpoint was invoked by storemgr, then the server cannot be independently shut down, as storemgr will automatically restart it. To shut down msdb_checkpoint , you must use the rc.m-store boot script.

msdb_checkpoint does not attempt to create the message store database shared memory regions if they do not already exist.msdb_test is used to create the region first, and then msdb_checkpoint is started.

msdb_checkpoint exits 0 on success, and >0 if an error occurs.

At least one of the -1, -k, and -p options must be specified. Both -1 and -d cannot be specified together.

Option	Description
-1	Checkpoint the log once and exit.
-d	Run as a daemon process, logging all output to the $syslogdLOG_MAIL$ facility.
-f config	Specify the path of an alternative message store configuration file.
-k <i>Kbytes</i>	Checkpoint the database at least as often as every <i>Kbytes</i> of log file are written.

 Table 12-13
 msdb
 checkpoint
 Options

	Table 12-13	continued) msc	db_checkpoint	Options	
	Option	Description			
	-p min	Checkpoint the da	tabase at least ev	ery min minutes.	
	-v	Write the time of e	each checkpoint to	o the standard out	tput or syslog.
Signals					
	msdb_checkp where the ms- to that proces	oint stores its proc path variable is de s ID will allow you msdb_checkpoint	cess ID in the file efined in the M-S u to control vari was run standal	e ms-path/run/ Store configurat: ous runtime fur one, sending SIG	'msdb_checkpoint.lock, ion file. Sending signals actions in the server.
	stop it. If msc storemgr to re	lb_checkpoint was estart it.	invoked by stor	remgr then send	ling SIGTERM will cause
Example					
	Checkpoint th	e log once and exi	it. Mostly used l	before archiving	; the database.
	msdb_check	point -1			
	Run as daemo log file are wr	on process and cheo itten.	ckpoint the log a	at least as often a	as every four kilobytes of
	msdb_check	point -d -k 4			
	Run as a daer checkpoint w	non process and cl ill appear in the sy	heckpoint the lo rslog output.	g at least every	hour. The time of the
	msdb_check	point -dv -p e	60		

Files		
	/etc/md/store/ms.conf	The default M-Store configuration file.
	<i>ms-path</i> /database	The default database home, where <i>ms-path</i> is defined in the ms.conf file.
	<i>ms-path</i> /run/msdb_checkpoint.lock	The lock file containing the process ID of the running msdb_checkpoint process.
	defaults to <i>ms-path</i> /var/md/store	
See Also		
	ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10
	<pre>msdb_test, "Database Test Tool (msdb_test)" on</pre>	page 140
	rc.m-store, "M-Store rc.m-store Script" in Chap	oter 10
	storemgr, "Store Manager (stormgr)" in Chapter	: 10
	Chapter 9, "File and Directory Layouts"	

Database Recovery Tool (msdb_recover)

Synopsis

msdb_recover [-cv] [-f config]

msdb_recover must be executed after an unexpected application, database, or system failure to restore the database to a consistent state. All committed transactions are guaranteed to appear after msdb_recover has run, and all uncommitted transactions will be completely undone. msdb_recover must be invoked as the superuser or the runtime-user as defined in the configuration file.

In the case of catastrophic failure, an archival copy or snapshot of all database files must be restored along with all of the log files written since the database file snapshot was made. (If disk space is a problem, log files may be referenced by symbolic links). For further information on creating a database snapshot, see "Database Backup Tool (msdb_backup)" on page 131. For further information on performing a recovery, see "Database Recovery Tool (msdb_recover)" on page 136.

msdb_recover exits 0 on success, and >0 if an error occurs.

If the failure was not catastrophic, the files present on the system at the time of failure are sufficient to perform recovery.

If log files are missing, msdb_recover will identify the missing log file(s) and exit on fail, in which case, the missing log files need to be restored and recovery performed again.

The msdb_recover utility attaches to one or more of the Berkeley DB shared memory regions. In order to avoid region corruption, it should always be given the chance to detach and exit gracefully. To cause msdb_recover to clean up after itself and exit, send it an interrupt signal (SIGINT).

If there are many existing transaction log files, msdb_recover may take a great deal of time to execute. This may give the appearance of being hung-up, even though it is continuing to function properly. This is common after doing bulk additions or deletions of users. msdb_archive may be used to list log files that may backed up and deleted.

Rarely, the transaction logs may become corrupted and cause all applications to hang at startup, and msdb_recover crashes due to a segfault. This is a database bug. The work-around is to delete all transaction log files and run msdb_test. Never attempt to do so on a live system.

 Table 12-14
 msdb_recover Options

Option	Description
-C	Failure was catastrophic.
-f config	Specify the path of an alternative message store configuration file.
-v	Run in verbose mode.

Example

Verbosely recover the database. This is performed at startup by the rc.m-store boot script to ensure the consistency of the database before starting imapd or any other M-Store applications. The command is equivalent to msdb_test -r.

	msdb_recover -v	
	Verbosely recover the database after a the database. This is performed by ms previously archived database.	catastrophic failure and subsequent restoration of db_restore as the final step in restoring a
	msdb_recover -c	
Files		
	/etc/md/store/ms.conf	The default M-Store configuration file.
	<i>ms-path</i> /database	The default database home, where <i>ms-path</i> is defined in the ms.conf file.
	<i>ms-path</i> defaults to /var/md/store on all systems.	
See Also		
	ms.conf, "Message Store Configurat	ion (ms.conf)" in Chapter 10
	msdb_archive, "Database Archive]	Fool (msdb_archive)" on page 129
	msdb_backup, "Database Backup To	ol (msdb_backup)" on page 131
	msdb_checkpoint, "Database Chec	kpoint Tool (msdb_checkpoint)" on page 134
	msdb_restore, "Database Restore-F	From-Backup Tool (msdb_restore)" on page 138
	msdb_test, "Database Test Tool (ms	db_test)" on page 140
	Chapter 9, "File and Directory Layout	ts"

Database Restore-From-Backup Tool (msdb_restore)

Synopsis

msdb_restore backup_path

msdb_restore provides a sample shell script that can be used to restore backups of M-Store's database that were created with msdb_backup.

	msdb_restore takes a single argument <i>backup_path</i> which must refer to the directory containing the archived database tables and transaction logs.		
	msdk adm sequ	p_restore is only a sample backup script th inistrators to write their own customized ba ence of events for restores is:	at can be used as a base for ackup restore scripts. The minimum
	1.	Cleanly shutdown all M-Store database rel- or all of the following: an imapd/pop3d shut tools are currently running, and stopping t	ated applications. This may entail any tdown file, ensuring no administration he rc.mdstore script.
	2.	Empty, or backup, the M-Store transaction	on_log and data directories.
	3.	Copy all archived data files (*.db) into the files (log.*) into the transaction_log dir	data directory. Copy all archived log rectory.
	4.	${\tt msdb_recover}$ -c to finish restoring the data	atabase.
	Any	existing database directories are renamed to	0:
	<diri< td=""><td>name>.asof<today's date="">.</today's></td><td></td></diri<>	name>.asof <today's date="">.</today's>	
	msdb scrip M-St	p_restore defines a number of paths in the of which may need to be changed to reflect a core installation. The ms.conf file will conta	PUBLIC DEPENDENCIES section of the any changes made from the default in any changed values.
Example	msdł	o_restore backup_path	
Files			
	/etc	:/md/store/ms.conf	The default M-Store configuration file.
	/var	r/md/store/database/data	The default M-Store database data directory.
	/var	/md/store/database/transaction_log	The default M-Store database log directory.
See Also			
	ms.	conf, "Message Store Configuration (ms.co	nf)" in Chapter 10
	msdl	o_archive, "Database Archive Tool (msdb	_archive)" on page 129

msdb_recover, "Database Recovery Tool (msdb_recover)" on page 136
msdb_restore, "Database Restore-From-Backup Tool (msdb_restore)" on page 138
Chapter 9, "File and Directory Layouts"

Database Test Tool (msdb_test)

Synopsis

msdb_test [-rv] [-f config]

msdb_test tests the message store database by quickly opening and closing the database tables, recovering any files if necessary. Any errors are written to standard error. msdb_test must be invoked as the superuser or the runtime-user (e.g., sms) as defined in the configuration file.

Certain deadlock conditions may cause msdb_test to hang while opening the database. In such cases, terminate msdb_test with ctrl-c and rerun msdb_test with the -r flag.

msdb_test exits 0 on success, and 1 if an error occurs

msdb_test will not run if any database files are missing, in such a case a backup containing all database files must be restored.

Table 12-15msdb_test Options

Option	Description
-f config	Specify the path of an alternative message store configuration file.
-r	Recover the database before testing. This should be used if starting M-Store from a boot script to cleanup the database in case it was not cleanly shutdown. This flag is equivalent to executing msdb_recover and is only be given by the M-Store runtime user. Please see msdb_recover, "Database Recovery Tool (msdb_recover)" on page 136, for possible risks associated with this flag.
-v	Verbosely display the state of the database upon exiting.

Example		
	Test the database and with the database the	display a message regarding its state. If there are any problems y will be echoed to standard error.
	msdb_test -v	
	Verbosely test the data to ensure the consister applications. This com	abase. This is performed at startup by the rc.m-store boot script ncy of the database before starting imapd or any other M-Store nmand is equivalent to msdb_recover -v.
	msdb_test -r	
	Verbosely test the data	abase and check for any deadlocks.
	msdb_test -lv	
Files		
	/etc/md/store/ms.conf	The default M-Store configuration file.
	<i>ms-path</i> /database/	Default database home, where <i>ms-path</i> is defined in the

ms-path defaults to /var/md/store

See Also

ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10
msdb_recover, "Database Recovery Tool (msdb_recover)" on page 136
rc.m-store, "M-Store rc.m-store Script" in Chapter 10
Chapter 9, "File and Directory Layouts"

ms.conf file.

M-Store Mailbox Cache Files Reconstruction (reconstruct)

Synopsis

reconstruct -r esys.ca "user/foobar"

reconstruct rebuilds one or more IMAP message store mailbox cache files within a given domain. It can be used to recover from almost any sort of data corruption. Since reconstruct can create new cache files it can be run as the M-Store runtime user.

When reconstruct finds existing header and index files, it attempts to preserve any data in them that is not derivable from the message files themselves. The state that reconstruct attempts to preserve includes: the flag name, flag state, and internal date. reconstruct derives all other information from the message files.

The mailbox arguments must be fully qualified IMAP mailbox names and may need to be quoted on the command line if the name contains shell-specific characters.

 Table 12-16
 reconstruct Options

Option	Description
-f config_file	Specify an alternate location for M-Store's configuration file.
-r	Recursively reconstruct all sub-mailboxes of the mailboxes or mailbox-prefixes given as arguments. If no mailbox arguments are given, all mailboxes within the specified domain will be reconstructed.
-u	Reconstruct a specific user's mailbox or mailboxes.
-v	Display program version information on standard error, then exit.

Example

reconstruct -r esys.ca "user/foobar"

This command recursively reconstructs all cache files for the personal hierarchy of user foobar@esys.ca

Table 12-17reconstruct Examples

Command Example	Description
reconstruct -r example.com	Reconstruct all mailboxes in the example.com domain.
reconstruct -r -u joe example.com	Reconstruct all of joe@example.com's mailboxes.

	Table 12-17 (continued) reconstruct Examples		
	reconstruct -u joe example.com	INBOX	Reconstruct only joe@example.com's mailbox.
	reconstruct -r -u joe example.c	om pub	Reconstruct joe@example.com's pub folder and all sub-folders.
	reconstruct foo.com admin		Reconstruct the shared folder admin in the foo.com domain.
	reconstruct -r example.com admi	n	Reconstruct the shared folder admin and all sub-folders in the example.com domain.
Files			
	/etc/md/store/ms.conf	The defa	ult M-Store configuration file.
	mailboxpath/fdb.*	Mailbox	cache files.
See Also			
	ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10		
	Chapter 9, "File and Directory Layouts"		

M-Store Database Creation (msdb_upgrade)

Synopsis

msdb_upgrade [-f config]

msdb_upgrade creates a new message store database or upgrades an existing database to the current revision. All files must be present for the upgrade. File locations are determined from the configuration file. Any errors are written to standard error.

msdb_upgrade must be executed before using the message store for the first time. By default, all the necessary store databases are created during installation. msdb_upgrade must be invoked as the superuser or the runtime-user as defined in the configuration file.

msdb_upgrad containing al time as any o success and	will not run if any database files are missing, In such a case, a backup latabase files must be restored. msdb_upgrade must not be run at the sam ner M-Store process that accesses the database. msdb_upgrade exits 0 or f an error occurs.	
Table 12-18	msdb_upgrade Options	
Option	Description	
E confic	Specify the path of an alternative message store configuration file	

Files

See Also

/etc/md/store/ms.conf	The default M-Store configuration file.
<i>ms-path</i> /database/	Default database home, where <i>ms-path</i> is defined in the ms.conf file.
<i>ms-path</i> defaults to /var/md/store	
ms.conf, "Message Store Configurat	tion (ms.conf)" in Chapter 10

Chapter 9, "File and Directory Layouts"

Mail Delivery to M-Store Mailbox Tool (deliver)

deliver Synopsis

deliver [-g] [-f config_file] [-F lmtp-mail-from] receipient

deliver will not run if any database files are missing; in such a case a backup containing all database files must be restored.

deliver reads a RFC 822 message from standard input and delivers it to the receipient.

By default, deliver rejects messages containing non-ASCII characters in the message headers. To maintain backward compatibility with MUA software that does not properly MIME-encode non-ASCII header data, add the line **allow8bitheaders on** to ms.conf. This will force deliver to accept the message by stripping the high-bit from any non-ASCII characters.

deliver delivers to a user's INBOX. To deliver to a specific mailbox, append the mailbox name to the recipient's local name. For example:

joe+important/March2000@foobar.com

will deliver the message to the mailbox: user/joe/important/March2000, where joe@foobar.com is a valid user in the message store. To deliver a shared mailbox, append the mailbox name to *lmtp-shared-name* name as defined in ms.conf. For example:

shared+bugreport@foobar.com

This method of delivery is known as Plus-Addressing. Plus-Addressing is not a standard, but it does result in a valid RFC822 address:

Option	Description		
-g	Deliver the message regardless of the recipient's quota. The configuration option lmtp-enable-overquota-delivery must be enabled for overquota delivery to succeed.		
-f config_file	Specify a non-default location for M-Store's configuration file.		
-F lmtp-mail-from	Use <i>lmtp-mail-from</i> as the address in the LMTP MAIL FROM command. This will also insert a Return-Path: <i>lmtp-mail-from</i> header into the message.		

 Table 13-1
 deliver Options (required)

Note: If the -F option is not specified, then the *lmtp-mail-from* address is read from the Return-Path: header in the message itself.

If any userid arguments are supplied, a copy of the message is delivered into each of the named user's INBOX folders.

Examples

Deliver a message to joe@example.com:

deliver joe@example.com

Deliver a message with a return address of fred@foobar.com to the mailbox user/joe/important/March2000 in the example.com domain:

deliver -F fred@foobar.com+important/March2000@foobar.com

Deliver a message with a return address of fred@foobar.com into the shared mailbox bugreports in the foobar.com domain:

deliver -F fred@foobar.com shared+bugreports@foobar.com

See Also

lmtpd, "LMTP Delivery Server (lmtpd)" in Chapter 11
ms.conf, "Message Store Configuration (ms.conf)" in Chapter 10
Chapter 9, "File and Directory Layouts"

Numbers

103664, 95

A

Accessing Domain Administration, 57 administering M-Store remotely, 57 domain administration link, 58 httpd server, 57 URL for the Administration Interface, 57 Accessing Site Administration, 49 administration permission levels, 50 default administration URLs, 51 site administration link, 50 URL for, 49 web administration defaults file, 51 Account Management, 67 User Passwords, 67 Add Shared Mailboxes, 63 basic information, 63 create a new user, 63 existing user, 63 mailbox list, 63 mailbox rights, 63 quota information, 63 quota size, 63 Add Users, 59 auth ID, 60 create internal authentication account, 59, 60 create personal folder space, 59, 60

enable internal authentication, 60 enable internal authentication account, 59 password, 60 quota, 60 user name @, 59 Add Users in Bulk to M-Store, 125 Adding Domains, 53 allow anonymous login, 53 enable domain, 53 quota size, 53 Adding Site Administrators, 55 add administrator, 55 ms.conf file, 55 Application Runtime Control, 21 starting, 21 example, 21 Irix 6.5, 113 Red Hat Linux 6.0, 113 Solaris 2.5.1/2.7, 113 stopping, 21, 113, 114 Red Hat Linux 6.0, 114 Solaris 2.5.1/2.7, 114 authproxyd account migration, 102 authentication mechanisms, 101 configuration variables, 101 configuration, 99 options, 100 configuration options (table), 100 files, 99 logging, 98 options, 98

protocol, 98 see also, 99 signals, 98 synopsis, 97 authproxyd Configuration options, 37, 90

В

bootscript locations (table), 72

С

Capacity Planning, 3 M-Sendmail mail transfer agent (MTA), 4 M-Store - message service, 3 planning summary, 5 server component requirements, 4 server performance, 3 Change Access Rights, 65 delete mailbox rights, 65 mailbox rights, 65 modify shared mailbox dialogue, 65 shared mailbox list, 65 Change Mailbox Quota, 64 Change Passwords, 62 authentication information, 62 password, 62 user list, 62 verify password, 62 Change Quotas, 61 modify user dialogue, 61 quota size, 61 set to zero, 61 user list, 61 Change User Password Page, 67 authentication ID, 67 change passwords, 67

users change own password, 67 verification, 67 Changing Quotas, 54 domain name, 54 quota size (in MB), 54 Configuration Files, 71 Conventions, xvi Correcting File Permissions, 43

D

Database Administration, 22 backups, 24 recovery, 28 restore, 26 validation, 22 Database Corruption, 45 transaction logs, 46 Database Files, 80 Database Files (table), 80 Database Organization, 16 Default directory paths, 71 Delete Shared Mailboxes, 64 delete mailboxes button, 64 existing mailbox quota, 64 shared mailbox, 64 Delete Users, 61 delete users button, 61 Deleting Domains, 54 Deleting Site Administrators, 56 deliver, 145 example, 146 options, 146 see also, 147 synopsis, 145 Domain Administration, 57, 58 accessing domain administration, 57

different from specified domain, 59 domain administration, 58 domain administration page, 59 list of domains, 59 shared mailbox management, 59, 62 user accounts, 59 Domain Management, 52

add domain dialogue, 53 adding domains, 53 apply filter field, 53 changing quotas, 54 deleting domains, 54 domain management sort order, 53 domain name, 53 navigation arrows, 53 Quota Limit(MB), 52 Domains, 18

auth ID, 59

main tools. 59

Е

Electronic Mail Infrastructure, 13

F

File Locations configuration files, 71 database files, 80 executable support files, 73 location of bootscripts (platform), 72 runtime control, 72 runtime data files, 75 database files, 80 Filesystem Parameters, 40 inode counts, 40 inodes per mailbox, 40

007-3878-001

н

Hardware Requirements, 5 active processes, 5 assumptions, formulae, 6 concurrent processes, 5 drive space requirements, 7 important file locations, 7 key server components, 6 usage assumptions, 6

L

imapd files, 105 IMAP4 standard extensions, 105 access control lists, 106 protocol extensions, 106 quota implementation, 106 logging, 104 options, 104 see also, 105 signals, 104 synopsis, 103 Inodes per mailbox, 40

L

Linux Platform System Parameters, 7 lmptd logging, 108 options, 108 lmtpd configuration, 109 files, 109 see also, 109 signals, 108 synopsis, 107

Μ

Mail Delivery to M-Store Mailbox Tool, 145 Mailbox Cache Recovery, 43 Mailbox Hierarchy, 63 add rights, 64 administrator, 64 example, 63 modify rights, 64 read, 64 read/write, 64 Mailbox Organization, 17 Message Server (imapd) IMAP4 standard extensions supported RFCs, 105 protocol extensions capability, 106 Messaging System Overview, 13 component overview, 13 msadm_bulkadd (source) data format, 126 example, 126 files, 127 options, 125 see also, 127 synopsis, 125 msadm_bulkdel (source) data format, 128 example, 128 options, 128 see also, 129 synopsis, 128 msadm_tclsh account management commands, 117 account management commands (table), 117 account mapping (alias) commands, 120 account mapping commands (table), 120 domain administration commands, 116 domain management commands (table), 116 example

add a new site administrator, 124 create a domain and add a first user, 124 generic commands, 115 generic commands (table), 115 options, 114 see also, 124 shared mailbox management commands, 121 (table), 123 site administration commands, 115 site administration commands (table), 115 synopsis, 114 user mailbox management commands (table), 121 ms-assignment-policy rules, 84 ms.conf authproxyd configuration, 37,90 files, 38, 91 optional configuration, 35, 87 optional entries, 35, 87 recommended configuration, 34, 86 options, 34, 86 Required Configuration, 32 required configuration, 84 options, 32, 84 SASL Plugin Examples, 34 SASL plugin options, 33, 85 SASL plugin options, example, 34, 85 see also, 38, 91 msdb_archive example, 130 files, 131 options, 130 see also, 131 synopsis, 129 msdb_backup directory structure, 24, 132 example, 25, 132 files, 25, 133 see also, 25, 133 sequence of events, 132 synopsis, 131

msdb_checkpoint example, 135 files, 136 options, 134 see Also, 136 signals, 135 synopsis, 134 msdb_deadlock files, 46 see also, 46 msdb_recover, 28 example, 29, 137 files, 29, 138 options, 29, 137 see also, 29, 138 synopsis, 136 msdb_restore, 26 example, 26, 139 files, 27, 139 see also, 27, 139 sequence of events, 139 synopsis, 138 msdb_test, 22 example, 23, 141 files, 23, 141 options, 22, 140 see also, 23, 141 synopsis, 140 msdb_upgrade options, 144 msdm_tclsh shared mailbox management commands, 123 M-Store Database Files, 80 M-Store File Locations /etc/md/store/, table, 71 /usr/local/md/, table, 73 /var/md/store/, table, 75 MTA, Sendmail, 4

Ν

Network Requirements, 7 Linux platform system parameters, 7

0

Operating System Parameters, 41 Linux, 7, 41

Ρ

Physical Mailbox Files, 81 binary mailbox files, 81 pop3 APOP, 110 pop3d files, 112 logging, 111 options, 110 protocol extensions, 111 see also, 112 signals, 111 synopsis, 110 Preface Conventions, xvi Preparation for Installation, 8 work sheet, 8 Provide Domain Administrative Rights, 62 add/modify/delete, 62 administrator check-box, 62 domain rights, 62

R

rc.m-store Script example, 93

files, 93 parameters, 92 see also, 93 synopsis, 92 reconstruct command examples, 44, 142 example, 44, 142 examples, 44 files, 45, 143, 144 options, 44, 142 see also, 45, 143, 144 synopsis, 141, 143 Runtime Control, 72

S

Scalability. See Volumetrics Shared Mailbox Management, 62 add shared mailboxes, 63 change access rights, 65 change mailbox quota, 64 delete shared mailboxes, 64 mailbox hierarchy, 63 Site Administration, 49 Auth ID, 52 domain management, 52 msadm_tclsh, 51 navigation, 51 site administrators, 55 Site Administrators, 55 adding site administrators, 55 deleting site administrators, 56 Store Component Overview, 14 servers, 15 authproxyd, 15 imapd, 15 lmtpd, 15 pop3d, 15 Store Concepts, 18

mailbox access control, 20 mailbox hierarchy, 19 partitions, 18 quotas, 19 user accounts, 20 Store Configuration, 31 store manager synopsis, 39 store manager (stormgr) logging, 94 see also, 94 signals, 94 synopsis, 93

Т

Typographic and Keyboard Conventions, xvi

U

User Accounts, 59 add users, 59 Change Passwords, 62 Change Quotas, 61 delete users, 61 provide domain administrative rights, 62 user accounts page, 59 User Passwords, 67 change user password page, 67

V

Volumetrics, 3

W

web administration defaults file, 51 Web Administration Interface administration permission levels(table) change user password, 50 domain administration, 50 site administration, 50 site administration login procedures, 52 site administrators domain management, 52