Sun Java™ System

Messaging Server 6
管理指南

2005Q1

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

文件号码 819-1056

版权所有 © 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 保留所有权利。

对于本文档中介绍的产品， Sun Microsystems, Inc. 对其所涉及的技术拥有相关的知识产权。需特别指出的是 （但不局限于此），这些知识产权可能包含在 http://www.sun.com/patents 中列出的一项或多项美国专利，以及在美国和其他国家 / 地区申请的一项或多项其他专利或待批专利。

本产品包含 Sun Microsystems, Inc. 的机密信息和商业机密。未经 Sun Microsystems, Inc. 的事先明确书面许可，不得使用、泄露或复制。

美国政府权利 — 商业软件。政府用户应遵循 Sun Microsystems, Inc. 的标准许可协议，以及 FAR （Federal Acquisition Regulations，即 “联邦政府采购法规”）的适用条款及其补充条款。

此发行版本可能包含由第三方开发的内容。

本产品的某些部分可能是从 Berkeley BSD 系统衍生出来的，并获得了加利福尼亚大学的许可。 UNIX 是 X/Open Company, Ltd. 在美国和其他国家 / 地区独家许可的注册商标。

Sun、Sun Microsystems、Sun 徽标、Java、Solaris、JDK、Java Naming、Directory Interface、JavaMail、JavaHelp、J2SE、iPlanet、Duke 徽标、Java 咖啡杯徽标、Solaris 徽标、SunTone Certified 徽标以及 Sun ONE 徽标是 Sun Microsystems, Inc. 在美国和其他国家 / 地区的商标或注册商标。

所有 SPARC 商标的使用均已获得许可，它们是 SPARC International, Inc. 在美国和其他国家 / 地区的商标或注册商标。标有 SPARC 商标的产品均基于由 Sun Microsystems, Inc. 开发的体系结构。

Legato 和 Legato 徽标是 Legato Systems, Inc. 的注册商标， Legato NetWorker 是 Legato Systems, Inc. 的商标或注册商标。 Netscape Communications Corp 徽标是 Netscape Communications Corporation 的商标或注册商标。

OPEN LOOK 和 Sun(TM) 图形用户界面是 Sun Microsystems, Inc. 为其用户和许可证持有者开发的。Sun 感谢 Xerox 在研究和开发可视或图形用户界面的概念方面为计算机行业所做的开拓性贡献。 Sun 已从 Xerox 获得了对 Xerox 图形用户界面的非独占性许可证，该许可证还适用于实现 OPEN LOOK GUI 和在其他方面遵守 Sun 书面许可协议的 Sun 许可证持有者。

本服务手册所介绍的产品以及所包含的信息受美国出口控制法制约，并应遵守其他国家 / 地区的进出口法律。严禁将本产品直接或间接地用于核设施、导弹、生化武器或海上核设施，也不能直接或间接地出口给核设施、导弹、生化武器或海上核设施的最终用户。严禁出口或转口到美国禁运的国家 / 地区以及美国禁止出口清单中所包含的实体，包括但不限于被禁止的个人以及特别指定的国家 / 地区的公民。

本产品包括由 Carnegie Mellon University 的 Computing Services (http://www.cmu.edu/computing/) 开发的软件。

文档按 “原样”提供，对于所有明示或默示的条件、陈述和担保，包括对适销性、适用性和非侵权性的默示保证，均不承担任何责任，除非此免责声明的适用范围在法律上无效。

目录

表 **21**

图 **27**

前言 **29**

目标读者 30
阅读本书之前 30
本书的结构 30
本指南中使用的约定 32
印刷约定 32
符号 32
默认路径和文件名 33
命令行提示符 33
相关文档 33
Messaging Server 文档 33
Communications Services 文档 34
本指南联机文档所在的位置 35
访问 Sun 资源联机文档 35
联系 Sun 技术支持 36
相关的第三方 Web 站点参考 36
Sun 欢迎您提出意见 36

第 1 章 安装后任务和布局 **37**
创建 UNIX 系统用户和组 38
为 Messaging Server 配置准备 Directory Server 39
comm_dssetup.pl 的位置 39
comm_dssetup.pl 要求 40
运行 comm_dssetup.pl 脚本 41
创建初始 Messaging Server 运行时配置 49
Messaging Server 先决条件 49

Messaging Server 配置核对表 49
运行配置程序 49
执行无提示安装 53
针对 Directory Server 拷贝安装 Messaging Server 54
安装 Messaging Server 置备工具 55
Delegated Administrator for Messaging 55
LDAP 置备工具 57
SMTP 中继阻止 58
在重新引导后启用启动 60
处理 sendmail 客户端 60
Solaris 8 61
Solaris 9 及更高版本 62
配置 Messenger Express 和 Communications Express 邮件过滤器 63
性能和调节 63
安装后的目录布局 64
安装后的端口号 65

第 2 章 升级到 Sun Java Systems Messaging Server 67
开始之前 67
升级过程概述 68
创建升级文件以更新配置 68
关于升级文件 68
运行 UpgradeMsg5toMsg6.pl Perl 脚本 70
运行升级实用程序 71
升级实用程序概述 72
运行 do_the_upgrade.sh 实用程序 72
MTA 配置 73
configutil 参数 73
备份配置 73
mboxlist 数据库 74
迁移用户邮箱 74
要求 75
迁移说明 75

第 3 章 配置高可用性 77
群集代理安装 78
Messaging Server 和高可用性注意事项 78
使用 useconfig 实用程序 78
Veritas Cluster Server 代理安装 79
Veritas Cluster Server 的要求 80
VCS 3.5 安装和配置说明 80
MsgSrv 属性 82

Sun Cluster 代理安装 83
Sun Cluster 的要求 83
关于 HAStoragePlus 84
使用 Sun Cluster 和 HA StoragePlus 配置 Messaging Server 84
在服务器上绑定 IP 地址 88
取消配置高可用性 90
取消配置 Veritas Cluster Server 90
为 Sun Cluster 3.x 取消配置 Messaging Server HA 支持 91

第 4 章 配置一般邮件传送能力 93
修改密码 94
管理邮件用户，邮递列表和域 95
从 Messaging Server 中删除用户 95
从 Messaging Server 中删除域 96
通过 Sun ONE Console 管理 Messaging Server 96
启动和停止服务 97
在 HA 环境中启动和停止服务 97
在非 HA 环境中启动和停止服务 98
失败的服务或未响应服务的自动重新启动 101
高可用性部署中的自动重新启动 102
安排自动任务时间 103
配置问候邮件 104
设置基于域的问候邮件 105
设置用户首选语言 107
设置域首选语言 107
配置服务器站点语言 107
自定义目录查找 108
加密设置 111
设置故障转移 LDAP 服务器 111

第 5 章 配置 POP、IMAP 和 HTTP 服务 113
一般配置 114
启用和禁用服务 114
指定端口号 114
用于加密通信的端口 115
服务标题 115
登录要求 116
设置 POP 客户机的登录分隔符 116
允许不使用域名登录 116
基于密码的登录 117
基于证书的登录 117
性能参数 118

进程数量 118
每个进程的连接数量 118
每个进程的线程数量 119
切断空闲连接 120
注销 HTTP 客户机 120
客户机访问控制 120
配置 POP 服务 121
配置 IMAP 服务 123
配置 HTTP 服务 125

第 6 章 启用单点登录 (SSO) 129
用于 Sun Java System 服务器的 Access Manager SSO 130
SSO 限制和注意事项 130
将 Messaging Server 配置为支持 SSO 130
SSO 错误诊断 132
信任范围 SSO （传统） 132
信任范围 SSO 概述和定义 132
信任范围 SSO 应用程序 133
信任范围 SSO 限制 134
信任范围 SSO 部署方案示例 134
设置信任范围 SSO 136
Messenger Express 信任 SSO 配置参数 140

第 7 章 配置和管理多路复用器服务 143
多路复用器服务 143
多路复用器的优点 144
关于 Messaging Multiplexor 145
Messaging Multiplexor 的工作原理 146
加密 (SSL) 选项 147
基于证书的客户机验证 147
用户预验证 148
MMP 虚拟域 148
关于 SMTP 代理 150
设置 Messaging Multiplexor 150
配置 MMP 之前 151
多路复用器的配置 151
多路复用器文件 152
启动多路复用器 153
修改现有 MMP 153
配置 MMP 以使用 SSL 153
样例拓扑 155
MMP 任务 159

用 MMP 配置邮件访问 159
设置故障转移 MMP LDAP 服务器 159
关于 Messenger Express Multiplexor 159
Messenger Express Multiplexor 的工作原理 160
设置 Messenger Express Multiplexor 161
测试您的设置 164
管理 Messenger Express Multiplexor 164

第 8 章 MTA 概念 167
MTA 功能 167
MTA 体系结构和邮件流概述 171
分发程序 172
服务器进程的创建和终止 173
启动和停止分发程序 173
重写规则 174
通道 175
主程序和从程序 175
通道邮件队列 177
通道定义 177
MTA 目录信息 179
作业控制器 179
启动和停止作业控制器 180

第 9 章 MTA 地址转换和路由 181
直接 LDAP 算法和实现 181
域位置确定 181
本地地址的别名扩展 185
处理 LDAP 结果 189
地址反向 201
异步 LDAP 操作 203
设置摘要 204

第 10 章 关于 MTA 服务和配置 205
编译 MTA 配置 206
MTA 配置文件 206
映射文件 208
映射文件中的文件格式 210
映射操作 211
其他 MTA 配置文件 220
别名文件 221
TCP/IP (SMTP) 通道选项文件 222
转换文件 222

分发程序配置文件 222
映射文件 223
选项文件 224
调整文件 224
作业控制器文件 225
别名 231
别名数据库 231
别名文件 232
在别名文件中包含其他文件 233
命令行实用程序 233
SMTP 安全性和访问控制 233
日志文件 233
将地址由内部格式转换为公用格式 234
设置地址反向控制 235
正向查找表和 FORWARD 地址映射 237
控制传送状态通知邮件 240
构造和修改状态通知 241
自定义和本地化传送状态通知邮件 242
将生成的通知国际化 245
附加的状态通知邮件功能 246
控制邮件处理通知 252
自定义和本地化邮件处理通知邮件 252

第 11 章 配置重写规则 255
重写规则结构 256
重写规则模式和标记 257
与百分比黑客匹配的规则 259
与 Bang 式样 (UUCP) 地址匹配的规则 259
与任何地址匹配的规则 260
标记的重写规则集 260
重写规则模板 260
普通重写模板：A%B@C 或 A@B 261
重复的重写模板 A%B 261
指定的路由重写模板 A@B@C@D 或 A@B@C 261
重写规则模板中的大小写区分 262
MTA 如何将重写规则应用到地址 262
步骤 1. 提取第一个主机或域说明 263
步骤 2. 扫描重写规则 264
步骤 3. 根据模板重写地址 265
步骤 4. 完成重写进程 266
重写规则失败 266
重写后的语法检查 266
处理域文字 266

模板替换和重写规则控制序列 267
用户名和子地址替换， $U、 $0U、 $1U 270
主机 / 域和 IP 文字替换， $D、 $H、 $nD、 $nH、 $L 270
文字字符替换， $$、 $%、 $@ 271
LDAP 查询 URL 替换， $]...[..... 271
常规数据库替换， $(...) 272
应用指定的映射， ${...} 273
用户提供的例程替换， $[...] 273
单个字段替换， $&、 $!、 $*、 $# 274
唯一字符串替换 274
特定于源通道的重写规则 （$M、 $N） 275
特定于目标通道的重写规则 ($C, $Q) 275
特定于方向和位置的重写规则 ($B, $E, $F, $R) 276
特定于主机位置的重写 （$A、 $P、 $S、 $X） 276
更改当前标记值， $T 277
控制与重写 ($?) 相关联的错误消息 277
处理大量的重写规则 278
测试重写规则 278
重写规则示例 279

第 12 章 配置通道定义 281
按字母顺序列出的通道关键字 282
按功能分类的通道关键字 285
配置通道默认值 298
配置 SMTP 通道 299
配置 SMTP 通道选项 300
SMTP 命令和协议支持 300
TCP/IP 连接和 DNS 查找支持 308
SMTP 验证、 SASL 和 TLS 315
在标题中使用来自 SMTP AUTH 的已验证的地址 316
指定 Microsoft Exchange 网关通道 317
传输层安全性 317
配置邮件处理和传送 318
设置通道方向性 320
实现延迟传送日期 320
为传送失败的邮件指定重试频率。 321
用于通道执行作业的处理池 322
服务作业限制 322
设置连接事务限制 324
基于大小的邮件优先级 324
SMTP 通道线程 325
多个地址扩展 326
启用服务转换 326

配置地址处理 327
地址类型和约定 327
解释使用 ! 和 % 的地址 329
在地址中添加路由信息 329
禁用显式路由地址的重写 330
邮件出队后的地址重写 330
指定修正不完整地址时使用的主机名 331
使缺少收件人标题行的邮件合法化 331
删除非法的空收件人标题 332
启用特定于通道的反向数据库使用 332
启用限制的邮箱编码 333
生成 Return-path: 标题行 333
从信封 To: 和 From: 地址设置限制 334
处理地址标题行中的注释 334
处理地址标题行中的个人名称 335
指定别名文件和别名数据库探测 336
子地址处理 336
启用特定于通道的重写规则检查 337
删除源路由 337
必须从别名指定地址 337
配置标题处理 338
重写嵌入式标题 338
删除选定的邮件标题行 339
生成 / 删除 X-Envelope-to: 标题行 340
将日期转换为两位数或四位数 340
在日期中指定星期几 340
自动分割长标题行 341
标题对齐和折叠 341
指定标题行最大长度 342
敏感度检查 342
设置标题中的默认语言 342
附件和 MIME 处理 343
忽略 Encoding: 标题行 343
Message/Partial 邮件的自动片段整理 343
大型邮件的自动分段 344
实施邮件行长度限制 345
对邮件、配额、收件人和验证尝试次数的限制 345
对不成功验证尝试的次数的限制 346
指定绝对邮件大小限制 346
重新定向超过大小限制或收件人限制的邮件。 347
处理对超过配额用户的邮件传送 348
处理包含超过 1000 个字符的行的 SMTP 邮件 349
控制通用内容类型参数、文件名内容类型参数和内容处理参数的长度 349

对邮件收件人进行限制 349
限制标题大小 350
MTA 队列中的文件创建 350
控制邮件中多个地址的处理方式 350
将通道邮件队列分布到多个子目录中 351
设置会话限制 351
配置记录和调试 352
记录关键字 352
调试关键字 352
设置 Loopcheck 353
其他关键字 353
进程通道覆盖 353
通道操作类型 354
Pipe 通道 354
指定邮箱过滤器文件位置 354
垃圾邮件过滤器关键字 355
地址验证之后扩展之前的路由 355
NO-SOLICIT SMTP 扩展支持 358
对错误 RCPT TO: 地址设置限制 359

第 13 章 使用预定义通道 361
使用 Pipe 通道将邮件传送给程序 362
配置本地 (/var/mail) 通道 363
使用 Hold 通道临时保留邮件 364
转换通道 365
MIME 概述 366
选择用于转换处理的通信 367
控制转换处理 368
使用转换通道输出退回、删除或保留邮件 377
转换通道示例 378
自动检测 Arabic 字符集 379
字符集转换和邮件重新格式化 383
字符集转换 385
邮件的重新格式化 386
服务转换 391

第 14 章 将垃圾邮件和病毒过滤程序集成至 Messaging Server 393
将垃圾邮件过滤程序集成至 Messaging Server—操作原理 394
部署和配置第三方垃圾邮件过滤程序 394
装入和配置垃圾邮件过滤软件客户机库 395
指定要过滤的邮件 396
指定要对垃圾邮件执行的操作 401

使用 Symantec Brightmail Anti-Spam 405
Brightmail 的工作方式 405
Brightmail 要求和性能注意事项 407
部署 Brightmail 407
Brightmail 配置选项 408
使用 SpamAssassin 409
SpamAssassin 概述 410
SpamAssassin/Messaging Server 操作原理 410
SpamAssassin 要求和使用注意事项 411
部署 SpamAssassin 412
SpamAssassin 配置示例 412
测试 SpamAssassin 418
SpamAssassin 选项 420
使用 Symantec Anti-Virus Scanning Engine (SAVSE) 422
SAVSE 概述 423
SAVSE 要求和使用注意事项 423
部署 SAVSE 424
SAVSE 配置示例 424
SAVSE 选项 426
支持 Sieve 扩展 428

第 15 章 LMTP 传送 431
LMTP 传送功能 432
不带有 LMTP 的两层部署中的邮件传送处理 433
带有 LMTP 的两层部署中的邮件传送处理 435
LMTP 概述 436
配置 LMTP 传送 437
配置与 LMTP 配合使用的外来 MTA 中继 437
配置具有 LMTP 而没有 MTA 的后端存储 441
配置中继以通过 LMTP 将邮件发送到带有邮件存储和完整 MTA 的后端系统 443
在具有完整 MTA 的后端邮件存储系统中配置 LMTP 444
要执行的 LMTP 协议 445

第 16 章 休假自动邮件回复 449
休假自动回复概述 449
配置自动回复 450
在后端存储系统中配置自动回复 450
在中继上配置自动回复 451
休假自动回复操作的原理 452
休假自动回复属性 453

第 17 章 邮件过滤和访问控制 455
第 1 部分：映射表 455
使用映射表控制访问 456
访问控制映射表 — 操作 456
访问控制映射表标志 457
SEND_ACCESS 和 ORIG_SEND_ACCESS 表 460
MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射表 462
FROM_ACCESS 映射表 463
PORT_ACCESS 映射表 466
限制指定 IP 地址到 MTA 的连接 467
应用访问控制后 468
测试访问控制映射 469
添加 SMTP 中继 470
允许为外部站点进行 SMTP 中继 471
配置 SMTP 中继阻止 472
MTA 如何区分内部邮件和外部邮件 473
区分已验证用户的邮件 474
阻止邮件中继 475
使用 DNS 查找（包括用于 SMTP 中继阻止的 RBL 检查） 476
处理大量访问条目 478
第 2 部分：邮箱过滤器 481
Sieve 过滤器支持 481
Sieve 过滤概述 482
创建用户级别的过滤器 482
创建通道级别的过滤器 483
创建 MTA 范围内的过滤器 485
将已放弃的邮件路由出 FILTER_DISCARD 通道 485
调试用户级别的过滤器 486
imsimta test -exp 输出 488
imsimta test -exp 语法 489

第 18 章 管理邮件存储 491
概述 492
邮件存储目录布局 493
邮件存储如何删除邮件 496
指定管理员对存储的访问权限 497
添加管理员 497
修改管理员条目 498
删除管理员条目 498
关于共享文件夹 499
共享文件夹访问权限 500
共享文件夹任务 503
创建公用文件夹 503

更改公用文件夹的访问控制权限 504
启用或禁用共享文件夹列表 505
设置分布式共享文件夹 505
监视和维护共享文件夹数据 507
关于邮件存储配额 509
用户配额 509
域配额 510
电话学应用程序服务器的异常 510
配置邮件存储配额 512
指定默认用户配额 512
指定单个用户配额 513
指定域配额 513
部署配额通知 513
启用或禁用强制配额 516
设置宽限期 517
Netscape Messaging Server 配额兼容性模式 518
设置自动删除邮件 （过期和清除）功能 518
imexpire 操作原理 519
部署自动删除邮件功能 519
配置邮件存储分区 529
添加分区 529
将邮箱移动到其它磁盘分区 531
更改默认邮件存储分区定义 531
执行邮件存储维护过程 532
管理邮箱 532
监视配额限制 537
监视磁盘空间 538
使用 stored 实用程序 538
由于重复存储相同的邮件而减少邮件存储大小 539
备份并恢复邮件存储 543
创建邮箱备份策略 544
创建备份组 545
Messaging Server 备份和恢复实用程序 547
执行备份时排除批量邮件 548
部分恢复的注意事项 549
从已被增量备份的邮箱中恢复邮件 550
使用 Legato Networker 551
使用除 Legato 以外其他的第三方备份软件 554
备份和恢复问题的故障排除 555
邮件存储灾难备份和恢复 555
监视用户访问 556
邮件存储故障排除 557
标准邮件存储监视过程 558

邮件存储启动和恢复 560
修复邮箱和邮箱数据库 563
常见问题和解决方案 567

第 19 章 配置安全和访问控制 571
关于服务器安全性 572
关于 HTTP 安全性 573
配置验证机制 573
配置访问纯文本密码的步骤 575
转换用户的步骤 576
用户密码登录 577
IMAP、 POP 和 HTTP 密码登录 577
SMTP 密码登录 578
配置加密和基于证书的验证 578
通过管理控制台获得证书 580
创建自签名证书 583
启用 SSL 并选择加密算法的步骤 584
设置基于证书的登录的步骤 586
如何使用 SMTP 代理服务器优化 SSL 性能 587
网络安全服务工具 587
管理证书和密钥 588
配置管理员对 Messaging Server 的访问 589
委派的管理的分层结构 589
提供对服务器的整体访问的步骤 590
限制对特定任务的访问权限的步骤 590
配置客户机对 POP、 IMAP 和 HTTP 服务的访问 591
客户机访问过滤器工作原理 592
过滤器语法 592
过滤器示例 597
为服务创建访问过滤器的步骤 599
为 HTTP 代理验证创建访问过滤器的步骤 600
启用 POP Before SMTP 601
安装 SMTP 代理的步骤 602
配置客户机对 SMTP 服务的访问 604
基于 SSL 的用户 / 组目录查找 604

第 20 章 管理 Communications Express Mail 的 S/MIME 605
什么是 S/MIME? 606
用户需要了解的概念 606
必需的软件和硬件组件 607
使用 S/MIME 的要求 608
专用密钥和公共密钥 608

存储在智能卡中的密钥 608
存储在客户机中的密钥 609
在 LDAP 目录中发布公共密钥 609
授予邮件用户使用 S/MIME 的权限 609
多语言支持 609
安装 Messaging Server 后开始使用 610
S/MIME Applet 610
基本的 S/MIME 配置 611
使用证书访问 LDAP 中的公共密钥、 CA 证书和 CRL 615
smime.conf 文件的参数 617
Messaging Server 选项 623
使用 SSL 确保 Internet 链路的安全 624
确保 Messaging Server 和 Communications Express Mail 之间的链路的安全 625
确保 Messaging Server 和 S/MIME Applet 之间的链路的安全 625
客户机的密钥访问库 626
示例 627
验证专用密钥和公共密钥 628
查找用户的专用或公共密钥 628
何时根据 CRL 检查证书？ 629
访问 CRL 629
代理服务器和 CRL 检查 631
使用过时 CRL 631
确定要使用的邮件发送时间 632
访问 CRL 时出现问题 633
当证书撤销时 633
授予使用 S/MIME 功能的权限 634
S/MIME 权限示例 634
管理证书 635
LDAP 目录中的 CA 证书 635
LDAP 目录中的公共密钥和证书 636
验证 LDAP 目录中是否存在密钥和证书 637
网络安全服务证书 639
Communications Express S/MIME 最终用户信息 639
首次登录 640
签名和加密设置 641
启用 Java 控制台 642

第 21 章 管理日志记录 643
日志记录概述 643
日志记录数据的类型 644
Messaging Server 日志文件的类型 644
跟踪分布在各种日志文件中的邮件 646
管理日志记录的工具 647

管理 MTA 邮件和连接日志 647
了解 MTA 日志条目格式 648
启用 MTA 日志记录 651
指定附加 MTA 日志记录选项 652
MTA 邮件日志记录示例 653
启用分发程序调试 667
管理服务日志 669
了解服务日志特性 669
了解服务日志文件格式 671
定义和设置服务日志记录选项 672
搜索并查看服务日志 674
处理服务日志 676
使用邮件存储日志记录的邮件跟踪 678
邮件存储日志记录示例 681

第 22 章 MTA 故障排除 683
故障排除概述 683
标准 MTA 故障排除过程 684
检查 MTA 配置 684
检查邮件队列目录 685
检查重要文件的拥有权 685
检查作业控制器和分发程序是否正在运行 686
检查日志文件 687
手动运行通道程序 688
启动和停止各个通道 688
MTA 故障排除示例 689
常见 MTA 问题和解决方案 693
TLS 问题 694
对配置文件或 MTA 数据库的更改未生效 694
MTA 可以发送外发邮件但不能接收外来邮件 694
分发程序 （SMTP 服务器）无法启动 695
外来 SMTP 连接超时 695
邮件未被排出队列 697
未传送 MTA 邮件 698
邮件在循环 699
接收到的邮件已编码 701
服务器端规则 （SSR）不生效 702
地址的本地部分或接收字段中的星号 703
一般错误消息 703
mm_init 中的错误 704
编译的配置版本不匹配 707
交换空间错误 708
文件打开或创建错误 708

非法主机 / 域错误 709
SMTP 通道中的错误：os_smtp_* 错误 709

第 23 章 监视 Messaging Server 711
自动监视和重新启动 711
每天的监视任务 712
检查邮寄主管邮件 712
监视和维护日志文件 712
设置 msprobe 实用程序 712
监视系统性能 713
监视端对端邮件传送时间 713
监视磁盘空间 713
监视 CPU 的使用率 716
监视 MTA 716
监视邮件队列的大小 716
监视传送失败率 717
监视入站 SMTP 连接 717
监视分发程序和作业控制器进程 718
监视 LDAP 目录服务器 719
监视 slapd 719
监视邮件访问 719
监视 imapd、 popd 和 httpd 720
监视 stored 721
监视邮件存储 722
监视邮件存储数据库锁定的状态 722
监视 mboxlist 目录中的数据库日志文件的数目 723
用于监视的实用程序和工具 723
immonitor-access 724
stored 724
counterutil 724
日志文件 728
imsimta 计数器 728
imsimta qm counters 731
使用 SNMP 的 MTA 监视 731
用于邮箱配额检查的 imquotacheck 732
使用 msprobe 和 watcher 功能进行监视 733

附录 A SNMP 支持 737
SNMP 实现 738
Messaging Server 中的 SNMP 操作 739
在 Solaris 8 中为 Messaging Server 配置 SNMP 支持 739
通过 SNMP 客户机监视 740

与 Unix 平台中的其他 Sun Java System 产品共存 741
来自 Messaging Server 的 SNMP 信息 741
applTable 741
assocTable 743
mtaTable 744
mtaGroupTable 745
mtaGroupAssociationTable 746
mtaGroupErrorTable 748

附录 B 在 Messaging Server 中管理事件通知服务 749
在 Messaging Server 中装入 ENS Publisher 749
在 Messaging Server 上装入 ENS Publisher 750
运行样例事件通知服务程序 750
运行样例 ENS 程序 750
管理事件通知服务 751
启动和停止 ENS 751
启动和停止 ENS 751
iPlanet Event Notification Service 配置参数 752

附录 C 使用 Console 界面管理邮件用户和邮件列表 （不建议采用此方式） 753
管理邮件用户 753
访问邮件用户 753
指定用户电子邮件地址 755
配置传送选项 756
指定转发地址 758
配置自动回复设置 759
配置授权服务 760
管理邮递列表 761
访问邮递列表 761
指定邮递列表设置 762
指定列表成员 765
定义邮件邮寄限制 767
定义中介人 768

附录 D 短消息服务 (SMS) 771
介绍 771
要求 773
SMS 通道操作原理 774
将电子邮件定向到通道 774
电子邮件到 SMS 的转换过程 775
SMS 消息提交过程 779
站点定义的地址有效性检查和转换 782

站点定义的文本转换 783
SMS 通道配置 788
添加 SMS 通道 788
创建 SMS 通道选项文件 790
可用选项 791
添加附加 SMS 通道 811
调整传送重试的频率 812
单向配置范例 (MobileWay) 812
为双向 SMS 配置 SMS 通道 814
SMS Gateway Server 操作原理 815
SMS Gateway Server 功能 815
SMPP 中继和服务器性能 816
远程 SMPP 到 Gateway SMPP 的通信 816
SMS 回复和通知的处理 818
SMS Gateway Server 配置 819
设置双向 SMS 路由选择 820
启用和禁用 SMS Gateway Server 821
启动和停止 SMS Gateway Server 821
SMS Gateway Server 配置文件 821
配置网关服务器上的电子邮件到移动设备 822
配置移动设备到电子邮件的操作 824
配置选项 825
全局选项 826
SMPP 中继选项 829
SMPP 服务器选项 831
网关配置文件选项 833
双向 SMS 配置示例 838
SMS Gateway Server 存储要求 841

附录 E 安装工作单 843
Directory Server 安装 844
Administration Server 初始运行时配置 846
Directory Server 安装程序脚本 (comm_dssetup.pl) 847
Messaging Server 初始运行时配置 848

词汇表 851

索引 853

表

表 1 本书的结构 30
表 2 印刷约定 32
表 3 符号约定 32
表 4 默认路径和文件名 33
表 1-1 用于 Messaging Server configure 程序的可选标志 50
表 1-2 对 Sun_MsgSvr 拥有权和访问模式的更改 60
表 1-3 安装后的目录和文件 64
表 1-4 安装期间指定的端口号 65
表 1-5 潜在的端口号冲突 66
表 2-1 生成 *.MERGED 或 *.CHANGES 文件的 Messaging Server 配置文件 69
表 3-1 受支持的 Sun Cluster Server 和 Veritas Cluster Server 版本 77
表 3-2 Veritas Cluster Server 属性 82
表 4-1 在 Messaging Server 初始运行时配置期间设置的密码 94
表 4-2 在 Sun Cluster 3.0/3.1 环境中启动、停止和重新启动 97
表 4-3 在 Veritas 1.3、 2.0、 2.1 和 3.5 环境中启动、停止和重新启动 97
表 4-4 由 watcher 和 msprobe 监视的服务 101
表 4-5 HA 自动重新启动参数 102
表 6-1 Access Manager 单点登录参数 131
表 6-2 SSO 互操作性 133
表 6-3 信任范围单点登录参数 140
表 7-1 Messaging Multiplexor 配置文件 152
表 7-2 MMP 命令 153
表 9-1 从各个 schematag 值得到的对象类 190
表 9-2 要进行检查的属性 191
表 9-3 设置检索到的磁盘配额和邮件配额属性的 MTA 选项 194
表 9-4 MTA 选项、默认属性和元字符 194
表 9-5 用于 DELIVERY_OPTIONS MTA 选项中的选项的单字符前缀。 195

表 9-6 传送选项中使用的附加元字符 196
表 9-7 控制 $nI 和 $nS 元字符的性能修改的整数 197
表 9-8 特殊的模板字符串 197
表 9-9 组扩展默认属性和用于设置属性名称的 MTA 选项 199
表 9-10 local.imta.schematag 值和属性 202
表 9-11 LDAP_USE_ASYNC MTA 选项的设置 203
表 10-1 地址和关联的通道 208
表 10-2 Messaging Server 映射表 209
表 10-3 映射模式通配符 212
表 10-4 映射模板替换和元字符 214
表 10-5 MTA 配置文件 221
表 10-6 作业控制器配置文件选项 230
表 10-7 REVERSE 映射表标志 235
表 10-8 FORWARD 映射表标志说明 238
表 10-9 通知邮件替换序列 242
表 10-10 传送状态和邮件处理通知选项 245
表 10-11 用于将通知邮件发送给邮寄主管和发件人的关键字 250
表 11-1 重写规则的特殊模式摘要 259
表 11-2 重写规则的模板格式摘要 260
表 11-3 提取的地址和主机名 263
表 11-4 重写规则模板替换和控制序列的摘要 268
表 11-5 LDAP URL 替换序列 271
表 11-6 单个字段替换 274
表 11-7 地址范例和重写 279
表 12-1 按字母顺序排列的通道关键字 282
表 12-2 按功能分类的通道关键字 285
表 12-3 SMTP 通道 299
表 12-4 SMTP 命令和协议关键字 301
表 12-5 TCP/IP 连接和 DNS 查找关键字 308
表 12-6 authrewrite 位值 316
表 12-7 邮件处理和传送关键字 318
表 12-8 missingrecipientpolicy 的值 332
表 13-1 预定义的通道 361
表 13-2 本地通道选项 364
表 13-3 转换通道环境变量 372
表 13-4 转换通道输出选项 375
表 13-5 转换通道常用的特殊指令 377

表 13-6 转换参数 380
表 13-7 CHARSET-CONVERSION 映射表关键字 384
表 14-1 垃圾邮件过滤器的 MTA 通道关键字 400
表 14-2 MTA 垃圾邮件过滤器选项 (option.dat) 403
表 14-3 选定的 Brightmail 配置文件选项 408
表 14-4 SpamAssassin 选项 (spamassassin.opt) 420
表 14-5 针对 SpamAssassin mode 选项返回的字符串 422
表 14-6 ICAP 选项 426
表 14-7 针对 ICAP mode 选项返回的结论字符串 428
表 15-1 收件人的 LMTP 状态代码 447
表 16-1 用于 DELIVERY_OPTIONS 中的自动回复规则的前缀字符 450
表 17-1 访问控制映射表 457
表 17-2 访问映射标志 458
表 17-3 PORT_ACCESS 映射表 466
表 17-4 filter 通道关键字 *URL-pattern* 替换标记 （不区分大小写） 484
表 18-1 邮件存储命令行实用程序 492
表 18-2 邮件存储目录说明 495
表 18-3 ACL 权限字符 501
表 18-4 用于配置分布式共享文件夹的变量 505
表 18-5 readership 选项 507
表 18-6 邮件存储配额属性 510
表 18-7 邮件存储 configutil 参数 511
表 18-8 imexpire 属性 522
表 18-9 使用正则表达式的 imexpire 文件夹模式 524
表 18-10 过期和清除 configutil 日志和调度参数 527
表 18-11 mboxutil 选项 533
表 18-12 stored 选项 539
表 18-13 relinker configutil 参数 543
表 18-14 stored 操作 560
表 18-15 邮件存储数据库快照参数 563
表 18-16 reconstruct 选项 564
表 19-1 某些 SASL 参数和与 SASL 相关的 configutil 参数 574
表 19-2 适用于 Messaging Server 的 SSL 加密算法 585
表 19-3 服务过滤器的通配符名称 594
表 20-1 客户机必需的硬件和软件 607
表 20-2 服务器必需的软件 607
表 20-3 smime.conf 参数摘要 614

表 20-4 smime.conf 文件中的 S/MIME 配置参数 618
表 20-5 客户机的特殊库 627
表 20-6 Communications Express Mail 的签名和加密复选框 642
表 21-1 Messaging Server 日志文件 644
表 21-2 日志记录条目代码 649
表 21-3 分发程序调试位 667
表 21-4 存储和管理服务的日志记录级别 669
表 21-5 日志事件的发生类别 670
表 21-6 存储和管理日志文件组件 671
表 22-1 MTA 日志文件 687
表 23-1 counterutil alarm 统计数据 725
表 23-2 counterutil imapstat 统计数据 726
表 23-3 counterutil diskstat 统计数据 727
表 23-4 counterutil serverresponse 统计数据 727
表 23-5 msprobe 和 watcher configutil 选项 733
表 23-6 有用的警报邮件 configutil 参数 735
表 B-1 iBiff 配置参数 752
表 C-1 LDAP URL 选项 765
表 D-1 SMS 属性 774
表 D-2 生成的 BIND_TRANSMITTER PDU 中的字段 779
表 D-3 生成的 SUBMIT_SM PDU 中的强制性字段 781
表 D-4 生成的 SUBMIT_SM PDU 中的可选字段 782
表 D-5 SMS 通道选项 791
表 D-6 USE_HEADER_FROM 值 796
表 D-7 USE_UCS2 有效值 797
表 D-8 数字规划指标值 798
表 D-9 典型 TON 值 799
表 D-10 针对每个 SMS 配置文件类型解释的 SMS 优先级值 799
表 D-11 将 Priority: 标题转换成 SMS 优先级标志的映射 800
表 D-12 DEFAULT_PRIVACY 和 USE_HEADER_SENSITIVITY 的值的结果 800
表 D-13 SMS 保密性值解释 801
表 D-14 将 Sensitivity: 标题转换成 SMS 保密性值的映射 801
表 D-15 DEFAULT_VALIDITY_PERIOD 格式和值 802
表 D-16 DEBUG 位掩码 808
表 D-17 替换序列 809
表 D-18 双向配置的例外情况 814
表 D-19 SMPP 服务器协议数据单元 817

表 D-20 全局选项 826
表 D-21 DEBUG 位掩码 828
表 D-22 SMPP 中继选项 829
表 D-23 SMPP 服务器选项 832
表 D-24 SMS Gateway Server 配置文件选项 833
表 D-25 从 SMS 到电子邮件的优先级标志映射 836
表 D-26 从 SMS 到电子邮件的优先级标志映射 837
表 D-27 SMS Gateway Server 存储要求 841
表 E-1 Directory Server 安装参数 844
表 E-2 Administration Server 初始运行时配置程序参数 846
表 E-3 comm_dssetup.pl 脚本参数 847
表 E-4 Messaging Server 初始运行时配置程序参数 848

图

图 3-3 简单 Sun Java System Messaging Server HA 配置 85
图 5-1 HTTP 服务组件 125
图 6-1 简单 SSO 部署 134
图 6-2 复杂 SSO 部署 135
图 7-1 MMP 安装中的客户机和服务器 146
图 7-2 多个 MMP 支持多个 Messaging Server 156
图 7-3 概述 iPlanet Messenger Express Multiplexor 160
图 8-1 Messaging Server，简化的组件视图（未显示 Messenger Express） 169
图 8-2 MTA 体系结构 170
图 8-3 主程序和从程序 176
图 8-4 ims-ms 通道 176
图 14-1 Brightmail 和 Messaging Server 体系结构 406
图 15-1 不带有 LMTP 的两层部署 433
图 15-2 带有 LMTP 的两层部署 435
图 18-1 邮件存储目录布局 494
图 18-2 Ed 的客户机共享邮件文件夹列表的示例 499
图 18-3 分布式共享文件夹示例 506
图 18-4 自动删除邮件（过期 / 清除）GUI 草图 525
图 18-5 邮件存储摘要系统信息库 540
图 18-6 备份组目录结构 552
图 19-1 与 Messaging Server 的加密通信 579
图 20-1 S/MIME Applet 610
图 20-2 验证专用密钥和公共密钥。 628
图 A-1 SNMP 信息流 739
图 D-1 单向和双向 SMS 逻辑流 772
图 D-2 SMS 通道的电子邮件处理 776
图 D-3 SMS 通道的电子邮件处理（续） 777

前言

本指南说明了如何管理 Sun Java™ System Messaging Server 及其附带的软件组件。通过使用开放的 Internet 标准， Messaging Server 为满足各种规模的企业和邮件传送主机的电子邮件需求提供了功能强大且灵活的跨平台解决方案。

本章包含以下主题：

- 目标读者
- 阅读本书之前
- 本书的结构
- 本指南中使用的约定
- 相关文档
- 本指南联机文档所在的位置
- 访问 Sun 资源联机文档
- 联系 Sun 技术支持
- 相关的第三方 Web 站点参考
- Sun 欢迎您提出意见

目标读者

本书的目标读者为负责在站点上管理和部署 Messaging Server 的用户。您还应当阅读 Sun Java System Communications Services Deployment Planning Guide (http://docs.sun.com/doc/819-0063)。

阅读本书之前

本指南假设您负责安装 Messaging Server 软件并且大致了解以下知识：

- Internet 和万维网
- Messaging Server 协议
- Sun Java System Administration Server
- Sun Java System Directory Server 和 LDAP
- Sun Java System Console
- 以下平台上的系统管理和联网：
- 常规部署体系结构

本书的结构

本指南包含以下章节和附录：

表 1 本书的结构

章节	说明
前言	关于使用本指南的一般信息。
第 1 章 “安装后任务和布局”	介绍要使 Messaging Server 正常运行所需的任务。
第 2 章 “升级到 Sun Java Systems Messaging Server”	介绍如何从 Messaging Server 5.2 升级到 Messaging Server 6 2005Q1。
第 3 章 “配置高可用性”	提供了有关如何配置 Veritas Cluster Server 和 Sun Cluster 高可用性群集软件以便与 Messaging Server 一起使用的信息。
第 4 章 “配置一般邮件传送能力”	介绍 Messaging Server 的一般任务。
第 5 章 “配置 POP、 IMAP 和 HTTP 服务”	介绍如何通过使用 Sun ONE Console 或命令行实用程序来配置服务器，以使其支持 POP、 IMAP 和 HTTP 服务。

表 1 本书的结构

章节	说明
第 6 章 “启用单点登录 (SSO)”	说明如何启用单点登录。
第 7 章 “配置和管理多路复用器服务”	介绍用于标准邮件协议 （POP、 IMAP 和 SMTP）的 Messaging Multiplexor (MMP) 和用于 Messenger Express Web 接口的 Messenger Express Multiplexor。
第 8 章 “MTA 概念”	提供了 MTA 的概念性说明。
第 9 章 “MTA 地址转换和路由”	介绍 MTA 地址转换和路由选择。
第 10 章 “关于 MTA 服务和配置”	介绍一般的 MTA 服务和配置。
第 11 章 “配置重写规则”	说明如何在 imta.cnf 文件中配置重写规则。
第 12 章 “配置通道定义”	说明如何在 MTA 配置文件 imta.cnf 中使用通道关键字定义。
第 13 章 “使用预定义通道”	介绍如何在 MTA 中使用预定义的通道定义。
第 14 章 “将垃圾邮件和病毒过滤程序集成至 Messaging Server”	介绍如何使用 Messaging Server 集成和配置垃圾邮件和病毒过滤软件。
第 15 章 “LMTP 传送”	介绍 LMTP 操作和部署。
第 16 章 “休假自动邮件回复”	介绍休假自动回复机制。
第 17 章 “邮件过滤和访问控制”	讨论如何基于邮件的源 （发件人、 IP 地址等）或标题字符串来过滤邮件。
第 18 章 “管理邮件存储”	介绍邮件存储和邮件存储管理界面。
第 19 章 “配置安全和访问控制”	介绍如何配置 Messaging Server 的安全性和访问控制。
第 20 章 “管理 Communications Express Mail 的 S/MIME”	介绍如何管理 S/MIME。
第 21 章 “管理日志记录”	介绍 Messaging Server 日志记录工具。
第 22 章 “MTA 故障排除”	介绍对 MTA 进行故障排除的常用工具、方法和过程。
第 23 章 “监视 Messaging Server”	介绍 Messaging Server 的监视功能。
附录 A “SNMP 支持”	介绍如何启用 Messaging Server 的 SNMP 支持功能。
附录 B “在 Messaging Server 中管理事件通知服务”	介绍如何在 Messaging Server 中启用 Event Notification Service Publisher (ENS Publisher) 和管理 Event Notification Service (ENS)。
附录 C “使用 Console 界面管理邮件用户和邮件列表 （不建议采用此方式）”	不建议使用。
附录 D “短消息服务 (SMS)”	介绍如何实现短消息服务 (SMS)。
附录 E “安装工作单”	提供可以用来规划安装的工作单。
词汇表	此文档集中所使用的术语的完整列表。
索引	索引

本指南中使用的约定

本节中的表格介绍了本指南中所使用的约定。

印刷约定

下表介绍本书所采用的印刷约定。

表 2 印刷约定

字样	含义	示例
AaBbCc123 （等宽）	任何显示在计算机屏幕上的文本或您应键入的文本。可能为 API 和语言元素、 HTML 标记、 Web 站点 URL、命令名、文件名、目录路径名、计算机屏幕输出以及样例代码。	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `% You have mail.`
AaBbCc123 （等宽粗体）	显示在代码示例中的您应键入的文本或其他计算机屏幕输出。	`% su` `Password:`
AaBbCc123 *（斜体）*	位于命令或路径名中、您应使用真实的名称和值将其替换的占位符 （例如，变量）。	文件位于 *msg_svr_base*`/bin` 目录中。 这些称为 *class* 选项。
新词术语强调	新术语或要被强调的字。	请**勿**保存该文件
《》	书名	阅读用户指南的第 6 章

符号

下表介绍了本指南中使用的符号约定。

表 3 符号约定

符号	说明	示例	含义
`[ ]`	可选命令选项。	`ls [-l]`	`-l` 选项不是必需的。
`{ | }`	包含用于所需命令选项的一组选择。	`-d {y|n}`	`-d` 选项需要您使用 `y` 变量或 `n` 变量。
-	连接需要同时按的多个按键。	Control-A	按 A 键的同时，按 Control 键。

表 3 符号约定 （续）

符号	说明	示例	含义
+	连接需要连续按的多个按键。	Ctrl+A+N	按 Control 键，松开它，然后再按随后的两个键。
>	表示图形用户界面中的菜单条目选项。	File > New > Templates	从 “文件” 菜单中，选择 “新建”。从 “新建” 子菜单中，选择 “模板”。

默认路径和文件名

下表介绍了本指南中使用的默认路径和文件名。

表 4 默认路径和文件名

术语	说明
msg_svr_base	表示 Messaging Server 的基本安装目录。 *msg_svr_base* 的默认安装目录如下所示： Solaris™ 系统：`/opt/SUNWmsgsr` Linux 系统：`/opt/sun/messaging`

命令行提示符

大多数示例中没有显示命令行提示符 （例如，`%` 表示 C Shell，或者 `$` 表示 Korn 或 Bourne Shell）。您会看到各种不同的命令行提示符，这取决于您使用的操作系统。但是，除非另有明确说明，否则您应该按照文档所示输入命令。

相关文档

`http://docs.sun.com` Web 站点使您可以访问 Sun 技术支持联机文档。您可以浏览归档文件或搜索某个特定的书名或主题。

Messaging Server 文档

使用以下 URL 可以查看所有 Messaging Server 文档：

`http://docs.sun.com/coll/MessagingServer_05q1` 和

`http://docs.sun.com/coll/MessagingServer_05q1_zh`

以下是所提供的文档：

- Sun Java SystemMessaging Server 发行说明
(http://docs.sun.com/doc/819-1052)
- Sun Java System Messaging Server 管理指南
(http://docs.sun.com/doc/819-1056)
- Sun Java System Messaging Server Administration Reference
(http://docs.sun.com/doc/819-0106)
- Sun Java System Messaging Server MTA Developer's Reference
(http://docs.sun.com/doc/819-0107)
- Sun Java System Messenger Express Customization Guide
(http://docs.sun.com/doc/819-0108)

Messaging Server 产品套件包含诸如 Sun Java™ System Console、Directory Server 和 Administration Server 等其他产品。在以下 URL 中可以找到这些产品和其他产品的文档：

http://docs.sun.com/db/prod/java.sys

除了软件文档，有关特定的 Messaging Server 产品问题的技术帮助，请参见 Messaging Server 软件论坛。该论坛位于以下 URL:

http://swforum.sun.com/jive/forum.jsp?forum=15

Communications Services 文档

使用以下 URL 可以查看适用于所有 Communications Services 产品的文档：

http://docs.sun.com/coll/MessagingServer_05q1 和

http://docs.sun.com/coll/MessagingServer_05q1_zh

以下是所提供的文档：

- Sun Java System Messenger Express Customization Guide
(http://docs.sun.com/doc/819-0108)
- Sun Java System Communications Services Delegated Administrator 指南
(http://docs.sun.com/doc/819-1103)
- Sun Java System Communications Services Deployment Planning Guide
(http://docs.sun.com/doc/819-0063)

- Sun Java System Communcations Services Schema Reference
(http://docs.sun.com/doc/819-0113)
- Sun Java System Communications Services Schema Migration Guide
(http://docs.sun.com/doc/819-0112)
- Sun Java System Event Notification Service Guide
(http://docs.sun.com/doc/819-0109)
- Sun Java System Communications Express 管理指南
(http://docs.sun.com/doc/819-1067)
- Sun Java System Communications Express Customization Guide
(http://docs.sun.com/doc/819-0116)

本指南联机文档所在的位置

您可以找到 PDF 和 HTML 格式的 Messaging Server 管理指南的联机文档。此联机文档位于以下 URL：

(http://docs.sun.com/doc/819-1056)

访问 Sun 资源联机文档

有关产品下载、专业服务、修补程序和支持以及其他开发者信息，请转至以下地址：

- 下载中心
http://wwws.sun.com/software/download/
- 专业服务
http://www.sun.com/service/sunps/sps.html
- Sun Enterprise 服务、 Solaris 修补程序以及支持
http://sunsolve.sun.com/
- 开发者信息
http://developers.sun.com/prodtech/index.html

联系 Sun 技术支持

如果您有关于此产品的技术问题，并且此问题未在产品文档中得到解答，请转至 http://www.sun.com/service/contacting。

相关的第三方 Web 站点参考

Sun 对本文档中提到的第三方 Web 站点的可用性不承担任何责任。对于此类站点或资源中的（或通过它们获得的）任何内容、广告、产品或其他材料， Sun 并不表示认可，也不承担任何责任。对于因使用或依靠此类站点或资源中的（或通过它们获得的）任何内容、产品或服务而造成的或连带产生的实际或名义损坏或损失， Sun 概不负责，也不承担任何责任。

Sun 欢迎您提出意见

Sun 致力于提高其文档的质量，并十分乐意收到您的意见和建议。

要共享您的意见，请转至 http://docs.sun.com 并单击“发送意见”。在联机表格中，提供了文档标题和文件号码。文件号码为七位或九位数字，可以在手册的标题页面或文档的顶部找到它。例如，本指南的标题为《Sun Java System Messaging Server 6 2005Q1 管理指南》，文件号码为 819-1056。在您提出意见时，可能需要在表单中输入英文版书名和文件号码，本书的英文版文件号码和书名为：819-0105，《Sun Java System Messaging Server 6 2005Q1 Administration Guide》。

第 1 章

安装后任务和布局

本章假定您已阅读了 Sun Java System Messaging Server Deployment Planning Guide (http://docs.sun.com/doc/819-0063)，并已通过 Sun Java™ Enterprise System 安装程序安装了 Messaging Server （请参见 Sun Java Enterprise System 安装指南 [http://docs.sun.com/doc/819-0811]）。执行以下任务后， Messaging Server 就可以正常运行。您还需要自定义部署以及置备和 / 或迁移用户和组。本指南的后续章节中将对自定义进行说明。Sun Java System Communications Services Delegated Administrator 指南 (http://docs.sun.com/doc/819-1103) 中对置备进行了介绍。

本章由以下各节组成：

- 第 38 页的 “创建 UNIX 系统用户和组”
- 第 39 页的 “为 Messaging Server 配置准备 Directory Server”
- 第 49 页的 “创建初始 Messaging Server 运行时配置”
- 第 54 页的 “针对 Directory Server 拷贝安装 Messaging Server”
- 第 55 页的 “安装 Messaging Server 置备工具”
- 第 58 页的 “SMTP 中继阻止”
- 第 60 页的 “在重新引导后启用启动”
- 第 60 页的 “处理 sendmail 客户端”
- 第 63 页的 “配置 Messenger Express 和 Communications Express 邮件过滤器”
- 第 63 页的 “性能和调节”
- 第 64 页的 “安装后的目录布局”
- 第 65 页的 “安装后的端口号”

创建 UNIX 系统用户和组

系统用户运行特定的服务器进程，需要将权限授予这些系统用户，这样他们才对其正在运行的进程具有相应权限。

设置用于所有 Sun Java System 服务器的系统用户帐户和组，并为该用户所拥有的目录和文件设置权限。要完成此任务，请执行以下步骤：

注 出于安全原因，在某些部署中不同的服务器可能需要有不同的系统管理员。这可以通过为每个服务器创建不同的系统用户和组来完成。例如， Messaging Server 的系统用户不同于 Web Server 的系统用户，并且 Messaging Server 的系统管理员无法管理 Web Server。

1. 以超级用户身份登录。
2. 创建一个组，您的系统用户将属于该组。在以下示例中，将创建 `mailsrv` 组：

```
# groupadd mail
```

3. 创建系统用户，并将其与刚才创建的组相关联。另外，为该用户设置密码。在以下示例中，将创建用户 `mail` 并将其与 `mailsrv` 组相关联：

```
# useradd -g mail mailsrv
```

`useradd` 和 `usermod` 命令位于 `/usr/sbin`。有关详细信息，请参见 UNIX 手册页。

4. 您可能还需要查看 `/etc/group` 和 `/etc/passwd` 文件，以确保已将用户添加到您创建的系统组中。

注 如果决定在安装 Messaging Server 之前不设置 UNIX 系统用户和组，您将可以在执行第 49 页的 “创建初始 Messaging Server 运行时配置”时指定这些用户和组。

为 Messaging Server 配置准备 Directory Server

本节说明了如何运行 Directory Server 安装程序脚本 (comm_dssetup.pl)，该脚本用于配置 LDAP Directory Server，使其能够与 Messaging Server、 Calendar Server 或用户管理实用程序配置结合使用。 comm_dssetup.pl 脚本通过在 Directory Server 中设置新的模式、索引和配置数据来准备 Directory Server。新安装 Messaging Server 和 Communications Express 时必须运行该脚本。如果要升级依赖于 Directory Server 的任何组件产品，最好运行最新的 comm_dssetup.pl。

本节说明了以下主题：

- 第 39 页的 “comm_dssetup.pl 的位置”
- 第 40 页的 “comm_dssetup.pl 要求”
- 第 41 页的 “运行 comm_dssetup.pl 脚本”

comm_dssetup.pl 的位置

在 Java Enterprise System 的早期版本中，此实用程序与 Messaging Server 和 Calendar Server 捆绑在一起，不必单独安装。但是，从 Java Enterprise System 2005Q1 开始，该脚本成为一个可单独安装的共享组件。

要安装 comm_dssetup.pl，请选择以下方法之一：

- 使用 Java Enterprise System 安装程序时，请在组件选择面板上选择 comm_dssetup.pl。（选择 Directory Server 也将自动选择 comm_dssetup.pl。）
- 如果您从 Java Enterprise System 的早期版本升级，而且未使用 Java Enterprise System 安装程序，则请下载以下修补程序：

  Solaris Sparc：118245 和 118242

  Solaris x86：118256 和 118243

  Linux：仅 118247

安装时，将在以下目录中找到 comm_dssetup.pl：

Solaris：/opt/SUNWcomds/sbin

Linux：/opt/sun/comms/dssetup/sbin

comm_dssetup.pl 要求

运行 comm_dssetup.pl 脚本之前，请务必阅读以下要求：

- 在运行 comm_dssetup.pl 脚本之前，必须先安装和配置 Directory Server。
- 以超级用户身份运行 comm_dssetup.pl 脚本。
- 在运行 Messaging Server、Calendar Server、Communications Express 或用户管理实用程序初始运行时配置程序之前，先运行 comm_dssetup.pl。
  - 通常，如果已在目录服务器上为某个产品 （例如 Calendar Server）运行了 comm_dssetup.pl，则不必为其他产品 （例如 Messaging Server）再次运行该脚本 （只要两种产品使用的是同一目录服务器）。但是，如果您更改了运行 comm_dssetup 时给出的某些回答，则需要再次运行 comm_dssetup。例如，如果您要为 Messaging Server 的下一个配置使用不同的用户 / 组后缀，比如由于运行 commdirmig（从 Sun LDAP Schema 1 迁移到 Sun LDAP Schema 2）。
- 必须在目录服务器计算机上运行 comm_dssetup.pl 脚本。
- 确保在运行 comm_dssetup.pl 之前先运行目录服务器。
- 每次安装新版本的 Messaging Server 时，都需要在 Directory Server 计算机上运行新版本的 comm_dssetup.pl。新的模式和索引可能会添加到每个 Messaging Server 分发中。
- 如果配置数据以及用户和组数据被分到两个不同的目录实例中，则需要在这两个实例中运行 comm_dssetup 脚本。
- 对于 UNIX 系统，使用 Directory Server 附带的 Perl 版本可以避免版本问题：*dir_server_root*/bin/slapd/admin/bin/perl。
- 如果在远程目录服务器上运行 comm_dssetup.pl，请执行以下操作：
  - 将 dssetup.zip 文件从 *msg_svr_base*/install 目录复制到远程目录服务器上。您可能希望将其复制到类似于 /tmp 或 /var/tmp 的目录中。如果不希望在所有的 Directory Server 计算机上安装 comm_dssetup，您可以将 zip 文件复制到而不是安装到 Directory Server 计算机上。
  - 解压缩 dssetup.zip 文件 （包含 comm_dssetup.pl 和必需模式）。
  - 在远程目录服务器上运行 comm_dssetup.pl 脚本。
- 如果运行的是复制的 Directory Server，则需确保对主目录和拷贝目录均运行 comm_dssetup.pl 脚本。
- 运行 Directory Server 安装程序脚本 (comm_dssetup.pl) 以准备用于 Messaging Server 配置的 Directory Server 时，请将安装参数记录在表 E-3 第 847 页中。您需要将其中的某些参数用于 Messaging Server 初始运行配置。

运行 comm_dssetup.pl 脚本

您可以使用以下模式之一运行 comm_dssetup.pl：

- 第 41 页的 “交互模式”
- 第 47 页的 “无提示模式”

请使用 Sun Java System Messaging Server Deployment Planning Guide (http://docs.sun.com/doc/819-0063) 中的安装工作单来记录您的答案。

交互模式

如果您指定了不带任何变量的 comm_dssetup.pl，系统将询问您以下问题：

1. 介绍

```
# perl comm_dssetup.pl

Welcome to the Directory Server preparation tool for Java Enterprise
Communications Server.
(Version X.X Revision X.X)

This tool prepares your directory server for Sun Java System Messaging
Server install.

The logfile is /var/tmp/dssetup_YYYYMMDDHHSS

Do you want to continue [y]:
```

按 Enter 键继续。输入 No 可以退出。

2. Directory Server 的安装根目录

```
Please enter the full path to the directory where the Java
Enterprise Directory Server was installed.

Directory server root [/var/opt/mps/serverroot]
```

请指明 Directory Server 计算机上 Directory Server 安装根目录的位置。请注意，在 Linux 上， Directory Server 根目录位置是不同的。

3. Directory Server 实例

```
Please select a directory server instance from the following
list:

[1]   slapd-varrius

Which instance do you want [1]:
```

如果计算机上有多个 Directory Server 实例，请选择要使用 Messaging Server 进行配置的实例。

4. 目录管理员的独特名称 (DN)

```
Please enter the directory manager DN [cn=Directory Manager]:
Password:
```

目录管理员 DN (`cn=Directory Manager`) 是负责组织树中用户和组数据的管理员。请确保此脚本中指定的目录管理员 DN 与您在 Directory Server 安装和 Messaging Server 安装中设置的 DN 相同。

5. 用户和组的 Directory Server

```
Will this directory server be used for users/groups [Yes]:
```

如果输入 `Yes`，系统将询问更多关于用户 / 组树的问题。

如果输入 `No`，则假定仅将此目录实例用于存储配置数据，您将跳到有关更新模式文件的问题。针对配置目录实例运行此脚本后，您需要针对存储用户和组数据的目录实例运行此脚本，然后才能继续安装过程。

6. 用户和组基本后缀

```
Please enter the Users/Groups base suffix [o=usergroup]:
```

用户和组基本后缀是组织树中的顶层条目，它包含用户和组条目的名称空间。请确保您选择的用户和组基本后缀与您在 Directory Server 安装和 Messaging Server 安装过程中指定的后缀相同。

注 如果安装了 Access Manager，请确保在安装 Access Manager 时指定的后缀与您为此问题指定的后缀相同。如果使用不同的后缀，Messaging Server 将无法识别您安装的 Access Manager。

有关组织树的更多信息，请参见位于 http://docs.sun.com/source/817-4244-10/provisioning-concepts.html 的《Sun Java Enterprise System 2003Q4 安装指南》的第 12 章 “Messaging Server 6.0 的置备和模式概念”。

7. 模式类型

```
There are 3 possible schema types:
  1   - schema 1 for systems with iMS 5.x data
  1.5 - schema 2 compatibility for systems with iMS 5.x data
        that has been converted with commdirmig
  2   - schema 2 native for systems using Access Manager

Please enter the Schema Type (1, 1.5, 2) [1]:
```

如果要使用 Sun LDAP Schema 1，请选择选项 `1`。

如果要使用 Sun LDAP Schema 2 的兼容模式，请选择选项 `1.5`。有关更多信息，请参见 Sun Java System Communications Services Schema Migration Guide。

如果要使用 Sun LDAP Schema 2 本机模式，请选择选项 `2`。

如果未安装 Access Manager，`comm_dssetup.pl` 将不再终止。而会警告未安装 Access Manager 并建议为您安装 Schema 2。警告屏幕如下：

```
Please enter the Schema Type (1, 1.5, 2) [1]: 2

Access Manager has not been configured for this new user/group suffix

You can opt to continue, but you will not be able to use features that
depend on Access Manager

Are you sure you want this schema type? [n]:
```

有关模式选项的更多信息，请参见 Sun Java System Messaging Server Deployment Planning Guide (`http://docs.sun.com/doc/819-0063`)。

8. 域组件 (DC) 树基本后缀

```
Please enter the DC Tree base suffix [o=internet]:
```

注 如果在步骤 7 中选择了选项 1 或 1.5，系统将要求您提供 DC 树基本后缀。如果选择了选项 2 （Sun LDAP Schema 2，本机模式），系统将不会提出此问题。

DC 树镜像本地 DNS 结构，系统使用它作为组织树 （包含用户和组数据条目）的索引。 DC 树基本后缀是 DC 树中顶层条目的名称。您可以选择默认值 `o=internet` 或其他名称。

有关 DC 树或组织树的更多信息，请参见位于 `http://docs.sun.com/source/817-4244-10/provisioning-concepts.html` 的《Sun Java Enterprise System 2003Q4 安装指南》中的第 12 章 “Messaging Server 6.0 的置备和模式概念”。

9. 更新模式文件

```
Do you want to update the schema files [yes]:
```

如果回答 `Yes`，模式中将添加新元素。建议您每次安装新版本的 Messaging Server 时都使用新模式文件更新目录。

10. 配置新索引

```
Do you want to configure new indexes [yes]:
```

如果在步骤 5 （用户和组 Directory Server）中回答 `Yes`，系统将询问您是否要配置新索引，将使用该索引创建高速缓存，以提高目录搜索的效率。建议您对此问题回答 `Yes`。但是，在某些情况下您不需要创建索引：

- 如果是为仅用于提供拷贝服务的主用户 / 组 Directory Server，即没有对用户 / 组 Directory Server 执行的直接查询。
- 如果您的生产用户 / 组 Directory Server 具有大量条目，您不希望在其中创建索引时耗费大量停机时间。

11. 设置摘要

```
Here is a summary of the settings that you chose:
  Server Root                          : /var/opt/mps/serverroot/
  Server Instance                      : slapd-varrius
  Users/Groups Directory               : Yes
  Update Schema                        : yes
  Schema Type                          : 1
  DC Root                              : o=internet
  User/Group Root                      : o=usergroup
  Add New Indexes                      : yes
  Directory Manager DN                 : cn=Directory Manager

Now ready to generate a shell script and ldif file to modify the
Directory.
No changes to the Directory Server will be made this time.

Do you want to continue [y]:
```

更新目录配置之前，将显示您的设置摘要。此时将不能进行更改。

注 如果在步骤 7 中选择了选项 2：Sun LDAP Schema 2 （本机模式），设置摘要中的 DC 根将与您输入的用户 / 组根的值相同。

如果要更改任何设置，请输入 No 并重新运行脚本。

如果输入 Yes 继续运行，comm_dssetup.pl 脚本将创建以下 LDIF 文件和 Shell 脚本，用于更新 Directory Server 中的索引和模式：

/var/tmp/dssetup_*YYYYMMDDHHMMSS*.sh
/var/tmp/dssetup_*YYYYMMDDHHMMSS*.ldif

其中 *YYYYMMDDHHMMSS* 表示文件的创建时间和日期戳。

注 您可以选择现在运行脚本或以后运行脚本。如果选择现在运行脚本，请在系统询问您是否要继续时输入 Yes。如果要在以后运行脚本，您可以使用 /var/tmp/dssetup_*YYYYMMDDHHMMSS*.sh 调用脚本。

无提示模式

要启用无提示模式，请一次指定所有变量：

语法

```
# perl comm_dssetup.pl -i yes|no -c Directory_Server_Root -d
Directory_instance -r DC_tree -u User_Group_suffix -s yes|no -D
"DirectoryManagerDN" -w password -b yes|no -t 1|1.5|2 -m yes|no [-S
path-to-schema-files]
```

选项

此命令的选项包括：

选项	说明
-i yes|no	回答以下问题：“是否要配置新索引？”指定 yes 可以配置新索引。如果不希望配置新索引，请指定 no。
-c *Directory_Server_Root*	Directory Server 根路径名称。例如：/var/opt/mps/serverroot
-d *Directory_instance*	Directory Server 实例子目录。例如：slapd-budgie
-r *DC_tree*	DC 树后缀。例如：o=internet
-u *User_Group_suffix*	用户 / 组后缀。例如 o=usergroup
-s yes|no	回答以下问题：“是否要更新模式？”指定 yes 可以更新模式文件。如果不希望更新模式文件，请指定 no。
-D *DirectoryManagerDN*	目录管理员 DN。例如， "cn=Directory Manager"
-w *password*	目录管理员密码
-b yes|no	回答以下问题：“是否将此目录服务器用于用户和组？”如果要将目录服务器用于配置和用户 / 组，请指定 yes。如果只将此目录用于配置数据，请指定 no。
-t 1|1.5|2	确定要用于 Messaging Server 的模式版本： • 要使用 Sun LDAP Schema 1，请选择 1。 • 要使用 Sun LDAP Schema 2（兼容模式），请选择 1.5。有关更多信息，请参见 Sun Java System Communications Services Schema Migration Guide 。 • 要使用 Sun LDAP Schema 2（本机模式），请选择 2。
-m yes|no	回答以下问题：“是否要修改 Directory Server？”指定 yes 将修改目录。如果不希望修改目录，请指定 no。

选项	说明
-R <yes|no>	如果找到新索引并提供了 -m yes，则执行重新索引
-S *path-to-schema-files*	指定模式文件的目录路径。例如：./schema。

示例

```
# perl comm_dssetup.pl -i yes -c /var/opt/mps/serverroot -d slapd-budgie
-r o=internet -u o=usergroup -s yes -D "cn=Directory Manager" -w password -b
yes -t 1 -m yes
```

为 comm_dssetup.pl 脚本设置所有选项后，您可以在脚本实际运行之前看到以下摘要屏幕：

```
Here is a summary of the settings that you chose:
  Server Root                          : /var/opt/mps/serverroot/
  Server Instance                      : slapd-budgie
  Users/Groups Directory               : Yes
  Update Schema                        : yes
  Schema Type                          : 1
  DC Root                              : o=internet
  User/Group Root                      : o=usergroup
  Add New Indexes                      : yes
  Schema Directory                     : ./schema
  Directory Manager DN                : "cn=Directory Manager"
```

第 41 页的 “交互模式”部分中对每个选项作了进一步说明。

创建初始 Messaging Server 运行时配置

初始运行时配置程序将对 Messaging Server 进行配置，使其启动并运行。即创建**初始运行时配置**可以设置具有普通功能的 Messaging Server 配置。这就为您提供了基本工作配置，通过这些配置可以进行特定的自定义操作。此程序只应运行一次。以后运行此程序将会导致您的配置被覆写。要修改初始运行时配置，请使用下面介绍的以及 Sun Java System Messaging Server 管理指南 (http://docs.sun.com/doc/819-0106) 中介绍的配置实用程序。

Messaging Server 先决条件

在运行初始运行时配置程序前，您必须：

- 安装和配置 Administration Server。请参见 Sun Java Enterprise System 安装指南 (http://docs.sun.com/doc/819-0811)。如果不配置 Administration Server，您仍可以配置 Messaging Server，但却不能使用控制台管理 Messaging Server。
- 安装和配置 Directory Server。（请参见 Sun Java Enterprise System Installation Guide。）
- 运行 `comm_dssetup.pl` 程序。（请参见第 39 页的 “为 Messaging Server 配置准备 Directory Server”）。
- 在附录 E “安装工作单”中所提供的核对表中记录 Administration 和 Directory 安装和配置参数。

Messaging Server 配置核对表

运行 Messaging Server 初始运行时配置程序时，请记录表 E-4 第 848 页中的参数。要回答某些问题，请参阅 Messaging Server Deployment Planning Guide 中的 Directory Server 和 Administration Server 安装核对表。

运行配置程序

以下步骤将引导您配置 Messaging Server 初始运行时配置：

1. 使用以下命令调用 Messaging Server 初始运行时配置：

```
/msg_svr_base/sbin/configure [flag]
```

如果配置远程系统上的 Messaging Server，您可能需要使用 xhost(1) 命令。

表 1-1 介绍了您可以设置的用于 configure 程序的可选标志：

表 1-1 用于 Messaging Server configure 程序的可选标志

标志	说明
-nodisplay	调用命令行配置程序。
-noconsole	调用 GUI 用户界面程序。
-state *[statefile]*	使用无提示安装文件。必须与 -nodisplay 和 -noconsole 标志一起使用。请参见执行无提示安装。

运行 configure 命令后，配置程序将启动：

2. 欢迎

   配置程序的第一个面板是版权页面。选择 “下一步”继续或选择 “取消”退出。如果未配置 Administration Server，系统会向您发出警告，请选择 “确定”继续。

3. 输入全限定主机名 (FQHN)。

   这是将要运行 Messaging Server 的计算机。使用 Java Enterprise System 安装程序安装了服务器后，您可能已指定了物理主机名。但是，如果您正在安装群集环境，则需要使用逻辑主机名。您可以在此处更改原来指定的主机名。

4. 选择要存储配置和数据文件的目录。

   选择要存储 Messaging Server 配置和数据文件的目录。指定 *msg_svr_base* 下没有的路径名。将会在 *msg_svr_base* 下创建指向配置和数据目录的符号链接。有关这些符号链接的详细信息，请参见第 64 页的 “安装后的目录布局”。

   请确保您为这些文件留出了足够的磁盘空间。

5. 将显示一个小窗口，表示正在装入组件。

   这可能需要几分钟时间。

6. 选择要配置的组件

   选择要配置的 Messaging Server 组件。

   - Message Transfer Agent：处理路由、发送用户邮件并处理 SMTP 验证。MTA 提供对托管域、域别名和服务器端过滤器的支持。
   - Message Store：使用通用的 Message Store 为统一的邮件传送服务奠定基础。可通过多个协议（HTTP、 POP、 IMAP）访问邮件存储。如果仅配置 Message Store，您还必须选择 MTA。

- Messenger Express：处理 HTTP 协议对来自 Message Store 的邮件的检索。如果仅配置 Messenger Express，您还必须选择 Message Store 和 MTA。
- Messaging Multiplexor：作为组织内多个邮件传送服务器计算机的代理。用户连接到 Multiplexor 服务器，该服务器将每个连接重定向到相应的邮件服务器。默认情况下该组件未启用。如果确实选中了 MMP 和 Message Store，将在同一系统上启用这两个组件；系统将显示警告消息，要求您在配置之后更改端口号 （有关执行此操作的说明，请参见第 65 页的 “安装后的端口号”）。

  要配置 MMP，请参见第 7 章 “配置和管理多路复用器服务”和 Sun Java System Messaging Server Administration Reference (http://docs.sun.com/doc/819-0106)。

请选中要配置的所有组件，并取消选择不希望配置的组件。

7. 输入将拥有所配置文件的系统用户名和组。

   有关设置系统用户和组的信息，请参见第 38 页的 “创建 UNIX 系统用户和组”。

8. 配置 Directory Server 面板

   输入您的配置目录 LDAP URL、管理员和密码。这来自 Administration Server 配置。

   从 Directory Server 安装收集配置服务器 LDAP URL。请参见 Messaging Server Deployment Planning Guide (http://docs.sun.com/doc/819-0063) 中的 Directory Server 安装工作单。

   目录管理员在 Directory Server 和使用 Directory Server 的所有 Sun Java System 服务器 （例如 Messaging Server）上具有全部管理员权限，还对 Directory Server 中的所有条目具有完全管理权限。默认和建议的独特名称 (DN) 是 `cn=Directory Manager`，它是在配置 Directory Server 时设置的。

注 如果选择非默认值， Administration Server 和 Configuration Directory Server 之间将出现不匹配。这将需要手动执行配置后的步骤。因此仅当您清楚要执行的操作时，才可以更改此条目。

9. 用户 / 组 Directory Server 面板

   输入您的用户和组目录 LDAP URL、管理员和密码。

   从主机收集用户 / 组服务器 LDAP URL 信息，并从 Directory Server 安装收集端口号信息。请参见 Messaging Server Deployment Planning Guide (http://docs.sun.com/doc/819-0063) 中的 Directory Server 安装工作单。

   目录管理员在 Directory Server 和使用 Directory Server 的所有 Sun Java System 服务器（例如 Messaging Server）上具有全部管理员权限，并可以管理 Directory Server 中的所有条目。默认和建议的独特名称 (DN) 是 `cn=Directory Manager`，它是在配置 Directory Server 时设置的。

   如果根据复制的 Directory Server 实例进行安装，则必须指定拷贝目录 （而不是主目录）的证书。

10. 邮寄主管电子邮件地址

    输入邮寄主管电子邮件地址。

    请选择管理员能够有效监视的地址。例如，将 `pma@siroe.com` 作为 siroe 域中邮寄主管的地址。请注意，该地址不能以 “Postmaster” 开头。

    请注意，电子邮件地址的用户不会自动创建。因此您需要使用置备工具创建该用户。

11. 管理员帐户的密码

    输入初始密码，该初始密码将用作服务管理员密码、服务器密码、用户 / 组管理员密码、最终用户管理员权限密码以及 PAB 管理员密码和 SSL 密码。

    完成初始运行时配置之后，您可以为单个管理员帐户更改此密码。有关更多信息，请参见第 94 页的 “修改密码”。

12. 默认电子邮件域

    输入默认电子邮件域。

    此电子邮件域是在未指定其他域的情况下使用的默认域。例如，如果 `siroe.com` 是默认的电子邮件域，则发往未指定域的用户 ID 的邮件将会被发送到该域。

    如果您要使用用户管理实用程序（使用 Sun LDAP Schema 2 置备用户和组的命令行界面），则需要在其配置过程中指定相同的默认域。有关更多信息，请参见 Sun Java System Communications Services Delegated Administrator 指南 (http://docs.sun.com/doc/819-1103)。

13. 组织 DN

    输入组织 DN （将在其下创建用户和组）。默认值是用户 / 组后缀前置电子邮件域

    例如，如果用户 / 组后缀是 o=usergroup，而电子邮件域为 siroe.com，则默认值为 o=siroe.com，o=usegroup （其中 o=usergroup 为在第 39 页的 “为 Messaging Server 配置准备 Directory Server”中指定的用户 / 组目录后缀）。

    如果选择的用户 / 组目录后缀与组织 DN 相同，则创建托管域时可能会遇到迁移问题。如果要在初始运行时配置期间设置托管域，请在用户 / 组后缀的下一级指定一个 DN。

14. 准备配置

    配置程序将检查计算机上是否有足够的磁盘空间，然后简单列出准备配置的组件。

    要配置 Messaging Server 组件，请选择 “现在配置”。要更改任何配置变量，请选择 “返回”。或者选择 “取消”退出配置程序。

15. 启动 “任务序列”、“已完成的序列”和 “安装摘要”面板

    在最后的 “安装摘要”页面上选择 “详细资料”可以查看安装状态。要退出程序，请选择 “关闭”。

    在 */msg_svr_base*/install/configure_*YYYYMMDDHHMMSS*.log 中创建了一个日志文件，其中 *YYYYMMDDHHMMSS* 表示配置的年 （4 位数）、月、日、小时、分钟和秒。

    现在 Messaging Server 的初始运行时配置已设置完毕。要更改任何配置参数，请参见本文档其他部分中的相关说明。

要启动 Messaging Server，请使用以下命令：

```
/opt/SUNWmsgsr/sbin/start-msg
```

执行无提示安装

Messaging Server 初始运行时配置程序将自动创建无提示安装 *state* 文件 （称作 saveState），可以使用该文件在已安装 Messaging Server Solaris 软件包的部署中快速配置其他 Messaging Server 实例。该文件中记录了您对配置提示的所有响应。

您可以通过运行无提示安装使 configure 程序读取无提示安装 *state* 文件。以后进行 Messaging Server 初始运行时配置时， configure 程序将使用此文件中的响应，而不会再次询问相同的安装问题。如果在新的安装中使用 *state* 文件，您将无需回答任何问题。系统将自动应用 *state* 文件中的所有响应，将其作为新的安装参数。

无提示安装 *state* 文件 saveState 存储在 *msg_svr_base*/install/configure_*YYYYMMDDHHMMSS* 目录中，其中 *YYYYMMDDHHMMSS* 表示 saveState 文件的年 （4 位数）、月、日、小时、分钟和秒。

要使用无提示安装 *state* 文件在部署中的其他计算机上配置其他 Messaging Server 实例，请执行以下步骤：

1. 将无提示安装 *state* 文件复制到要执行新安装的计算机的临时区域中。
2. 根据需要查看和编辑无提示安装 *state* 文件。

   您可能希望更改 *state* 文件中的某些参数和具体设置。例如，新安装的默认电子邮件域可能与 *state* 文件中记录的默认电子邮件域不同。请记住， *state* 文件中列出的参数将会自动应用到此安装中。
3. 运行以下命令，以使用无提示安装文件配置其他计算机：

   msg_svr_base/sbin/configure -nodisplay -noconsole -state \
   fullpath/saveState

   其中 *fullpath* 是 saveState 文件所在位置的完整目录路径。（请参见本节中的步骤 1）。

注 运行无提示安装程序后，将在以下目录位置创建新的无提示安装 *state* 文件：*msg_svr_base*/install/configure_*YYYYMMDDHHMMSS*/saveState，其中 *YYYYMMDDHHMMSS* 表示包含 saveState 文件的目录的年（4 位数）、月、日、小时、分钟和秒。

针对 Directory Server 拷贝安装 Messaging Server

以下限制可能使您无法针对主 Directory Server 安装 Messaging Server：

- 不具有主 Directory Server 的证书。
- Messaging Server 无法与主 Directory Server 直接通信。

要针对 Directory Server 拷贝安装 Messaging Server，请执行以下步骤：

1. 如第 40 页的 “comm_dssetup.pl 要求”中所述，针对所有 Directory Server（包含 Directory Server 拷贝）运行 `comm_dssetup.pl` 程序。
2. 如 “创建初始 Messaging Server 运行时配置”中的步骤 8 和步骤 9 所述，使用复制的 Directory Server 证书运行 Messaging Server 的 `configure` 程序 （位于 *msg_svr_base*`/sbin/configure` 中）。

   由于权限无效， `configure` 程序尝试配置 Directory Server 管理员将失败。但是它将生成 *msg_svr_base*`/config/*.ldif` 文件，需要具有此文件才能对 Directory Server 拷贝拥有相应权限。
3. 将 `*.ldif` 文件移到主 Directory Server 中。
4. 对 `*.ldif` 文件运行 `ldapmodify` 命令。

   有关 `ldapmodify` 的详细信息，请参见 Sun Java System Directory Server 文档，或查看 *msg_svr_base*`/install/configure_`*YYYYMMDDHHMMSS*`.log` 文件。
5. 重新运行 `configure` 程序。

   现在 Directory Server 拷贝 （以及主 Directory Server）已配置完毕，可以与 Messaging Server 协同工作。

安装 Messaging Server 置备工具

以下各节提供了关于支持的置备工具的安装信息摘要：

- 第 55 页的 “Delegated Administrator for Messaging”
- 第 57 页的 “LDAP 置备工具”
- 第 38 页的 “创建 UNIX 系统用户和组”

Delegated Administrator for Messaging

Messaging Server 可以使用两个 GUI 置备工具 iPlanet Delegated Administrator (Sun LDAP Schema 1) 和 Communications Services Delegated Administrator (Sun LDAP Schema 2)。本节介绍了前一种 GUI 置备工具。有关后一种 GUI 置备工具的详细信息，请参见 Sun Java System Communications Services Delegated Administrator 指南 (`http://docs.sun.com/doc/819-1103`)。

要安装 iPlanet Delegated Administrator (Sun LDAP Schema 1)，需要从 Sun 软件页面将其下载。请与您的 Sun Java System 代表联系，以获得有关下载位置的信息。

注 只有在安装和配置了 Messaging Server 和 Web Server 之后才可以安装 iPlanet Delegated Administrator。有关安装 iPlanet Delegated Administrator 的更多信息，请参见 iPlanet Delegated Administrator 文档。

iPlanet Delegated Administrator 仅提供给已安装 Messaging Server 5.x 并且当前要安装 Messaging Server 6 的用户。对初次安装 Messaging Server 产品的用户不予提供。

必须将 iPlanet Delegated Administrator 与 Sun Java System Web Server 6.0 （仅与以前的 Messaging Server 5.2 产品捆绑）一起使用。不能将 Web Server 6.1 （与 Java Enterprise System 安装程序捆绑）与 iPlanet Delegated Administrator 一起使用。

请确保阅读 Sun Java System Messaging Server 发行说明 (http://docs.sun.com/doc/819-1052)。

安装步骤摘要：要使用 Messaging Server 安装和配置 iPlanet Delegated Administrator for Messaging，请执行以下操作：

注 安装以下产品时，请使用 Java Enterprise System 安装程序。请注意，某些产品有自己的配置，而其他产品的配置嵌入在 Java Enterprise System 安装程序 / 配置器中。有关详细信息，请参见特定的产品文档。

1. 确保已安装和配置 Sun Java System Directory Server 5.2。

   有关详细信息，请阅读相应的 Sun Java System Directory Server Installation Guide。

2. 安装和配置 Messaging Server。

   由于将不安装 Sun Java System Access Manager，因此 Messaging Server 将检测到您使用的是 Sun LDAP Schema 1。

3. 使用以前 Messaging Server 5.2 中捆绑的软件安装 Sun Java System Web Server 6.0。

   请查看 Sun Java System Web Server 文档和 Sun Java System Delegated Administrator 文档。

4. 安装 iPlanet Delegated Administrator for Messaging 1.2 Patch 2。请与您的 Sun 支持代表联系，以获得最新的版本。

   请参阅 iPlanet Delegated Administrator 文档。

LDAP 置备工具

可以使用 LDAP Directory 工具置备 Sun LDAP Schema 1 用户和组 （不支持 Schema 2）。

安装步骤摘要：

1. 如果尚未安装 Directory Server，请确保对其进行安装和配置。

   有关更多信息，请参阅 Sun Java Enterprise System 安装指南 (http://docs.sun.com/doc/819-0811)。

2. 配置 Access Manager 以识别 Directory Server 中的数据。

   在 Access Manager 可以识别 LDAP 目录中的数据之前，您必须将特殊对象类添加到将由 Access Manager 管理的所有组织、组和用户的条目中。如果尚未进行此操作，请先执行此操作，再开始置备新帐户。样例脚本已捆绑在 Access Manager 产品中，以帮助您将上述对象类自动添加到目录中。有关这些安装后的步骤的更多信息，请参见 Sun Java System Access Manager Migration Guide (http://docs.sun.com/doc/819-7645)。

3. 借助本指南安装和配置 Messaging Server。

   Messaging Server 将检测您使用的是哪一个 Sun Java System LDAP Schema，这取决于是否安装了 Access Manager。

4. 安装和配置 Sun Java System Web Server 6.1，以启用 Messenger Express 中的邮件过滤。有关启用邮件过滤的详细信息，请参见第 63 页的 “配置 Messenger Express 和 Communications Express 邮件过滤器”。要安装 Web Server，请参见 Sun Java Enterprise System 安装指南。

   虽然邮件过滤不是置备工具，但是它的功能存在于以前的 GUI 版本的 Delegated Administrator for Messaging 中。

5. 请参见 Sun Java System Messaging Server 文档以执行 LDAP 置备。

   对于 Sun LDAP Schema 1 LDAP 置备，请使用 Messaging Server 5.2 Provisioning Guide 和 Sun Java System Communications Services Schema Reference Manual。（Sun Java System Schema Reference Manual 包含用于 Sun LDAP Schema 1 和 v.2 的对象类和属性。）

SMTP 中继阻止

默认情况下，将 Messaging Server 配置为阻止尝试的 SMTP 中继，即拒绝从未经授权的外部源 （外部系统是指服务器本身所位于的主机之外的任何其他系统）到外部地址的尝试的邮件提交。此默认配置在阻止 SMTP 中继时相当主动，因为它将所有其他系统都认作外部系统。

安装后，请务必手动修改配置，以满足站点的需要。尤其是， Messaging Server 应该识别其自身的内部系统及子网，来自内部系统及子网的 SMTP 中继应该始终被接收。如果未升级此配置，则测试 MTA 配置时可能会遇到问题。

如果 IMAP 和 POP 客户机尝试通过 Messaging Server 系统的 SMTP Server 将邮件提交到外部地址时，并且未使用 SMTP AUTH (SASL) 进行验证，将会发现其提交尝试被拒绝。将哪些系统和子网视为内部系统通常由 `INTERNAL_IP` 映射表控制，在文件 *msg_svr_base*`/config/mappings` 中可以查看该表。

例如，在 IP 地址为 `192.45.67.89` 的 Messaging Server 系统上，默认的 `INTERNAL_IP` 映射表显示如下：

```
INTERNAL_IP

  $(192.45.67.89/24)  $Y
  127.0.0.1  $Y
  *  $N
```

初始条目 （使用 `$(IP-pattern/significant-prefix-bits)` 语法）指定与第一个 24 位的 `192.45.67.89` 匹配的任何 IP 地址都应该匹配并被视为内部地址。第二个条目将回送 IP 地址 `127.0.0.1` 视为内部地址。最后一个条目指定所有其他 IP 地址均不被视为内部地址。

您可以通过在最后的 $N 条目之前指定其他 IP 地址或子网来添加其他条目。这些条目必须在左侧指定 IP 地址或子网 （使用 $(.../...) 语法来指定子网）并在右侧指定 $Y。或者可以修改现有的 $(.../...) 条目，以接受更通用的子网。

例如，如果上述的同一样例站点具有 C 类网络，即拥有所有 192.45.67.0 子网，则此站点需要修改初始条目，使映射表显示如下：

```
INTERNAL_IP

  $(192.45.67.89/24)  $Y
  127.0.0.1  $Y
  *  $N
```

或者如果站点仅拥有 192.45.67.80-192.45.67.99 范围内的 IP 地址，则此站点将希望使用：

```
INTERNAL_IP

  ! Match IP addresses in the range 192.45.67.80-192.45.67.95
  $(192.45.67.80/28)  $Y
  ! Match IP addresses in the range 192.45.67.96-192.45.67.99
  $(192.45.67.96/30)  $Y
  127.0.0.1  $Y
  *  $N
```

请注意，*msg_svr_base*/sbin/imsimta test -match 实用程序在检查 IP 地址是否与特定的 $(.../...) 测试条件相匹配方面非常有用。 imsimta test -mapping 实用程序更普遍的用途是检查 INTERNAL_IP 映射表是否返回了各种 IP 地址输入所需的结果。

修改 INTERNAL_IP 映射表后，请务必执行 *msg_svr_base*/sbin/imsimta cnbuild 和 *msg_svr_base*/sbin/imsimta restart 实用程序，以使更改生效。

可以在 Sun Java System Messaging Server 管理指南 (http://docs.sun.com/doc/819-0106) 中找到有关映射文件和一般映射表格式以及关于 imsimta 命令行实用程序的详细信息。此外，可以在第 470 页的 “添加 SMTP 中继”中找到有关 INTERNAL_IP 映射表的信息。

在重新引导后启用启动

通过使用以下引导脚本，您可以在系统重新引导后启用 Messaging Server 启动：*msg_svr_base*/lib/Sun_MsgSvr。也就是说，在默认情况下，除非您运行该脚本，否则 Messaging Server 将不会在系统重新引导后重新启动。此外，此脚本还可以启动 MMP （如果已启用）。

要启用 Sun_MsgSvr，请执行以下操作：

1. 将 Sun_MsgSvr 脚本复制到 /etc/init.d 目录中。
2. 更改 Sun_MsgSvr 脚本的以下拥有权和访问模式：

表 1-2 对 Sun_MsgSvr 拥有权和访问模式的更改

拥有权 (chown(1M))	组拥有权 (chgrp(1M))	访问模式 (chmod(1M))
root （超级用户）	sys	0744

3. 转至 /etc/rc2.d 目录并创建以下链接：

```
ln /etc/init.d/Sun_MsgSvr S92Sun_MsgSvr
```

4. 转至 /etc/rc0.d 目录并创建以下链接：

```
ln /etc/init.d/Sun_MsgSvr K08Sun_MsgSvr
```

处理 sendmail 客户端

如果最终用户通过 sendmail 客户机发送邮件，则可以配置 Messaging Server，使其根据协议与客户机协同工作。用户可以继续使用 UNIX sendmail 客户端。

要使 sendmail 客户端和 Messaging Server 兼容，可以创建并修改 sendmail 配置文件。

注 每次将新的 sendmail 修补程序应用于系统时，都需要修改 submit.cf 文件（如以下关于 Solaris 9 及更高版本的说明中所述）。在 Solaris 8 上，请按照以下说明操作。

当您升级以前版本的 Messaging Server 时， /usr/lib/sendmail 二进制将由 sendmail 产品的组件替换。在 Messaging Server 6 2005Q1 中，升级过程中的这种替换将不再出现。因此，您需要从最新的 sendmail 修补程序中获得正确版本的 /usr/lib/sendmail 二进制。

Solaris 8

在 Solaris 8 操作系统上，请执行以下步骤：

1. 在目录 /usr/lib/mail/cf 中找到 main-v7sun.mc 文件并创建此文件的副本。

   在本节的示例中，创建了名为 sunone-msg.mc 的副本。

2. 在 sunone-msg.mc 文件中，将以下各行添加到 MAILER 宏之前：

```
FEATURE('nullclient', 'smtp:rhino.west.sesta.com')dnl
MASQUERADE_AS('west.sesta.com')dnl
define('confDOMAIN_NAME', 'west.sesta.com')dnl
```

   请注意， rhino.west.sesta.com 是本地主机名， west.sesta.com 是默认的电子邮件域 （如 “创建初始 Messaging Server 运行时配置”中的第 52 页的 “默认电子邮件域”所述）。在 HA 环境中，请使用逻辑主机名。有关用于高可用性环境的逻辑主机名的详细信息，请参见第 3 章 “配置高可用性”。

3. 编译 sunone-msg.mc 文件：

```
/usr/ccs/bin/make sunone-msg.cf
```

   sunone-msg.mc 将输出 sunone-msg.cf。

4. 创建 /etc/mail 目录中现有 sendmail.cf 文件的副本。

   a. 复制 /usr/lib/mail/cf/sunone-msg.cf，并将其重命名为 sendmail.cf 文件。

   b. 将新的 sendmail.cf 文件移到 /etc/mail 目录中。

Solaris 9 及更高版本

在 Solaris 9 平台上， sendmail 不再是 setuid 程序。它是一个 setgid 程序。

要在 Solaris 9 平台上创建 sendmail 配置文件，请执行以下操作：

1. 在目录 /usr/lib/mail/cf 中找到 submit.mc 文件并创建此文件的副本。

   在本节的示例中，创建了名为 sunone-submit.mc 的副本。

2. 将文件 sunone-submit.mc: 中的以下行：

```
FEATURE('msp')dn
```

   更改为

```
FEATURE('msp', 'rhino.west.sesta.com')dnl
```

   其中 rhino.west.sesta.com 是本地主机名。

   请注意， rhino.west.sesta.com 是本地主机名， west.sesta.com 是默认的电子邮件域 （如 “创建初始 Messaging Server 运行时配置”中的第 52 页的 “默认电子邮件域”所述）。在 HA 环境中，请使用逻辑主机名。有关用于高可用性环境的逻辑主机名的详细信息，请参见第 3 章 “配置高可用性”。

3. 编译 sunone-submit.mc 文件：

```
/usr/ccs/bin/make sunone-submit.cf
```

   sunone-submit.mc 将输出 sunone-submit.cf。

4. 创建 /etc/mail 目录中现有 submit.cf 文件的副本。

   a. 复制 /usr/lib/mail/cf/sunone-submit.cf 文件，并将其重命名为 submit.cf 文件。

   b. 将新的 submit.cf 文件移到 /etc/mail 目录中。

配置 Messenger Express 和 Communications Express 邮件过滤器

可以通过 Messenger Express 和 Communications Express 访问邮件过滤器。如果仅使用 Communications Express，则无需部署 .war 文件，但是要在 Messenger Express 中部署邮件过滤器，则需要发出以下命令：

如果使用 *Web Server* 作为 *Web* 容器：

```
# cd web_svr_base/bin/https/httpadmin/bin/
# ./wdeploy deploy -u /MailFilter -i https-srvr_instance -v
https-virtual_srvr_instance msg_svr_base/SUNWmsgmf/MailFilter.war
```

如果使用 *App Server* 作为 *Web* 容器：

```
# cd app_svr_base/sbin
# ./asadmin
asadmin> deploy --user admin msg_svr_base/SUNWmsgmf/MailFilter.war
```

在这两种情况下，设置以下 configutil 参数并重新启动 mshttpd：

```
# cd msg_svr_base/sbin/
# ./configutil -o "local.webmail.sieve.port" -v "WS_port_no|AS_port_no"
# ./stop-msg http
# ./start-msg http
```

您还可以使用管理控制台部署 .war 文件，有关更多信息，请参阅 《Sun Java System Web Server 6.1 管理员指南》(http://docs.sun.com/app/doc/819-0823) 或 《Sun Java System Application Server Enterprise Edition 8.1 管理指南 》(http://docs.sun.com/doc/819-1553)。

关于最终用户邮件过滤器的信息位于 Messenger Express 和 Communications Express 的联机帮助文件中。

性能和调节

请参阅位于 http://docs.sun.com/doc/819-0063 的 Messaging Server Deployment Planning Guide （特别是有关 Messaging Server 体系结构的性能注意事项的部分）。

安装后的目录布局

安装了 Sun Java System Messaging Server 后，其目录和文件将被放置在表 1-3 中描述的组织中。此表并不全面；它只显示了用户最感兴趣的、用于典型服务器管理任务的那些目录和文件。

表 1-3 安装后的目录和文件

目录	默认位置和说明
Messaging Server 基目录 (*msg_svr_base*)	/opt/SUNWmsgsr/ （默认位置）
	Messaging Server 计算机上用于保存服务器程序文件、配置文件、维护文件和信息文件的目录。
	请注意，每台计算机只允许有一个 Messaging Server 基目录。
配置目录 config	*msg_svr_base*/config/
	包含所有 Messaging Server 配置文件，例如 imta.cnf 和 msg.conf 文件。
	仅在 Solaris 和 Linux 平台上：此目录符号链接 （在 UNIX 平台上）到在初始运行时配置中指定的数据和配置目录的 config 子目录 （默认目录：/var/opt/SUNWmsgsr/）。
日志目录 log	*msg_svr_base*/log/
	包含 Messaging Server 日志文件，例如 mail.log_current 文件。
	仅在 Solaris 和 Linux 平台上：此目录符号链接 （在 UNIX 平台上）到在初始运行时配置中指定的数据和配置目录的 log 子目录 （默认目录：/var/opt/SUNWmsgsr/）。
数据目录 data	*msg_svr_base*/data/ （必需位置）
	包含数据库文件、配置文件、日志文件、站点程序文件、队列文件、存储文件和消息文件。
	data 目录包括 config 和 log 目录。
	仅在 Solaris 和 Linux 平台上：此目录符号链接 （在 UNIX 平台上）到在初始运行时配置中指定的数据和配置目录 （默认目录：/var/opt/SUNWmsgsr/）。
系统管理员程序目录 sbin	*msg_svr_base*/sbin/ （必需位置）
	包含 Messaging Server 系统管理员可执行的程序和脚本，例如 imsimta、configutil、 stop-msg、 start-msg 和 uninstaller。
库目录 lib	*msg_svr_base*/lib/ （必需位置）
	包含共享库文件、专用可执行程序和脚本文件、守护程序文件和不可定制的内容数据文件。例如：imapd 和 qm_maint.hlp。

表 1-3 安装后的目录和文件 （续）

目录	默认位置和说明
SDK 包含文件目录 `include`	*msg_svr_base*`/include/` （必需位置） 包含软件开发工具包 (SDK) 的 Messaging 头文件。
示例目录 `examples`	*msg_svr_base*`/examples/` （必需位置） 包含各种 SDK （例如 Messenger Express AUTH SDK）的示例。
安装数据目录 `install`	*msg_svr_base*`/install/` （必需位置） 包含与安装相关的数据文件，例如安装日志文件、无提示安装文件、出厂默认配置文件和初始运行时配置日志文件。

安装后的端口号

在安装程序和初始运行时配置程序中，需要为各种服务选择端口号。这些端口号可以是 1 到 65535 之间的任何数字。

表 1-4 列出了安装期间指定的端口号：

表 1-4 安装期间指定的端口号

端口号	服务 （configutil 参数）
389	安装 Directory Server 的计算机上的标准 Directory Server LDAP 端口。此端口在 Directory Server 安装程序中指定。 (`local.ugldapport`)
110	标准 POP3 端口。如果此端口与 MMP 端口安装在同一计算机上，则可能发生冲突。 (`service.pop.enable`)
143	标准 IMAP4 端口。如果此端口与 MMP 端口安装在同一计算机上，则可能发生冲突。 (`service.imap.port`)
25	标准 SMTP 端口。 (`service.http.smtpport`)
80	Messenger Express HTTP 端口。如果此端口与 Web Server 端口安装在同一计算机上，则可能发生冲突。 (`service.http.port`)
992	基于 SSL 的 POP3 端口。用于加密通信。 (`service.pop.sslport`)
993	基于 SSL 的 IMAP 端口。用于加密通信。如果此端口与 MMP 端口安装在同一计算机上，则可能发生冲突。 (`service.imap.sslport`)
443	基于 SSL 的 HTTP 端口。用于加密通信。 (`service.http.sslport`)
7997	Messaging and Collaboration ENS （事件通知服务）端口。
27442	作业控制程序用以进行内部产品通信的端口。

表 1-4 安装期间指定的端口号 （续）

端口号	服务 （configutil 参数）
49994	Watcher 用以进行内部产品通信的端口。有关 Watcher 的详细信息，请参见 Sun Java System Messaging Server 管理指南。(local.watcher.port)
用户指定的端口号	Administration Server HTTP 端口。（用于侦听控制台请求。）

如果某些产品安装在同一计算机上，则可能发生端口号冲突。表 1-5 显示了潜在的端口号冲突：

表 1-5 潜在的端口号冲突

冲突的端口号	端口	端口
143	IMAP Server	MMP IMAP Proxy
110	POP3 Server	MMP POP3 Proxy
993	基于 SSL 的 IMAP	具有 SSL 的 MMP IMAP Proxy
80	Web Server 端口	Messenger Express

建议您在可能的情况下将带有冲突端口号的产品安装在不同的计算机上。如果无法这样做，则需要更改其中一个冲突产品的端口号。

要更改端口号，请使用 configutil 实用程序。有关完整语法和用法，请参见 Sun Java System Messaging Server 管理指南 (http://docs.sun.com/doc/819-1056)。

以下示例使用 service.http.port configutil 参数将 Messenger Express HTTP 端口号更改为 8080。

```
configutil -o service.http.port -v 8080
```

第 2 章

升级到 Sun Java Systems Messaging Server

本章介绍了如何从 Messaging Server 5.2 升级到 Messaging Server 6 2005Q1。

开始之前

执行升级之前，请确保满足以下要求：

- 在与 Messaging Server 5.2 系统相同或不同的系统上安装和配置 Messaging Server 6 2005Q1。

注 与以前版本的 Messaging Server 不同，如果没有先安装并配置 Messaging Server 6 2005Q1，则无法升级现有的 Messaging Server。

另外请注意，不能对版本低于 5.2 的 Messaging Server 使用此升级程序。因此，必须首先迁移或升级到 Messaging Server 5.2，安装 Messaging Server 6 2005Q1，然后再运行此升级程序。有关迁移到 Messaging Server 5.2 的更多信息，请参见 《iPlanet Messaging Server 5.2 Migration Guide》 (http://docs.sun.com/source/816-6017-10/index.html)。

- 现有的 Messaging Server 5.2 安装被配置为使用 MTA Direct LDAP Lookup（而不是 `imsimta dirsync`）。
- 此外， Messaging Server 6 2005Q1 不支持多个实例。如果具有 Messaging Server 5.2 版的多个实例，则只能选择将一个实例升级到 Messaging Server 6 2005Q1。此外，多次运行升级实用程序以尝试迁移多个实例将覆写您的配置。

升级过程概述

从 Messaging Server 5.2 升级到 Messaging Server 6 2005Q1 包括三个步骤。以下主题概括了此过程：

1. 第 68 页的 “创建升级文件以更新配置”(`UpgradeMsg5toMsg6.pl`)
2. 第 71 页的 “运行升级实用程序”(`do_the_upgrade.sh`)
   - MTA 配置 (`make_mta_config_changes.sh`)
   - configutil 参数 (`make_configutil_changes.sh`)
   - 备份配置 (`make_backup_config_changes.sh`)
   - mboxlist 数据库 (`make_mboxlistdb_changes.sh`)
3. 第 74 页的 “迁移用户邮箱”（可选）

创建升级文件以更新配置

本节介绍了如何创建特殊的升级文件来更新 Messaging Server 6 2005Q1 系统上的配置：

- 第 68 页的 “关于升级文件”
- 第 70 页的 “运行 UpgradeMsg5toMsg6.pl Perl 脚本”

关于升级文件

运行升级实用程序从 Messaging Server 5.2 升级到 Messaging Server 6 之前，需要先运行 `UpgradeMsg5toMsg6.pl` Perl 脚本 （位于 *msg_svr_base*`/sbin`）。

`UpgradeMsg5toMsg6.pl` 将比较 Messaging Server 5.2 配置文件和 Messaging Server 6 配置文件，并为每个配置文件创建以下两个文件集：`*.CHANGES` 文件和 `*.MERGED` 文件。

将在工作区目录 `/var/tmp/UpgradeMsg5toMsg6.ScratchDir` 中生成 `*.CHANGES` 文件和 `*.MERGED` 文件。

*.CHANGES 文件显示了 Messaging Server 5.2 和 Messaging Server 6 2005Q1 之间的重要的配置文件差异。这些文件突出显示了仅在 Messaging Server 6 2005Q1 中找到的配置实体、来自 Messaging Server 5.2 但在 Messaging Server 6 2005Q1 中被淘汰的配置实体，以及仅在 Messaging Server 5.2 中找到的配置实体。请注意，并非所有 *.CHANGES 文件都会显示不同版本的配置文件之间的差异，而且并非所有配置文件都会生成 *.CHANGES 文件。

*.MERGED 文件合并了 Messaging Server 5.2 和 Messaging Server 6 配置的值和设置。通常，如果符合以下条件，Messaging Server 6 2005Q1 版本将保留 Messaging Server 5.2 的配置参数值：

- Messaging Server 6 2005Q1 版本中没有默认值，或
- 在 Messaging Server 5.2 配置中指定的值不是默认设置。

表 2-1 列出了生成 *.MERGED 或 *.CHANGES 文件的配置文件：

表 2-1 生成 *.MERGED 或 *.CHANGES 文件的 Messaging Server 配置文件

配置信息	说明	生成 *.MERGED 文件	生成 *.CHANGES 文件
job_controller.cnf	作业控制程序文件	X	X
conversions	转换文件	X	
*channel*_option（其中 *channel* 为 SMTP 通道）	SMTP 通道选项文件	X	
native_option	本地通道选项文件（*channel*_option 除外）	X	X
*channel*_headers.opt（其中 *channel* 为 SMTP 通道）	标头选项文件	X	
dispatcher.cnf	分发程序文件	X	X
imta_tailor	定制文件	X	X
option.dat	全局 MTA 选项文件	X	X
别名	别名文件	X	
imta.cnf	MTA 配置文件；仅更改了包含引用（如文件目录位置）。保留了 Messaging Server 5.2 配置中的重写规则和通道设置。要在 imta.cnf 中包含 LMTP，请从 Messaging Server 6 imta.cnf 文件中复制 LMTP 信息。	X	在某些实例中，可能会生成 *.CHANGES 文件。

表 2-1 生成 *.MERGED 或 *.CHANGES 文件的 Messaging Server 配置文件 （续）

配置信息	说明	生成 *.MERGED 文件	生成 *.CHANGES 文件
mappings	映射文件	X	
mappings.locale	本地化映射文件	X	
internet.rules	Internet 规则配置文件	X	
backup-groups.conf	备份组定义	X	X
configutil	对 local.conf 和 msg.conf 配置文件中的配置参数的更改。		X

运行 UpgradeMsg5toMsg6.pl Perl 脚本

要运行 UpgradeMsg5toMsg6.pl 以创建文件集 （通过此文件集可以更新配置），请执行以下步骤：

1. Messaging Server 5.2 和 Messaging Server 6 2005Q1 系统此时均可以运行。
2. 如果 Messaging Server 5.2 版和 Messaging Server 6 版不在同一计算机上，将 Messaging Server 5.2 *server-root* 目录传送、解压缩并复制到 Messaging Server 6 2005Q1 系统。如果两个版本安装在同一计算机上，则可以跳过此步骤。

   如果邮件存储过大，无法从一个系统传送到另一个系统，则可以仅将服务器实例的重要部分传送到新系统。 UpgradeMsg5toMsg6.pl 中的注释详细说明了这种情况。

   无需将 Messaging Server 5.2 存储数据复制到 Messaging Server 6 2005Q1 系统，但是必须确保在升级过程中可以访问 Messaging Server 5.2 mboxlist 目录。

3. 针对 Messaging Server 5.2 版的 `msg-`*instance* 和 Messaging Server 6 2005Q1 版的 *msg_svr_base* 运行 `UpgradeMsg5toMsg6.pl` 升级脚本 （位于 *msg_svr_base*`/sbin`）。例如：

```
perl UpgradeMsg5toMsg6.pl /usr/sunone/server5/msg-budgie \
  /opt/SUNWmsgsr
```

   其中 `/usr/sunone/server5/msg-budgie` 为 Messaging Server 5.2 的 `msg-`*instance*， `/opt/SUNWmsgsr` 为 Messaging Server 6 2005Q1 的 *msg_svr_base*。

   将创建 `*.MERGED` 和 `*.CHANGES` 文件 （如表 2-1 中所述）。

4. 请仔细查看 `*.MERGED` 文件；如果您不想使用建议的设置，则必须手动调整设置。

此实用程序无法更新 Messenger Express 定制文件。因此，需要手动更改这些文件，以保存来自 Messaging Server 5.2 的相关信息并添加来自 Messaging Server 6 2005Q1 安装的所有新信息。

运行升级实用程序

本节介绍了 `do_the_upgrade.sh` 实用程序 （位于 `/var/tmp/UpgradeMsg5toMsg6.ScratchDir`），该实用程序是由四个子脚本组成的 shell 脚本。本节包含以下主题：

- 第 72 页的 “升级实用程序概述”
- 第 72 页的 “运行 do_the_upgrade.sh 实用程序” (`do_the_upgrade.sh`)
- 第 73 页的 “MTA 配置” (`make_mta_config_changes.sh`)
- 第 73 页的 “configutil 参数” (`make_configutil_changes.sh`)
- 第 73 页的 “备份配置” (`make_backup_config_changes.sh`)
- 第 74 页的 “mboxlist 数据库” (`make_mboxlistdb_changes.sh`)

升级实用程序概述

do_the_upgrade.sh 实用程序由四个 shell 脚本组成，它使用 *.MERGED 文件更新 Messaging Server 6 2005Q1 系统中 MTA 配置的配置和文件目录位置、configutil 参数、备份参数以及 mboxlist 数据库。

您可以运行 do_the_upgrade.sh 实用程序，也可以单独运行组成 do_the_upgrade.sh 实用程序的一个或多个脚本（make_mta_config_changes.sh、 make_configutil_changes.sh、make_backup_config_changes.sh 和 make_mboxlistdb_changes.sh）。

如果希望将 MTA 中继计算机从 Messaging Server 5.2 升级到 Messaging Server 6 2005Q1，则只需运行 make_mta_config_changes.sh 和 make_backup_config_changes.sh（如第 73 页的 “备份配置”所述）。

执行 do_the_upgrade.sh 实用程序或任何子脚本时，请确保 Messaging Server 5.2 和 Messaging Server 6 2005Q1 均未启动和运行。

运行 do_the_upgrade.sh 实用程序

要运行 do_the_upgrade.sh 实用程序，请执行以下操作：

1. 将 Messaging Server 5.2 和 Messaging Server 6 都关闭。
2. 运行实用程序：

```
# sh /var/tmp/UpgradeMsg5toMsg6.ScratchDir/do_the_upgrade.sh
```

运行 do_the_upgrade.sh 脚本后，您可以继续引用 Messaging Server 5.2 的分区路径（但您将无法删除 Messaging Server 5.2 *server-root* 目录），也可以将 Messaging Server 5.2 的存储分区手动移动到相应的 Messaging Server 6 2005Q1 目录位置。您应该在重新启动 Messaging Server 之前执行此步骤。

MTA 配置

作为 do_the_upgrade.sh 实用程序组成部分的 MTA 升级配置子脚本称为 make_mta_config_changes.sh （位于 /var/tmp/UpgradeMsg5toMsg6.ScratchDir）。

make_mta_config_changes.sh 脚本将在 Messaging Server 6 2005Q1 文件目录结构内对 *.MERGED 服务器配置文件备份，然后将其改回原始名称并移至原始位置。

完成重命名并移动文件后，此脚本将自动运行 imsimta cnbuild 命令重新编译 MTA 配置。

注 如果希望将 MTA 中继计算机从 Messaging Server 5.2 升级到 Messaging Server 6 2005Q1，则只需运行 make_mta_config_changes.sh 和 make_backup_config_changes.sh （如第 73 页的 “备份配置”所述）。

configutil 参数

作为 do_the_upgrade.sh 实用程序组成部分的 configutil 升级配置子脚本称为 make_configutil_changes.sh 脚本 （位于 /var/tmp/UpgradeMsg5toMsg6.ScratchDir 中）。

make_configutil_changes.sh 脚本包含 msg.conf 和 local.conf 文件中的新参数或更新参数。如果 Messaging Server 6 2005Q1 中的 configutil 参数中未指定默认值，则所有 Messaging Server 5.2 中的值将在 Messaging Server 6 2005Q1 版中继续使用。

备份配置

作为 do_the_upgrade.sh 实用程序组成部分的备份升级配置子脚本称为 make_backup_config_changes.sh 脚本 （位于 /var/tmp/UpgradeMsg5toMsg6.ScratchDir 中）。

make_backup_config_changes.sh 脚本升级备份服务 （例如 backup-groups.conf 文件中的服务）的配置。

mboxlist 数据库

作为 do_the_upgrade.sh 实用程序组成部分的 mboxlist 数据库升级配置子脚本称为 make_mboxlistdb_changes.sh 脚本 （位于 /var/tmp/UpgradeMsg5toMsg6.ScratchDir）。

make_mboxlistdb_changes.sh 脚本传送 Messaging Server 5.2 的 mboxlist 数据库并将其升级到 Messaging Server 6 2005Q1 目录结构。此脚本将四个 *.db 文件（folder.db、quota.db、peruser.db 和 subscr.db）从 Messaging Server 5.2 系统上的 *server-root*/msg-*instance*/store/mboxlist 复制到 Messaging Server 6 2005Q1 系统上的 *msg_svr_base*/data/store/mboxlist。

迁移用户邮箱

本节介绍了如何将用户邮箱从 Messaging Server 5.2 系统迁移到 Messaging Server 6 2005Q1 系统。如果要将 Messaging Server 5.2 升级到 Messaging Server 6，并升级整个邮件存储数据库，则无需执行此过程。上一节中所述的 make_mboxlistdb_changes.sh 脚本可用于更有效地升级数据库。

您只需执行此过程，如果：

- 您要从 Windows 迁移到 UNIX 或从 UNIX 迁移到 Windows。
- 您不想一次全部迁移整个邮件存储。
- 您需要重命名您的用户，包括 UID、域名和默认域更改。

如果您选择使用此过程迁移邮箱，请不要将分区路径映射到 Messaging Server 5.2 分区，并且也不要运行 make_mboxlist_changes.sh 脚本。

由升级脚本生成的 make_configutil_changes.sh 脚本会自动将分区路径设置为映射到 Messaging Server 5.2 分区。您需要手动对其进行更改。此外，您应当从 do_the_upgrade.sh 脚本中删除 make_mboxlistdb_changes.sh 脚本的调用。

要以联机方式将用户邮箱数据从 Messaging Server 5.2 移动到 Messaging Server 6 2005Q1，请执行本节中介绍的步骤。移动数据时无需关闭 Messaging Server。

本节说明了以下主题：

- 第 75 页的 “要求”
- 第 75 页的 “迁移说明”

要求

迁移的唯一要求是在新旧邮件传送服务器上都要运行 stored。

迁移说明

要将用户邮箱从 Messaging Server 5.2 系统迁移到 Messaging Server 6 2005Q1 系统，请执行以下操作：

1. 事先通知用户，在数据移动过程完成之前，他们将无法访问邮箱。请确保用户已在数据移动开始之前从其邮件系统注销。
2. 将 Messaging Server 5.2 邮件存储中所有用户条目的 mailUserStatus 用户 LDAP 属性从 active 更改为 hold，以将传入的用户邮件保留在保留队列中，并防止通过 IMAP、 POP 和 HTTP 访问邮箱。

   有关 mailUserStatus 的更多信息，请参见 Sun Java System Communcations Services Schema Reference Manual (http://docs.sun.com/doc/819-0113)。
3. 确保在此过程期间 Messaging Server 5.2 和 Messaging Server 6 2005Q1 都已启动并正在运行。
4. 将所有用户条目中的 mailHost 属性从旧邮件服务器更改为新邮件服务器。

   要这样做，请使用以下 ldapsearch 命令查找需要修改其 mailHost 属性的用户条目：

```
ldapsearch -h ldap.siroe.com -b "o=internet" \
   "(&(objectclass=maildomain)(mailHost=oldmail.siroe.com))"
```

   然后使用 ldapmodify 命令将各个条目更改为相应的新邮件服务器。（使用 Messaging Server 和 / 或 Directory Server 附带的 ldapmodify。请勿使用 Solaris ldapmodify。）

   有关 mailhost 的更多信息，请参见 Sun Java System Communcations Services Schema Reference Manual。
5. 在旧系统中，使用 backup-groups.conf 文件将用户条目分为均等的组。（也可以将用户名放入文件，并在步骤 6 中使用 -u 选项）

6. 将用户数据从 Messaging Server 5.2 邮件存储移动到 Messaging Server 6 2005Q1 邮件存储中。

   完成此步骤的方法为：使用 `imsbackup` 实用程序备份 Messaging Server 5.2 邮件存储，然后使用 `imsrestore` 实用程序将邮件存储恢复到 Messaging Server 6 2005Q1 中。例如，要将邮箱从 `oldmail.siroe.com` 迁移到 `newmail.siroe.com`，请在 `oldmail.siroe.com` 上运行以下命令：

```
/<server-root>/bin/msg/store/bin/imsbackup -f- /<instance>/<group>      \
| rsh newmail.siroe.com /opt/SUNWmsgsr/lib/msg/imsrestore.sh   \
-f- -cy -v1
```

   您可以运行多个并发的备份和恢复会话 （每组一个），以使传送到新邮件存储的速率达到最大化。有关 `imsbackup` 和 `imsrestore` 实用程序的更多信息，请参见 Messaging Server 参考手册 (`http://docs.sun.com/doc/819-0106`) 以及第 543 页的 “备份并恢复邮件存储”。

7. 将 Messaging Server 6 2005Q1 设置为新的系统默认邮件传送服务器。

   将 `oldmail.siroe.com` 的 `A` 记录更改为指向 `newmail.siroe.com` （此服务器负责以前将 `oldmail.siroe.com` 作为主机的域）。

8. 执行以下命令释放 Messaging Server 5.2 系统上保留队列中的邮件：

```
imsimta process_held -uid=user -domain=domain
```

   其中 *user* 是用户 ID， *domain* 是用户所在的域。

9. 确保用户客户机将指向新的邮件服务器。

   升级完成后，通过用户的邮件客户机程序使用户指向新服务器 （在此示例中，使用户从 `oldmail.siroe.com` 指向 `newmail.siroe.com`）。

   或者使用 MMP，使用户无需将其客户机直接指向新邮件服务器。 MMP 将从存储在 LDAP 用户条目中的 `mailHost` 属性中获取此信息，并自动将客户机重定向到新服务器。

第 3 章

配置高可用性

本节提供了配置 Veritas Cluster Server 或 Sun Cluster 高可用性群集软件以及准备将该软件与 Messaging Server 配合使用所需的信息。假定您已阅读 Messaging Server Deployment Planning Guide (http://docs.sun.com/doc/819-0063) 中有关高可用性的章节，也阅读了有关详细规划、安装说明、必需的修补程序和其他所需信息的相应的 Veritas Cluster Server 或 Sun Cluster Server 文档。

表 3-1 列出了 Messaging Server 当前所支持的 Sun Cluster Server 和 Veritas Cluster Server 版本：

表 3-1 受支持的 Sun Cluster Server 和 Veritas Cluster Server 版本

群集	受支持的版本
Sun Cluster Server	Sun Cluster 3.1
Veritas Cluster Server	Veritas Cluster Server 1.3、 Veritas Cluster Server 2.0 和 Veritas Cluster Server 3.5

本章由以下各节组成：

- 第 78 页的 “群集代理安装”
- 第 79 页的 “Veritas Cluster Server 代理安装”
- 第 83 页的 “Sun Cluster 代理安装”
- 第 90 页的 “取消配置高可用性”

群集代理安装

群集代理是一种在群集框架下运行的 Messaging Server 程序。

Sun Cluster Messaging Server 代理 (SUNWscims) 是在您通过 Java Enterprise System 安装程序选择 Sun Cluster 3.1 时安装的。可以在 Java Enterprise System CD 的 Messaging Server Product 子目录 (Solaris_sparc/Product/messaging_svr/Packages/SUNWmsgvc) 中找到 Veritas Cluster Messaging Server 代理 (SUNWmsgvc)。（请注意，您必须使用 pkgadd(1M) 命令来安装 VCS 群集代理。）

Messaging Server 和高可用性注意事项

有关 Messaging Server 和高可用性 （适用于 Veritas Cluster 和 Sun Cluster）安装的一些说明项：

- 需要在安装和配置 Messaging Server 之前安装群集软件。在 Messaging Server 的 HA 逻辑主机名当前所指的群集节点上运行安装。当系统提示使用任何节点名称时，请使用群集别名。安装 Messaging Server 时，请通知 Administration Server，安装群集软件的节点是群集的逻辑名称 （不论涉及的是哪台物理计算机）。
- 运行 Messaging Server 初始运行时配置 （请参见第 49 页的 “创建初始 Messaging Server 运行时配置”）时，请确保指定 Messaging Server 群集的全限定 HA 逻辑主机名。
- 使用群集主机名来配置 Messaging Server。如果没有按此操作，您将需要使用群集主机名再一次重新配置。

使用 useconfig 实用程序

useconfig 实用程序使您可以在 HA 环境中的多个节点之间共享单一配置。此实用程序并不升级或更新现有配置。

例如，如果您正在升级第一个节点，则可以通过 Java Enterprise System 安装程序安装 Messaging Server，然后对其进行配置。随后，可以故障转移到第二个节点，在该节点上通过 Java Enterprise System 安装程序安装 Messaging Server 软件包，但不必再次运行初始运行时配置程序 (configure)。您也可以使用 useconfig 实用程序。

要启用该实用程序，请运行 useconfig 实用程序，以指向先前的 Messaging Server 配置。

```
msg_svr_base/sbin/useconfig install/configure_YYYYMMDDHHMMSS
```

其中， configure_*YYYYMMDDHHMMSS* 是先前的配置设置文件。

在一个全新的节点上，您可以在共享磁盘的 *msg_svr_base*/data/setup 目录中找到 configure_*YYYYMMDDHHMMSS*。

以下有关第 79 页的“Veritas Cluster Server 代理安装”和第 83 页的“Sun Cluster 代理安装”的章节介绍了您何时可以使用 useconfig 实用程序。

Veritas Cluster Server 代理安装

可以使用 Veritas Cluster Server 1.3、2.0 和 3.5 配置 Messaging Server。本节中的说明只涵盖 Veritas Cluster 3.5；有关 Veritas 1.3 和 2.0 的说明，请查阅 Sun Java Enterprise System 安装指南 (http://docs.sun.com/doc/819-0811)。

执行以下步骤之前，请确保查阅 Veritas Cluster Server 文档。

注

- Veritas Volume Manager (VxVM) 的群集功能需要获得单独许可。此功能提供有关共享存储的文件系统全局视图，与 Sun Cluster 3.0 全局文件系统类似。有关详细信息，请参见 Veritas Cluster Server 文档。
- FsckOpt 在 3.5 之前的 Veritas 版本中是可选项。不过，它是配置 Mount 资源所必需的。FsckOpt 必须包括 -y 或 -n，否则资源将无法在线使用。
- Veritas Cluster Server 2.0 Explorer 不能用于管理 Veritas Cluster Server 3.5。

通过 Java Enterprise System 安装程序安装 Messaging Server 并配置 HA 之后，请确保查阅第 88 页的 “在服务器上绑定 IP 地址”以了解与配置 HA 支持相关的其他步骤。

Veritas Cluster Server 的要求

- 已安装和配置了 Veritas Cluster 软件。
- 如以下说明 （位于第 80 页的 “VCS 3.5 安装和配置说明”中）所述，您将在两个节点上安装 Messaging Server 的 Veritas Cluster 代理软件包和 Messaging Server 软件。

VCS 3.5 安装和配置说明

以下说明介绍了如何使用 Veritas Cluster Server 3.5 将 Messaging Server 配置为 HA 服务。

默认的 `main.cf` 配置文件将设置名为 `ClusterService` 的资源组，该资源组将启动 `VCSweb` 应用程序。此资源组包含诸如 `csgnic` 和 `webip` 等网络逻辑主机 IP 资源。此外，还会为事件通知创建 `ntfr` 资源。

1. 从其中的一个节点启动 Cluster Explorer。

   请注意，这些 Veritas Cluster Server 说明假设您正在使用图形用户界面以将 Messaging Server 配置为 HA 服务。

   要启动 Cluster Explorer，请运行以下命令：

```
# /opt/VRTSvcs/bin/hagui
```

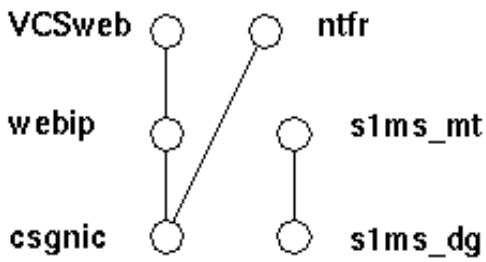
   为了使用 GUI，必须安装 `VRTScscm` 软件包。

2. 添加 `DiskGroup` 类型的 `s1ms_dg` 磁盘组资源并启用它。
3. 添加 `Mount` 类型的 `s1ms_mt` 安装资源。
   a. 与在 Veritas Cluster Server 2.0 中不同，您必须将 `-y` （或 `-n`）添加到 `FsckOpt`。空选项将导致 `Mount` 挂起。有关 `fsck_vxfs` 的详细信息，请参见 Solaris 手册页。
   b. 如果尚未启用链接资源，请确保单击 “链接”按钮以启用链接资源。

4. 在 s1ms_mt 和 s1ms_dg 之间创建一个链接。启用 s1ms_mt 资源。

   下图说明相关性树：

   图 3-1 Veritas Cluster Server 相关性树



5. 运行 Java Enterprise System 安装程序，选择 Administration Server 和 Messaging Server。

   a. 在配置 Administration Server 期间，请确保在系统要求提供主机名时指定逻辑主机名。

   b. 从主节点 （例如， Node_A）运行 Messaging Server 初始运行时配置以安装 Messaging Server。

   c. 使用 pkgadd(1M) 命令安装 Veritas Cluster Server 代理软件包 SUNWmsgvc （位于 Java Enterprise System CD 上的 Messaging Server Product 子目录中）。

      至此，已将 Messaging Server 和 Veritas 代理安装在 Node_A 上。

6. 切换至备份节点 （例如， Node_B）。

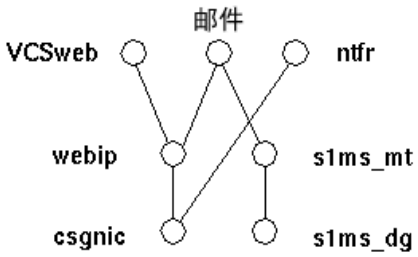
7. 运行 Java Enterprise System 安装程序，以在备份节点 (Node_B) 上安装 Messaging Server。

8. 安装 Messaging Server 之后，您可以使用 useconfig 实用程序，而不必在备份节点 (Node_B) 上创建其他初始运行时配置。 useconfig 实用程序使您可以在 HA 环境中的多个节点之间共享单一配置。此实用程序并不升级或更新现有配置。请参见第 78 页的 “使用 useconfig 实用程序”。

   至此，已将 Veritas 代理安装在 Node_B 上。

9. 从 Cluster Explorer 的 “文件” 菜单 （将显示文件选择框）中选择 “导入类型 ...”。
10. 从 `/etc/VRTSvcs/conf/config` 目录中导入 `MsgSrvTypes.cf` 类型。导入此类型文件。请注意，您需要在群集节点上才能找到此文件。
11. 现在创建一个 `MsgSrv` 类型的资源 （例如， `Mail`）。此资源需要设置逻辑主机名属性。
12. `Mail` 资源取决于 `s1ms_mt` 和 `webip`。如以下相关性树所示，在资源之间创建链接：

图 3-2 Veritas Cluster 相关性树



   a. 启用所有的资源并使 `Mail` 联机。
   b. 应该启动所有的服务器。
13. 切换至 Node_A 并检查高可用性配置是否正在工作。
14. 将组属性 `OnlineRetryLimit` 从 `3` 改为 `0`，否则可能会在同一节点上重新启动故障转移服务。

MsgSrv 属性

本节介绍了控制 `mail` 资源行为的 `MsgSrv` 附加属性。要使用 Veritas Cluster Server 配置 Messaging Server，请参见表 3-2。

表 3-2 Veritas Cluster Server 属性

属性	说明
`FaultOnMonitorTimeouts`	如果未设置 (=0)，则监视器 （探测）超时不会被视为资源故障。建议将此属性值设置为 2。如果监视器超时两次，则将重新启动资源或进行故障转移。

表 3-2 Veritas Cluster Server 属性 （续）

属性	说明
ConfInterval	计数故障 / 重新启动的时间间隔。如果在此期间服务仍然处于联机状态，则将删除先前的历史记录。建议设为 600 秒。
ToleranceLimit	监视器返回 OFFLINE 以声明资源故障的次数。建议将此值保留为 “0”（默认值）。

Sun Cluster 代理安装

本节介绍了如何安装 Messaging Server 以及如何将其配置为 Sun Cluster 高可用 (HA) 数据服务。此安装说明适用于 Sun Cluster 3.1。本节包含以下主题：

- 第 83 页的 “Sun Cluster 的要求”
- 第 84 页的 “关于 HAStoragePlus”
- 第 84 页的 “使用 Sun Cluster 和 HA StoragePlus 配置 Messaging Server”
- 第 88 页的 “在服务器上绑定 IP 地址”

可以在以下位置找到 Sun Cluster 3.1 的文档：

http://docs.sun.com/db/prod/cluster#hic

请注意， Sun Cluster 3.1 支持 Veritas 文件系统 (VxFS)。

Sun Cluster 的要求

本节假定以下情况：

- 在 Solaris 8 或 9 操作系统 （具有必需的修补程序）中安装并配置了 Sun Cluster 3.1。
- 您的系统上安装了 Sun Cluster 代理 SUNWscims。
- 如果要创建逻辑卷，可使用 Solstice DiskSuite 或 Veritas 卷管理器。

关于 HAStoragePlus

强烈建议您使用 HAStoragePlus 资源类型以使本地安装的文件系统在 Sun Cluster 环境中实现高可用性。位于 Sun Cluster 全局设备组中的任何文件系统均可以与 HAStoragePlus 结合使用。与全局安装的文件系统 （例如 HAStorage）不同，HAStoragePlus 只能在任何给定的时间点在一个群集节点上使用。这些本地安装的文件系统只能在故障转移模式和故障转移资源组中使用。与 HAStorage 的 GFS （全局文件系统）不同， HAStoragePlus 提供 FFS （故障转移文件系统）。

HAStoragePlus 具有许多优点：

- HAStoragePlus 可以完全避开全局文件服务层。对于磁盘 IO 密集的数据服务，这会显著提高性能。
- HAStoragePlus 可以与任何文件系统 （例如， UFS、 VxFS 等），甚至是那些可能无法与全局文件服务层一同工作的文件系统协同工作。如果 Solaris 操作系统支持某一文件系统，则该文件系统可与 HAStoragePlus 协同工作。

有关 HAStoragePlus 的详细信息，请阅读 《 Sun Cluster 3.1 **数据服务规划和管理指南** 》。

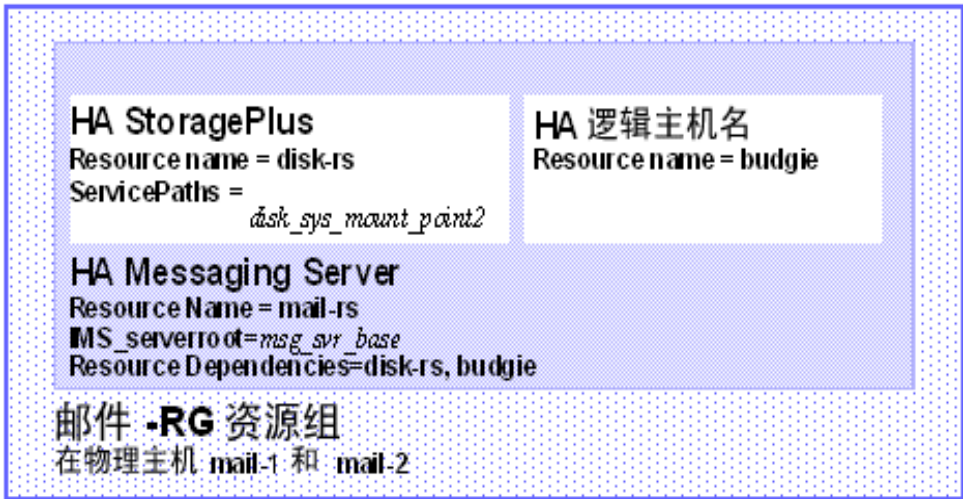
使用 Sun Cluster 和 HA StoragePlus 配置 Messaging Server

本节介绍了如何通过简单的示例为 Sun Cluster 3.1 配置 Sun Java System Messaging Server 的 HA 支持和 HA StoragePlus。

配置 HA 后，请确保查阅第 88 页的 “在服务器上绑定 IP 地址”以了解与 HA 支持相关的其他步骤。

以下示例假设已使用 HA 逻辑主机名和 IP 地址配置了邮件传送服务器。假设物理主机名为 `mail-1` 和 `mail-2`， HA 逻辑主机名为 `budgie`。图 3-3 说明了您在配置 Messaging Server HA 支持时要创建的不同 HA 资源的嵌套相关性。

图 3-3 简单 Sun Java System Messaging Server HA 配置



1. 成为超级用户并打开控制台。

   以下所有 Sun Cluster 命令都要求您已使用超级用户身份登录。您还需要有一个控制台或窗口来查看输出到 `/dev/console` 中的邮件。

2. 添加所需的资源类型。

   配置 Sun Cluster 以了解要使用的资源类型。这可以使用 `scrgadm -a -t` 命令来完成：

   ```
   # scrgadm -a -t SUNW.HAStoragePlus
   # scrgadm -a -t SUNW.ims
   ```

3. 为 Messaging Server 创建资源组。

   如果您尚未执行此操作，请创建一个资源组并使其显示在要运行 Messaging Server 的群集节点上。以下命令将创建名为 `MAIL-RG` 的资源组，并使其显示在 `mail-1` 和 `mail-2` 群集节点上。

   ```
   # scrgadm -a -g MAIL-RG -h mail-1,mail-2
   ```

   当然，您可以按照您的意愿对资源组使用任何名称。

4. 创建 HA 逻辑主机名资源并启动资源组。

   如果尚未执行此操作，请为 HA 逻辑主机名创建并启用资源，将其置于资源组中。以下命令使用逻辑主机名 `budgie` 执行此操作。因为忽略了 `-j` 切换，所以创建的资源名称将仍旧为 `budgie`。

   ```
   # scrgadm -a -L -g MAIL-RG -l budgie
   # scswitch -Z -g MAIL-RG
   ```

5. 创建 HAStoragePlus 资源。

   接下来，您需要为 Messaging Server 所依据的文件系统创建 HAStoragePlus 资源类型。以下命令将创建名为 `disk-rs` 的 HAStoragePlus 资源，并会将文件系统 *disk_sys_mount_point* 置于其控件之下：

   ```
   # scrgadm -a -j disk-rs -g MAIL-RG \
   -t SUNW.HAStoragePlus \
   -x ServicePaths=disk_sys_mount_point-1, disk_sys_mount_point-2
   ```

   以逗号分隔的 `ServicePaths` 列表是 Messaging Server 所依据的群集文件系统的装入点。在以上示例中，仅指定了两个装入点 *disk_sys_mount_point-1* 和 *disk_sys_mount_point-2*。如果某个服务器具有其所依据的附加文件系统，则您可以创建附加的 HA 存储资源并在步骤 10 中指示该附加相关性。

6. 安装和配置 Administration Server （请参见 Sun Java Enterprise System 安装指南）。

   在指定全限定域名时，请使用步骤 4 中创建的 HA 逻辑主机名。

7. 安装和配置 Messaging Server。请参见第 49 页的 “创建初始 Messaging Server 运行时配置”。

   a. 在初始运行时配置中，您需要在第 49 页的 “创建初始 Messaging Server 运行时配置”中指定配置目录。请确保使用 HAStoragePlus 资源的共享磁盘目录路径。

   b. 运行以下命令以启用 Sun Cluster 下的 watcher 进程：

```
configutil -o local.autorestart -v 1
```

有关 watcher 进程的更多信息，请参阅第 *101* 页的 “失败的服务或未响应服务的自动重新启动”。

8. 运行 ha_ip_config 脚本以设置 service.listenaddr 和 service.http.smtphost 并配置 dispatcher.cnf 和 job_controller.cnf 文件，从而实现高可用性。该脚本可确保为这些参数和文件设置逻辑 IP 地址，而非物理 IP 地址。它还启用 watcher 进程 （将 local.watcher.enable 设置为 1）和自动重新启动进程 （将 local.auto.restart 设置为 1）。

   有关运行该脚本的说明，请参见第 88 页的 “在服务器上绑定 IP 地址”。

   只能在具有共享磁盘 （用于配置和数据）的计算机上运行一次 ha_ip_config 脚本。

9. 修改 imta.cnf 文件并用群集的逻辑名称替换所有出现的物理主机名。

10. 创建 HA Messaging Server 资源。

    现在应该创建 HA Messaging Server 资源并将其添加到资源组。此资源取决于 HA 逻辑主机名和 HA 磁盘资源。

    在创建 HA Messaging Server 资源时，我们需要指示指向 Messaging Server 顶层目录的路径，即 *msg_svr_base* 路径。如以下命令所示，这些操作可通过使用 IMS_serverroot 扩展属性来完成。

    ```
    # scrgadm -a -j mail-rs -t SUNW.ims -g MAIL-RG \
              -x IMS_serverroot=msg_svr_base \
              -y Resource_dependencies=disk-rs,budgie
    ```

    以上命令为 Messaging Server （安装在 *msg_svr_base* 目录的 IMS_serverroot 中）创建名为 mail-rs 的 HA Messaging Server 资源。 HA Messaging Server 资源取决于 HA 磁盘资源 disk-rs 和 HA 逻辑主机名 budgie。

    如果 Messaging Server 具有附加文件系统相关性，则您可以为这些文件系统创建附加 HA 存储资源。请确保在以上命令的 Resource_dependencies 选项中包含该附加 HA 存储资源名。

11. 从 /etc/vfstab 文件中删除术语 global。引导时，必须将 /etc/vbstab 设置为 no。有关详细信息，请参见 Sun Cluster 3.1 文档。

    使用 HAStoragePlus 启用 vfstab 文件之前，可能要首先 umount 当前为全局文件系统的文件系统。然后可以使用 HAStoragePlus 来启用 vfstab 文件并重新安装文件系统。

12. 启用 Messaging Server 资源。

    现在应该激活 HA Messaging Server 资源，从而使邮件传送服务器联机。要执行此操作，请使用命令

    ```
    # scswitch -e -j mail-rs
    ```

    以上命令将启用 MAIL-RG 资源组的 mail-rs 资源。因为 MAIL-RG 资源先前已联机，所以上述命令也会使 mail-rs 联机。

13. 验证上述操作是否正在生效。

    使用 scstat 命令以查看 MAIL-RG 资源组是否联机。您可能需要查看导向控制台设备的输出，以了解所有诊断信息。另外，还需查看 syslog 文件中的 /var/adm/messages。

14. 将资源组故障转移至其他群集节点，以确保故障转移正常工作。

    将资源组手动故障转移至其他群集节点。（请确保您对故障转移到的节点具有超级用户权限。）

    使用 scstat 命令查看资源组当前正在哪个节点上运行 （“联机”）。例如，如果该资源组在 mail-1 上联机，则使用以下命令将其故障转移至 mail-2：

    ```
    # scswitch -z -g MAIL-RG -h mail-2
    ```

如果您正在升级第一个节点，则可以通过 Java Enterprise System 安装程序安装 Messaging Server，然后对其进行配置。随后，可以故障转移到第二个节点，在该节点上通过 Java Enterprise System 安装程序安装 Messaging Server 软件包，但不必再次运行初始运行时配置程序 (configure)。您也可以使用 useconfig 实用程序。

在服务器上绑定 IP 地址

如果使用的是对称或 N + 1 高可用性模型，则应该在配置期间注意一些附加设置，以便为 Messaging Server 准备 Sun Cluster Server。

在服务器上运行的 Messaging Server 需要有正确的 IP 地址与其绑定。这是在 HA 环境中正确配置邮件传送所必需的。

配置 HA 的 Messaging Server 的一部分工作涉及为实现连接而配置 Messaging Server 绑定和侦听所使用的接口地址。默认情况下，服务器将绑定到所有可用的接口地址。但是，在 HA 环境下，您需要将服务器专门绑定到与 HA 逻辑主机名关联的接口地址。

因此，将使用脚本来配置服务器 （属于给定的 Messaging Server 实例）所使用的接口地址。请注意，脚本通过 IP 地址标识接口地址，此 IP 地址已经或将要与服务器所使用的 HA 逻辑主机名相关联。

该脚本通过修改或创建以下配置文件来实现配置更改。对于文件

msg_svr_base/config/dispatcher.cnf

该脚本为 SMTP 和 SMTP Submit 服务器添加或更改 INTERFACE_ADDRESS 选项。对于文件

msg_svr_base/config/job_controller.cnf

该脚本为作业控制器添加或更改 INTERFACE_ADDRESS 选项。

最后，它将设置供 POP、 IMAP 和 Messenger Express HTTP 服务器使用的 configutil service.listenaddr 和 service.http.smtphost 参数。

请注意，原始配置文件 （如果有）将被重命名为 *.pre-ha。

按照以下方式运行该脚本：

1. 成为超级用户。
2. 执行 *msg_svr_base*/sbin/ha_ip_config
3. 该脚本将显示下述问题。通过键入 control-d 来响应其中的任何一个问题，可能会中止该脚本。这些问题的默认答案将显示在方括号 [ ] 中。要接受默认答案，只需按 RETURN 键。

   a. 逻辑 IP 地址：指定已分配给逻辑主机名 （Messaging Server 将使用）的 IP 地址。必须将 IP 地址指定为带有圆点的十进制数字形式，例如，123.456.78.90。

      逻辑 IP 地址是在 configutil 参数 service.http.smtphost 中自动设置的，您可以使用此 IP 地址来查看哪台计算机正在运行群集中的邮件传送系统。例如，如果您使用的是 Messenger Express，则服务器可以确定从哪台邮件主机发送外发邮件。

   b. Messaging Server Base (*msg_svr_base*)：指定在其中安装 Messaging Server 的顶层目录的绝对路径。

   c. 是否希望更改以上任何选项：回答 “否”将接收您的答案并实现配置更改。如果希望更改答案，则回答 “是”。

注 此外， ha_ip_config 脚本将使用以下参数自动启用两个新的进程 watcher 和 msprobe：local.autorestart 和 local.watcher.enable。这两个新的参数将协助监视邮件传送服务器的运行状况。进程故障和服务未响应都会导致显示指示特定故障的日志消息。群集代理现在将监视 watcher 进程并在退出时进行故障转移。请注意，为了使 Sun Cluster 正常工作，必须启用这两个参数。

有关 watcher 和 msprobe 进程的详细信息，请参见第 101 页的 “失败的服务或未响应服务的自动重新启动”。

取消配置高可用性

本节介绍如何取消配置高可用性。要卸载高可用性，请按照 Veritas 或 Sun Cluster 文档中的说明进行操作。

根据您要删除 Veritas Cluster Server 还是 Sun Cluster，高可用性取消配置说明会有所不同。

本节包含以下主题：

- 第 90 页的 “取消配置 Veritas Cluster Server”
- 第 91 页的 “为 Sun Cluster 3.x 取消配置 Messaging Server HA 支持”

取消配置 Veritas Cluster Server

要取消配置 Veritas Cluster Server 的高可用性组件，请执行以下操作：

1. 使 `iMS5` 服务组脱机并禁用其资源。
2. 删除 `mail` 资源、 `logical_IP` 资源和 `mountshared` 资源之间的相关性。
3. 使 `iMS5` 服务组返回联机状态，以使 `sharedg` 资源可用。
4. 删除安装期间创建的所有 Veritas Cluster Server 资源。
5. 停止 Veritas Cluster Server 并删除两个节点上的以下文件：

   ```
   /etc/VRTSvcs/conf/config/MsgSrvTypes.cf
   /opt/VRTSvcs/bin/MsgSrv/online
   /opt/VRTSvcs/bin/MsgSrv/offline
   /opt/VRTSvcs/bin/MsgSrv/clean
   /opt/VRTSvcs/bin/MsgSrv/monitor
   /opt/VRTSvcs/bin/MsgSrv/sub.pl
   ```

6. 从两个节点上的 `/etc/VRTSvcs/conf/config/main.cf` 文件中删除 Messaging Server 条目。
7. 从两个节点中删除 `/opt/VRTSvcs/bin/MsgSrv/` 目录。

为 Sun Cluster 3.x 取消配置 Messaging Server HA 支持

本节介绍了如何为 Sun Cluster 撤消 HA 配置。本节假设简单的示例配置（如 第 83 页的 “Sun Cluster 代理安装”中所述）。对于其他配置，具体的命令 （例如，步骤 3）可能会不同，但会遵循相同的逻辑顺序。

1. 成为超级用户。

   以下所有 Sun Cluster 命令都要求您以超级用户身份运行。

2. 使资源组脱机。

   要关闭资源组中的所有资源，请发布命令

   ```
   # scswitch -F -g MAIL-RG
   ```

   这将关闭资源组中的所有资源 （例如 Messaging Server 和 HA 逻辑主机名）。

3. 禁用各个资源。

   下一步，使用以下命令从资源组逐个删除资源：

   ```
   # scswitch -n -j mail-rs
   # scswitch -n -j disk-rs
   # scswitch -n -j budgie
   ```

4. 从资源组删除各个资源。

   禁用资源后，您可以使用以下命令从资源组逐个删除资源：

   ```
   # scrgadm -r -j mail-rs
   # scrgadm -r -j disk-rs
   # scrgadm -r -j budgie
   ```

5. 删除资源组。

   从资源组删除所有资源后，可以使用以下命令删除资源组本身：

   ```
   # scrgadm -r -g MAIL-RG
   ```

6. 删除资源类型 （可选）。

   如果需要从群集中删除资源类型，请发布以下命令：

   ```
   # scrgadm -r -t SUNW.ims
   # scrgadm -r -t SUNW.HAStoragePlus
   ```

第 4 章

配置一般邮件传送能力

本章介绍可以通过使用 Sun ONE Server Console （以下简称 Console）或使用命令行实用程序执行的一般 Messaging Server 任务，例如启动和停止服务以及配置目录访问。特定于各个 Messaging Server 服务 （例如 POP、 IMAP、 HTTP 和 SMTP）的任务将在后续各章中介绍。本章包含以下各节：

- 第 94 页的 “修改密码”
- 第 95 页的 “管理邮件用户，邮递列表和域”
- 第 96 页的 “通过 Sun ONE Console 管理 Messaging Server”
- 第 97 页的 “启动和停止服务”
- 第 101 页的 “失败的服务或未响应服务的自动重新启动”
- 第 103 页的 “安排自动任务时间”
- 第 104 页的 “配置问候邮件”
- 第 107 页的 “设置用户首选语言”
- 第 108 页的 “自定义目录查找”
- 第 111 页的 “加密设置”
- 第 111 页的 “设置故障转移 LDAP 服务器”

修改密码

由于在初始配置期间为多个管理员设置的密码相同（请参见第 49 页的 “创建初始 Messaging Server 运行时配置”），因此您可能希望更改这些管理员的密码。

请参见表 4-1，该表显示了在初始运行时配置期间用来设置默认密码的参数以及可用来更改默认密码的实用程序。有关那些使用 `configutil` 实用程序更改的参数，请参见完整的语法和用法。

表 4-1 在 Messaging Server 初始运行时配置期间设置的密码

参数	说明
`local.ugldapbindcred`	通过 `configutil` 实用程序设置的用户 / 组管理员密码。
`local.service.pab.ldappasswd`	由绑定 DN 指定的用户进行 PAB 搜索时使用的密码，该密码通过 `configutil` 实用程序进行设置。
密钥文件的 SSL 密码	在 `sslpassword.conf` 文件中直接设置的密码。
服务管理员证书	这些证书是在 LDAP Directory 中直接设置的（使用 `ldapmodify` 命令）。
Delegated Administrator 的服务管理员	仅当已启用 Sun LDAP Schema 1 并要使用 iPlanet Delegated Administrator 实用程序时，您才需更改此管理员密码。 您可以在 Sun ONE Console、 LDAP Directory （使用 `ldapmodify` 命令）或 Delegated Administrator UI 中更改 Delegated Administrator 服务管理员密码。
存储管理员	您可以在 Sun ONE Console 或 LDAP Directory （使用 `ldapmodify` 命令）中更改存储管理员密码。

以下示例使用 `local.enduseradmincred configutil` 参数更改了最终用户管理员的密码。

```
configutil -o local.enduseradmincred -v newpassword
```

管理邮件用户，邮递列表和域

所有用户、邮递列表和域信息都将存储为 LDAP 目录中的条目。 LDAP 目录可以包含有关组织的员工、成员、客户或以各种方式 “属于” 组织的其他类型个人的广泛信息。这些个人构成了组织的**用户**。

在 LDAP 目录中，有关用户的信息采用了有利于高效搜索的结构形式，每个用户条目都由一组属性标识。与用户相关联的目录属性可以包含用户的名称和其它标识、部门成员资格、作业分类、物理位置、管理员的名称、直接下属的名称、对组织各部分的访问权限以及各种首选项。

在具有电子邮件传送服务的组织中，许多用户 （如果不是所有用户）都具有邮件帐户。对于 Messaging Server，邮件帐户信息不存储在本地服务器上，而是 LDAP 用户目录的一部分。每个邮件帐户的信息均作为附加到用户条目的邮件属性存储在目录中。

创建和管理邮件用户和邮递列表包括创建和修改目录中的用户和邮递列表条目。可以使用 Sun LDAP Schema 2 的 Delegated Administrator 和 iPlanet Delegated Administrator for Messaging （对于 Sun LDAP Schema 1）、 Delegated Administrator 命令行实用程序或通过直接修改 Sun LDAP Schema 1 的 LDAP 目录来完成此操作。

从 Messaging Server 中删除用户

1. 通过运行 `commadmin user delete` 命令将用户标记为删除。（请参见位于 http://docs.sun.com/doc/819-1103 的 Sun Java System Communications Services Delegated Administrator 指南。）
2. 从用户中删除服务。

   服务可以为邮箱或日历。对于 Messaging Server，该程序为 `msuserpurge`。（请参见位于 http://docs.sun.com/doc/819-0106 的 Sun Java System Messaging Server Administration Reference。）对于日历服务，该程序为 `csclean`。（请参见位于 http://docs.sun.com/doc/819-1478 的 Sun Java System Calendar Server 管理指南。）
3. 通过调用 `commadmin domain purge` 命令永久删除用户。

从 Messaging Server 中删除域

1. 通过运行 `commadmin domain delete` 命令将域标记为删除。（请参见位于 http://docs.sun.com/doc/819-1103 的 Sun Java System Communications Services Delegated Administrator 指南。）
2. 从域的用户中删除服务。

   服务可以为邮箱或日历。对于 Messaging Server，该程序为 `msuserpurge`。（请参见位于 http://docs.sun.com/doc/819-0106 的 Sun Java System Messaging Server Administration Reference。）对于日历服务，该程序为 `csclean`。（请参见位于 http://docs.sun.com/doc/819-1478 的 Sun Java System Calendar Server 管理指南。）
3. 通过调用 `commadmin domain purge` 命令永久删除域。

通过 Sun ONE Console 管理 Messaging Server

在 Messaging Server 的安装过程和初始运行时配置程序完成之后，您可以通过管理控制台启动 Messaging Server。如果 Directory Server 和 Messaging Server 位于同一计算机上，则可以使用 Console 界面对两者进行管理。

要调用 Console，请运行 `/var/opt/mps/serverroot/startconsole` 命令。

您可以通过查看 Sun ONE Server Console 中的 “信息”表单来查看有关已安装的 Messaging Server 的某些基本信息。

要显示 “信息”表单，请执行以下步骤：

1. 在 Console 中，打开要查看其信息的 Messaging Server。
2. 在左窗格中选择服务器的图标。
3. 在左窗格中单击 “配置”选项卡。
4. 在右窗格中单击 “信息”选项卡 （如果它尚未显示在最前端）。

   将显示 “信息”表单。其中显示了服务器名称、服务器根目录、安装目录和实例目录。

启动和停止服务

根据服务是否安装在 HA 环境中，将以不同方式启动和停止服务。

在 HA 环境中启动和停止服务

当 Messaging Server 在 HA 控制下运行时，不能使用常规的 Messaging Server 启动、重新启动和停止命令来控制各个 Messaging Server 服务。如果尝试在 HA 部署中使用 `stop-msg`，系统将警告检测到 HA 设置并告诉您如何正确地停止系统。

下表显示了相应的启动、停止和重新启动命令。请注意，没有分别用于启动、重新启动或停止其他 Messaging Server 服务 （例如 SMTP）的特定 HA 命令。但是，您可以运行 `stop-msg` *service* 命令来停止 / 重新启动各个服务器，例如 `imap`、 `pop` 或 `sched`。

Sun Cluster 的最佳粒度是单个的资源。因为 Messaging Server 对于 Sun Cluster 来说是一个资源，所以 `scswitch` 命令将从整体上影响所有 Messaging Server 服务。

表 4-2 在 Sun Cluster 3.0/3.1 环境中启动、停止和重新启动

操作	单个资源	整个资源组
启动	`scswitch -e -j` *resource*	`sscswitch -Z -g` *resource_group*
重新启动	`scswitch -n -j` *resource* `scswitch -e -j` *resource*	`scswitch -R -g` *resource_group*
停止	`scswitch -n -j` *resource*	`scswitch -F -g` *resource_group*

表 4-3 在 Veritas 1.3、 2.0、 2.1 和 3.5 环境中启动、停止和重新启动

操作	单个资源	整个资源组
启动	hares -online *resource* -sys *system*	hagrp -online *group* -sys *system*
重新启动	hares -offline *resource* -sys *system* hares -online *resource* -sys *system*	hagrp -offline *group* -sys *system* hagrp -online *group* -sys *system*
停止	hares -offline *resource* -sys *system*	hagrp -offline *group* -sys *system*

在非 HA 环境中启动和停止服务

您可以从 Console 或命令行启动和停止服务。另外，您只需运行服务器实际使用的服务。例如，如果使用 Messaging Server 单独作为邮件传输代理 (MTA)，则可以只打开 MTA。或者，如果由于维护、检修或安全原因需要关闭服务器，则可以只关闭受影响的服务。（如果永远不想运行某个特定服务，则应当禁用该服务而不是只将其关闭。）

注 必须首先启用服务（例如 POP、IMAP 和 HTTP），然后才能启动或停止服务。有关更多信息，请参见第 114 页的 “启用和禁用服务”。

重要提示：如果某个服务器进程崩溃，则其他进程可能会由于等待该崩溃的进程所保留的锁定而挂起。如果没有使用自动重新启动（请参见第 101 页的 “失败的服务或未响应服务的自动重新启动”），则如果任何服务器进程崩溃，都应当停止所有进程，然后重新启动所有进程。这包括 POP、IMAP、HTTP 和 MTA 进程，以及 `stored`（邮件存储）进程和用于修改邮件存储的任何实用程序（例如 `mboxutil`、`deliver`、`reconstruct`、`readership` 或 `upgrade`）。

Console：Console 使您可以启动和停止各个服务以及查看有关每个服务的状态信息。

对于每个服务（IMAP、POP、SMTP 和 HTTP），该表单都显示了服务的当前状态（打开或关闭）。如果服务正运行，表单会显示上次启动该服务的时间。表单还可以显示其他状态信息。

要启动、关闭或查看任何邮件传送服务的状态，请执行以下步骤：

1. 从 Console 中，打开要启动或停止其服务的 Messaging Server。
2. 通过以下两种方法之一访问 “服务常规配置”表单：
   a. 单击 “任务”选项卡，然后单击 “启动服务 / 停止服务”。
   b. 单击 “配置”选项卡并在左窗格中选择 “服务”文件夹。然后在右窗格中单击 “常规”选项卡。
3. 将显示 “服务常规配置”表单。

   “进程控制”字段的左列中列出了服务器所支持的服务，右列给出了每个服务的基本状态（“打开”或 “关闭”；另外如果是 “打开”，还将给出上次启动服务的时间）。

4. 要查看有关当前打开的服务的状态信息，请在“进程控制”字段中选择该服务。

   “服务状态”字段将显示有关该服务的状态信息。

   对于 POP、 IMAP 和 HTTP，该字段将显示上次连接时间、连接总数、当前连接次数、自上次启动该服务以来失败的连接次数以及自上次启动该服务以来失败的登录次数。

   此字段中的信息可帮助您了解服务器上的负载及其服务的可靠性，并且可以帮助突出显示对服务器安全性的攻击。

5. 要打开某个服务，请在 “进程控制”字段中选择该服务并单击 “启动”。

6. 要关闭某个服务，请在 “进程控制”字段中选择该服务并单击 “停止”。

7. 要同时打开或关闭所有已启用的服务，请单击 “全部启动”或 “全部停止”按钮。

命令行：您可以使用 `start-msg` 和 `stop-msg` 命令来启动或停止任何邮件传送服务（`smtp`、 `imap`、 `pop`、 `store`、 `http`、 `ens`、 `sched`）。示例：

msg_svr_base`/sbin/start-msg imap`
msg_svr_base`/sbin/stop-msg pop`
msg_svr_base`/sbin/stop-msg sched`
msg_svr_base`/sbin/stop-msg smtp`

请注意，必须启用了服务，才能停止或启动服务。请参见第 100 页的 “指定要启动的服务”。

注 `start-msg smtp` 和 `stop-msg smtp` 命令将启动和停止所有 MTA 服务，而不仅仅是 SMTP 服务器。如果您希望在启动或停止 MTA 服务时能够进行更细微的控制，可以将 start/stop msg 命令用于分发程序和作业控制器。有关更多信息，请参见 Messaging Server Reference Manual。

指定要启动的服务

默认情况下将使用 start-msg 启动以下服务：

```
# ./start-msg
Connecting to watcher ...
Launching watcher ...
Starting ens server ....21132
Starting store server ....21133
checking store server status ... ready
Starting imap server ....21135
Starting pop server ....21138
Starting http server ....21141
Starting sched server ....21143
Starting dispatcher server ....21144
Starting job_controller server .... 21146
```

可以通过启用或禁用以下 configutil 参数来控制这些服务：service.imap.enable、service.pop.enable、 service.http.enable、 local.smsgateway.enable、local.snmp.enable、 local.imta.enable、 local.mmp.enable、 local.ens.enable 和 local.sched.enable。请注意，必须将 service.imap.enable 和 service.imap.enablesslport 都设置为 0 才能禁用 IMAP。禁用 POP 和 HTTP 的操作同理。有关这些参数如何工作的详细信息，请参见 Sun Java System Messaging Server Administration Reference。

失败的服务或未响应服务的自动重新启动

Messaging Server 提供了两个名为 watcher 和 msprobe 的进程，它们可以透明地监视服务并且可以在服务崩溃或未响应 （服务挂起）时自动重新启动服务。 watcher 监视服务器的崩溃。 msprobe 通过检查响应时间监视服务器挂起。当服务器失败或停止响应请求时，将自动重新启动该服务器。表 4-4.

表 4-4 由 watcher 和 msprobe 监视的服务

watcher （崩溃）	msprobe （未响应挂起）
IMAP、POP、HTTP、作业控制器、分发程序、邮件存储 (stored)、imsched、 MMP。（LMTP/SMTP 服务器由分发程序监视， LMTP/SMTP 客户机由 job_controller 监视。）	IMAP、POP、HTTP、cert、作业控制器、邮件存储 (stored)、imsched、 ENS、 LMTP、 SMTP

设置 local.watcher.enable=on （默认值）将监视进程故障和未响应的服务，并且会将错误消息记录到 default 日志文件中以表明特定的故障。要启用服务器自动重新启动，请将 configutil 参数 local.autorestart 设置为 yes。默认情况下，此参数被设置为 no。

如果任何邮件存储服务失败或冻结，则重新启动所有在启动时启用的邮件存储服务。例如，如果 imapd 失败，则至少重新启动 stored 和 imapd。如果其他邮件存储服务 （例如 POP 或 HTTP 服务器）正在运行，则这些服务也将被重新启动，而无论其失败与否。

如果某个邮件存储实用程序失败或冻结，自动重新启动仍然可以工作。例如，如果 mboxutil 失败或冻结，则系统将自动重新启动所有邮件存储服务器。但是请注意，系统不会重新启动该实用程序。 msprobe 将每 10 分钟运行一次。在 10 分钟内最多将执行两次服务和进程的重新启动 （可使用 local.autorestart.timeout 配置）。

无论 local.autorestart 是否设置为 yes，系统都将监视服务并向控制台和 *msg_svr_base*/data/log 发送失败或未响应的错误消息。默认情况下， watcher 将侦听端口 49994，但是可以使用 local.watcher.port 配置此设置。

Watcher 日志文件生成于 *msg_svr_base*/data/log/watcher 中。此日志文件不是由日志系统管理的 （不进行翻滚或清理），并且可以记录所有服务器启动和停止。下面显示了一个日志示例：

```
watcher process 13425 started at Tue Oct 21 15:29:44 2003

Watched 'imapd' process 13428 exited abnormally
Received request to restart:  store imap pop http
Connecting to watcher ...
Stopping http server 13440 .... done
Stopping pop server 13431 ... done
Stopping pop server 13434 ... done
Stopping pop server 13435 ... done
Stopping pop server 13433 ... done
imap server is not running
Stopping store server 13426 .... done
Starting store server .... 13457
checking store server status ...... ready
Starting imap server ..... 13459
Starting pop server ....... 13462
Starting http server ...... 13471
```

有关如何配置此功能的详细信息，请参见第 733 页的 “使用 msprobe 和 watcher 功能进行监视”。

由 imsched 控制 msprobe。如果 imsched 崩溃， watcher 将检测到此事件，并触发重新启动 （如果已启用 autorestart）。但是，在极少发生的 imsched 挂起中，您需要使用 kill *imsched_pid* 中止 imsched，以使 watcher 重新启动 imsched。

高可用性部署中的自动重新启动

高可用性部署中的自动重新启动需要设置以下 configutil 参数：

表 4-5 HA 自动重新启动参数

参数	说明 /HA 值
local.watcher.enable	启用 watcher。打开 （默认设置为 “打开”）
local.autorestart	启用 autorestart。 On

表 4-5 HA 自动重新启动参数

参数	说明 /HA 值
local.autorestart.timeout	失败重试超时。如果服务器在此指定时间内失败超过两次，则系统将停止尝试重新启动服务器。如果这种情况发生在 HA 系统上，则将关闭 Messaging Server 并向另一个系统进行故障转移。应当将该值（以秒为单位设置）设置为比 msprobe 间隔 (local.schedule.msprobe) 长的时间段值。
local.schedule.msprobe	msprobe 运行时间安排。crontab 式样的时间安排字符串（请参见表 18-10 第 527 页）。默认值为 600 秒。

安排自动任务时间

Messaging Server 使用名为 imsched 的进程提供了一般任务时间安排机制。它将用于调度 Messaging Server 进程。不支持调度非 Messaging Server 任务。它是通过设置 local.schedule.*taskname* configutil 参数来启用的。如果要修改时间安排，则必须使用命令 stop-msg sched 和 start-msg sched 重新启动调度程序，或者使用 refresh sched 刷新调度程序进程。

此参数需要一个命令和执行该命令的时间安排。格式如下：

configutil -o local.schedule.*taskname* -v "*schedule*"

taskname 是此命令 / 时间安排组合的唯一名称。

schedule 的格式如下所述：

minute hour day-of-month month-of-year day-of-week command args

command args 可以是任何 Messaging Server 命令及其参数。需要全限定命令路径名。

minute hour day-of-month month-of-year day-of-week 是用于运行该命令的时间安排。它采用 UNIX crontab 格式。

这些值以空格或 Tab 分隔符分隔，可以分别为 0-59、0-23、1-31、1-12 或 0-6（其中 0 = 星期天）。每个时间字段都可以为以下内容之一：一个星号（表示所有合法值）、一个以逗号分隔的值的列表或一个以连字符分隔的两个值表示的范围。请注意，可以同时使用几号和星期几来指定时间，如果这样指定，将需要同时满足两者。例如，如果设置月份的第 17 日和星期二，则仅在某月的第 17 日是星期二时才运行该命令。有关如何设置时间安排参数的示例，请参见表 18-10 第 527 页。

请注意，如果要修改调度程序，则必须使用命令 `stop-msg sched` 和 `start-msg sched` 重新启动调度程序，或者向调度程序进程发送 SIGHUP：

`kill -HUP` *scheduler_pid*

调度程序示例

在 12:30am、 8:30am 和 4:30pm 以详细模式运行 `imexpire`：

```
configutil -o local.schedule.rm_messages -v "30 0,8,16 * * *"
/opt/SUNWmsgsr/sbin/imexpire -v
```

每 20 分钟显示一次 MTA 通道队列邮件计数器：

```
configutil -o local.schedule.counters -v "20,40,60 * * * *"
/opt/SUNWmsgsr/sbin/imsimta qm counters -show > temp.txt
```

在星期一到星期五的午夜 (12AM) 运行 `imsbackup`：

```
configutil -o local.schedule.msbackup -v "0 0 * * 1-5"
/opt/SUNWmsgsr/sbin/imsbackup -f backupfile /primary
```

配置问候邮件

Messaging Server 允许您创建发送给每个新用户的问候电子邮件。

Console 要使用 Console 创建新用户问候，请执行以下操作：

1. 在 Console 中，打开要配置其新用户问候的 Messaging Server。
2. 单击 “配置” 选项卡。如果左窗格中尚未突出显示该服务器的图标，请选择该图标。
3. 在右窗格中单击 “其他” 选项卡。
4. 创建新用户问候或根据需要进行更改。

   必须将问候编排成电子邮件格式，包括标题 （至少包含一个主题行），然后空一行，最后是邮件主体。

   创建邮件时，请使用邮件字段上方的下拉列表指定其语言。如果需要，可以使用多种语言创建多封邮件。
5. 单击 “保存”。

命令行：要使用命令行创建新用户问候，请运行以下命令：

`configutil -o gen.newuserforms -v` *Message*

其中 *Message* 必须包含一个标题 （至少具有一个主题行），接着是 $$，然后是邮件主体。 $ 表示一个新的行。

例如，要启用此参数，您可以设置以下配置变量：

```
configutil -o gen.newuserforms -v 'Subject: Welcome!!$$ Sesta.com welcomes you
to the premier internet experience in Dafandzadgad!
```

可能需要在 $ 前面添加一个特殊字符，使其不再具有特殊含义 （取决于所使用的 shell）。（$ 通常是 shell 的换码符。）

设置基于域的问候邮件

只要创建新的托管域，就最好创建所支持语言的基于域的问候邮件。否则，将发送通过 gen.newuserforms 设置的通用问候邮件。

您可以为每个域中的新用户设置问候邮件。邮件可以根据用户的首选语言、域的首选语言或站点的首选语言而有所不同。通过设置所需的 LDAP 域条目中的 mailDomainWelcomeMessage 属性来完成此操作。属性语法如下：

```
mailDomainWelcomeMessage;lang-user_prefLang
mailDomainWelcomeMessage;lang-domain_prefLang
mailDomainWelcomeMessage;lang-gen.sitelanguage
```

以下示例设置了英语的域欢迎邮件：

```
mailDomainWelcomeMessage;lang-en: Subject: Welcome!!$$Welcome to the mail
system.
```

以下示例设置了法语的域欢迎邮件：

```
mailDomainWelcomeMessage;lang-fr: Subject: Bienvenue!!$$Bienvenue a siroe.com!
```

在以上示例中，我们假定：

- 域为 siroe.com
- 新用户属于该域
- 用户的首选语言是法语，这由 LDAP 属性 preferredlanguage 指定。
- siroe.com 可以使用上述英语和法语欢迎邮件
- 站点语言是英语，这由 gen.sitelanguage 指定。

有关所支持的语言环境及其语言值标记的列表，请参见 Directory Server Reference Manual (http://docs.sun.com/source/816-6699-10/ax_inter.html#18744)。

用户首次登录时，他们将收到法语问候。如果法语欢迎邮件不可用，他们将收到英语问候。

问候邮件操作原理

问候邮件可以通过 LDAP 属性 mailDomainWelcomeMessage 和 configutil 参数 gen.newuserforms 设置。选择邮件的顺序 （最上面的具有最高优先级）如下所示：

mailDomainWelcomeMessage;lang-*user_prefLang*
mailDomainWelcomeMessage;lang-*domain_prefLang*
mailDomainWelcomeMessage;lang-*gen.sitelanguage*
mailDomainWelcomeMessage
gen.newuserforms;lang-"$user-*prefLang*"
gen.newuserforms;lang-"$domain-*prefLang*"
gen.newuserforms;lang-"$gen.*sitelanguage*"
gen.newuserforms

算法如下：如果没有域 （或者有，但是没有为每个域置备的欢迎邮件），则会使用 gen.newuserforms 参数配置一封欢迎邮件 （如果已指定）。如果用户具有首选语言（使用 preferredlanguage LDAP 属性设置）并且设置了 gen.newuserforms;lang-*user_prefLang*，则当用户首次登录服务器时将收到该欢迎邮件。如果设置了 gen.newuserforms;lang-*gen.sitelanguage*，没有设置 preferredlanguage，但是设置了站点语言 （使用 gen.sitelanguage 参数），则用户将收到该语言的欢迎邮件。如果未设置任何语言标记参数，但设置了无标记的 gen.newuserforms，系统会将该邮件发送给用户。如果以上各个值均未设置，用户将不会收到任何欢迎邮件。

如果用户位于某个域中，则与上面讨论的情况类似，该用户可能会收到其中一封 mailDomainWelcomeMessage;lang-xx，这取决于列表中的哪一项可用及给定的顺序。

示例：域为 fantasia.com。域的首选语言为德语 (de)。但是，此域中的新用户的首选语言为土耳其语 (tr)。站点语言为英语。可用值如下 （mailDomainWelcomeMessage 是域 fantasia.com 的属性）：

mailDomainWelcomeMessage;lang-fr
mailDomainWelcomeMessage;lang-ja
gen.newuserforms;lang-de
gen.newuserforms;lang-en
gen.newuserforms

根据算法，发送给用户的邮件将是 gen.newuserforms;lang-de。

设置用户首选语言

管理员可以通过设置用户的 LDAP 条目中的属性 preferredLanguage 为 GUI 和服务器生成的邮件设置首选语言。

当服务器向服务器的管理域以外的用户发送邮件时，它并不知道用户的首选语言是什么，除非它响应一封在邮件标题中指定了首选语言的外来邮件。标题字段（accept-language、 Preferred-Language 或 X-Accept-Language）是根据在用户的邮件客户机中指定的属性设置的。

如果有多个首选语言设置 （例如，如果用户具有在 Directory Server 中存储的首选语言属性，还具有在其邮件客户机中指定的首选语言），则服务器将按照以下顺序选择首选语言：

1. 原始邮件中的 accept-language 标题字段。
2. 原始邮件中的 Preferred-Language 标题字段。
3. 原始邮件中的 X-Accept-Language 标题字段。
4. 发件人的首选语言属性 （如果已在 LDAP 目录中找到）。

设置域首选语言

域首选语言是为特定域指定的默认语言。例如，您可能希望为名为 mexico.siroe.com 的域指定西班牙语。管理员可以通过设置域的 LDAP 条目中的属性 preferredLanguage 来设置域首选语言。

配置服务器站点语言

您可以按照如下所示为服务器指定默认站点语言。如果未设置用户首选语言，则会使用站点语言来发送特定语言版本的邮件。

Console：要从 Console 指定站点语言，请执行以下操作：

1. 打开要配置的 Messaging Server。
2. 单击 “配置” 选项卡。
3. 在右窗格中单击 “其他” 选项卡。
4. 从站点语言下拉列表中，选择要使用的语言。
5. 单击 “保存”。

命令行：您也可以用如下所示的命令行指定站点语言：

```
configutil -o gen.sitelanguage -v value
```

其中， *value* 是本地支持的语言之一。有关所支持的语言环境和语言值标记的列表，请参见 Directory Server Reference Manual (http://docs.sun.com/source/816-6699-10/ax_inter.html#18744)。

自定义目录查找

如果没有基于 LDAP 的目录系统 （例如 Sun Java System Directory Server），Messaging Server 将无法工作。 Messaging Server 和 Console 需要访问目录以用于多种用途。例如：

- 首次安装 Messaging Server 时，需要为该服务器输入配置设置。这些设置存储在中心**配置目录**中。安装进程的一部分包括配置与该目录的连接。
- 创建或更新邮件用户或邮件组的帐户信息时，这些信息将存储在称为**用户目录**的目录中。安装时会配置服务器组的 Administration Server，这样当您访问用户和组时，默认情况下 Console 将连接到定义您的**管理拓扑** （共享同一个配置目录和用户目录的 Sun Java System 服务器集）的配置目录。
- 当路由邮件以及向邮箱中传送邮件时， Messaging Server 将在用户目录中查找有关发件人或收件人的信息。默认情况下， Messaging Server 将在与 Administration Server 所配置使用的同一用户目录中查找。
- 验证用户以进行邮件路由查找。

您可以通过以下方法修改其中的每个目录配置设置：

- 您可以使用 Console 的 “Administration Server”界面更改配置目录的连接设置。（有关详细信息，请参见 《 Sun ONE Server Console 5.2 Server Management Guide 》中的 "Administration Server" 一章。）
- 当更改用户和组的信息时，可以使用 Console 的 “用户和组”界面临时连接到一个与默认用户目录不同的用户目录。（有关详细信息，请参见 《 Sun ONE Server Console 5.2 Server Management Guide 》中的 "Users and Groups" 一章。）
- 您可以使用 Console 的 “Messaging Server”界面将 Messaging Server 配置为连接到与 Administration Server 定义的默认用户目录不同的用户目录。这就是本节中讨论的配置任务。

将 Messaging Server 重新配置为连接到其他用户目录以进行用户和组的查找确实是可选的。大多数情况下，定义服务器的管理域的用户目录是该域中所有服务器使用的用户目录。

注 如果为 Messaging Server 的查找指定了自定义的用户目录，则也必须在访问 Console 的 “用户和组”界面时指定同一个目录以便更改该目录的用户和组信息。

Console：要使用 Console 修改 Messaging Server 的 LDAP 用户查找设置，请执行以下操作：

1. 从 Console 中打开要自定义其 LDAP 连接的 Messaging Server。
2. 单击 “配置”选项卡。
3. 在左窗格中选择 “服务”文件夹。
4. 在右窗格中选择 “LDAP”选项卡。将显示 “LDAP”表单。

   “LDAP”表单显示了配置目录和用户目录的配置设置。但是，配置目录设置在此表单中是只读的。如果需要更改设置，请参见 《 Sun ONE Server Console 5.2 Server Management Guide 》中的 "Administration Server" 一章。
5. 要更改用户目录连接设置，请单击标有 “使用邮件传送服务器的特定目录设置”的框。
6. 通过输入或修改以下任意信息来更新 LDAP 配置 （有关目录概念的解释，包括诸如**独特的名称**等术语的定义，请参见 Directory Server Administration Guide）：

   主机名：包含安装的用户信息的目录所在主机的名称。通常与 Messaging Server 主机不是同一个主机，虽然在极少数安装情况下可能是相同的。

   端口号：目录主机上的端口号， Messaging Server 必须使用它来访问目录以进行用户查找。此号码由目录管理员定义，并且不一定是默认端口号 (389)。

   基本 DN：搜索基准 — 即表示用户查找起点的目录条目的独特名称。要加快查找进程，搜索基准应当在目录树中尽可能靠近要查找的信息。如果您的安装的目录树具有 “人员”或 “用户”分支，则这是合理的起点。

   绑定 DN：Messaging Server 连接到目录服务器以进行查找时用于表示自身的独特名称。绑定 DN 必须是用户目录自身中某个条目 （被赋予了对目录的用户部分进行搜索的权限）的独特名称。如果目录允许匿名搜索访问，则可以将此条目保留为空白。

7. 要更改使用的密码（与绑定 DN 相结合，用于向 LDAP 目录验证此 Messaging Server 以进行用户查找），请单击“更改绑定密码”按钮。“密码条目”窗口将打开，可以在其中输入更新的密码。

   您自己的安全性策略应当确定在这种情况下使用的密码。该密码最初被设置为无密码。如果通过将“绑定 DN”字段保留为空白指定了匿名访问，则不使用密码。

   此步骤将更新存储在服务器配置中的密码，但是并不更改 LDAP 服务器中的密码。默认情况下，此帐户也用于 PAB 查找。更改密码后需要执行以下两个步骤。

8. 为配置属性 `local.ugldapbinddn` 中指定的用户修改密码。此用户帐户存在于配置属性 `local.ugldaphost` 中指定的目录服务器中。

9. 如果将同一个帐户用于在属性 `local.service.pab.ldapbinddn` 和 `local.service.pab.ldaphost` 中指定的 PAB 访问，则必须更新存储在 `local.service.pab.ldappasswd` 中的密码。

要返回到使用默认用户目录，请取消选取“使用邮件传送服务器的特定目录设置”框。

命令行：您也可以通过以下命令行设置用户目录连接设置的值。还请确保按照以上步骤 8 和步骤 9 中所述设置 LDAP 和 PAB 密码。

要指定是否使用 Messaging Server 的特定目录设置，请运行以下命令：

```
configutil -o local.ugldapuselocal -v [ yes | no ]
```

要指定用于用户查找的 LDAP 主机名，请运行以下命令：

```
configutil -o local.ugldaphost -v name[:port_number]
```

要指定用于用户查找的端口号，请运行以下命令：

```
configutil -o local.ugldapport -v number
```

要指定用于用户查找的 LDAP 基本 DN，请运行以下命令：

```
configutil -o local.ugldapbasedn -v basedn
```

要指定用于用户查找的 LDAP 绑定 DN，请运行以下命令：

```
configutil -o local.ugldapbinddn -v binddn
```

加密设置

您可以使用 Console 为 Messaging Server 启用安全套接字层 (SSL) 加密和验证，并选择服务器将在其所有服务中支持的特定加密算法。

虽然此任务是一般配置任务，但第 19 章 “配置安全和访问控制”中的 “启用 SSL” 一节仍对其进行了说明，其中还包含有关 Messaging Server 的所有安全性和访问控制主题的背景信息。

设置故障转移 LDAP 服务器

可以为用户 / 组目录指定多个 LDAP 服务器，以便在一个服务器出现故障时可以由另一个服务器接管：

1. 将 `local.ugldaphost` 设置到多台 LDAP 计算机。示例：

   ```
   configutil -o local.ugldaphost -v "server1 server2 ..."
   ```

2. 将 `local.ugldapuselocal` 设置为 `yes`。这将指定用户 / 组 LDAP 配置数据将存储在本地配置文件中。否则，该数据将存储在 LDAP 中。示例：

   ```
   configutil -o local.ugldapuselocal -v yes
   ```

如果列表中的第一个服务器出现故障，则现有 LDAP 连接将被识别为关闭，同时进行新的连接。当需要新的 LDAP 连接时， LDAP 库将按照所列出的顺序尝试所有 LDAP 服务器。

与用户 / 组目录的故障转移一样，可以类似地为配置目录设置故障转移服务器。该配置属性为 `local.ldaphost`。

第 5 章

配置 POP、 IMAP 和 HTTP 服务

Messaging Server 支持客户机访问邮箱时使用邮局协议 3 (POP3)、 Internet 邮件访问协议 4 (IMAP4) 和超文本传输协议 (HTTP)。 IMAP 和 POP 都是 Internet 标准邮箱协议。 Messenger Express 是启用了 Web 的电子邮件程序，它使最终用户可以使用浏览器访问其邮箱，浏览器运行于使用 HTTP 的与 Internet 连接的计算机系统中。

本章介绍如何使用 Sun ONE Console 或命令行实用程序配置服务器，以使其支持一项或多项上述服务。

有关配置简单邮件传输协议 (SMTP) 服务的信息，请参见第 10 章 “关于 MTA 服务和配置”。

本章包含以下各节：

- 第 114 页的 “一般配置”
- 第 116 页的 “登录要求”
- 第 118 页的 “性能参数”
- 第 120 页的 “客户机访问控制”
- 第 121 页的 “配置 POP 服务”
- 第 123 页的 “配置 IMAP 服务”
- 第 125 页的 “配置 HTTP 服务”

一般配置

配置 Messaging Server POP、 IMAP 和 HTTP 服务的一般功能包括启用或禁用服务、指定端口号和修改发送给连接客户机的服务标题 （可选）。本节提供了背景信息；有关完成这些设置所需的步骤，请参见第 121 页的 “配置 POP 服务”、第 123 页的 “配置 IMAP 服务”和第 125 页的 “配置 HTTP 服务”。

启用和禁用服务

您可以控制任何特定的 Messaging Server 实例是否提供 POP、 IMAP 或 HTTP 服务。这与启动和停止服务不同 （请参见第 97 页的 “启动和停止服务”）；要使 POP、 IMAP 或 HTTP 发挥作用，必须对其启用并启动。

与启动或停止服务相比，启用服务是更为 “全局”的过程。例如，启用的设置在系统重新引导后仍然可用，但是在重新引导后，您必须重新启动以前 “停止”的服务。

无需启用不准备使用的服务。例如，如果只将 Messaging Server 实例用作邮件传输代理 (MTA)，则应该禁用 POP、 IMAP 和 HTTP。如果只将其用于 POP 服务，则应该禁用 IMAP 和 HTTP。如果只将其用于基于 Web 的电子邮件，则应该禁用 POP 和 IMAP。

您可以在服务器级别启用或禁用服务。本章介绍了这一过程。第 100 页的 “指定要启动的服务”也对此过程作了介绍。您还可以通过设置指定的 LDAP 属性 `mailAllowedServiceAccess` 在用户级别启用或禁用服务。

指定端口号

对于每项服务，您都可以指定服务器用于服务连接的端口号：

- 如果启用 POP 服务，可以指定服务器用于 POP 连接的端口号。默认端口号为 110。
- 如果启用 IMAP 服务，可以指定服务器用于 IMAP 连接的端口号。默认端口号为 143。
- 如果启用 HTTP 服务，可以指定服务器用于 HTTP 连接的端口号。默认端口号为 80。

有时可能需要指定不同于默认值的端口号，例如，如果一台主机计算机中有两个或多个 IMAP 服务器实例，或者同一主机计算机既用作 IMAP 服务器又用作 Messaging Multiplexor 服务器。（有关 Multiplexor 的信息，请参见第 7 章 “配置和管理多路复用器服务”。）

指定端口时请注意以下两点：

- 端口号可以是 1 到 65535 之间的任何数字。
- 确保所选择的端口未被使用或为其他服务所保留。

用于加密通信的端口

Messaging Server 支持使用安全套接字层 (SSL) 协议与 IMAP、 POP 和 HTTP 客户机进行加密通信。有关在 Messaging Server 中支持 SSL 的一般信息，请参见第 578 页的 “配置加密和基于证书的验证”。

基于 SSL 的 IMAP

您可以接受默认 （建议）的基于 SSL 的 IMAP 端口号 (993)，也可为基于 SSL 的 IMAP 指定其他端口。

由于大多数当前 IMAP 客户机要求使用单独的端口，因此 Messaging Server 提供了使用单独的 IMAP 端口和基于 SSL 的 IMAP 端口这一选项。与 IMAP 和基于 SSL 的 IMAP 通信时使用同一端口是新兴标准；只要 Messaging Server 已安装 SSL 证书（请参见第 580 页的 “通过管理控制台获得证书”），它便可以支持同一端口的基于 SSL 的 IMAP。

基于 SSL 的 Pop

默认独立的基于 SSL 的 POP 端口为 995。您可以使用命令 "STLS" 启动普通的基于 SSL 的 POP 端口 （请参见第 121 页的 “配置 POP 服务”）。

基于 SSL 的 HTTP

您可以接受默认的基于 SSL 的 HTTP 端口号 (443)，也可以为 HTTPS 指定其他端口。

服务标题

客户机首次连接到 Messaging Server POP 或 IMAP 端口时，服务器将向该客户机发送标识文本字符串。此服务标题 （通常不向客户机用户显示）将服务器标识为 Sun Java System Messaging Server，并给出服务器的版本号。此标题主要用于客户机调试或问题隔离。

如果要向连接的客户机发送其他消息，则可以替换 POP 或 IMAP 服务的默认标题。

您可以使用 Sun ONE Console 或 configutil 实用程序 （service.imap.banner、service.pop.banner）来设置服务标题。有关 configutil 的详细语法信息，请参见 Sun Java System Messaging Server Administration Reference (http://docs.sun.com/doc/819-0106)。

登录要求

您可以控制允许用户登录到 POP、 IMAP 或 HTTP 服务以检索邮件的方式。可以允许基于密码的登录（适用于所有服务）和基于证书的登录（适用于 IMAP 或 HTTP 服务）。本节提供的是背景信息；有关完成这些设置所需的步骤，请参见第 121 页的 “配置 POP 服务”、第 123 页的 “配置 IMAP 服务”或第 125 页的 “配置 HTTP 服务”。此外，您可以指定用于 POP 登录的有效登录分隔符。

设置 POP 客户机的登录分隔符

某些邮件客户机不接受 @ 作为登录分隔符 （也就是说，类似 uid@domain 的地址中的 @）。这些客户机包括 Netscape Messenger 4.76、 Netscape Messenger 6.0 和 Windows 2000 中的 Microsoft Outlook Express。解决方法如下：

1. 使用以下命令使 + 成为有效的分隔符：

   ```
   configutil -o service.loginseparator -v "@+"
   ```

2. 通知 POP 客户机用户，登录时应将 + （而不是 @）作为登录分隔符。

允许不使用域名登录

典型登录需要用户输入用户 ID，后跟分隔符和域名，然后是密码。但是，在安装过程中指定的默认域中的用户可以直接登录，而不必输入域名或分隔符。

要允许其他域的用户只输入用户 ID 即可登录 （即无需使用域名和分隔符），请将

sasl.default.ldap.searchfordomain 设置为 0。请注意，用户 ID 对整个目录树而言必须是唯一的。如果不唯一，则不使用域名登录将无法工作。

您可能希望修改用户登录时必须输入的属性，例如，您要允许用户使用电话号码 (telephoneNumber) 或员工编号 (employeeID) 登录，请更改由 configutil 参数 sasl.default.ldap.searchfilter 定义的 LDAP 搜索。此参数是基于域的属性

inetdomainsearchfilter 的全局默认设置，并且使用与该属性相同的语法。

有关这些参数的详细信息，请参阅 Sun Java System Messaging Server Administration Reference (http://docs.sun.com/doc/819-0106)。

基于密码的登录

在典型的邮件传送安装中，用户通过在其 POP、 IMAP 或 HTTP 邮箱客户机中输入密码来访问邮箱。客户机将密码发送给服务器，服务器使用该密码来验证用户。对用户进行验证后，服务器将根据访问控制规则来决定是否授权用户访问存储在该服务器中的特定邮箱。

如果允许密码登录，用户可以通过输入密码访问 POP、 IMAP 或 HTTP。（基于密码或基于 SSL 的登录是用于 POP 服务的唯一验证方法。）密码存储在 LDAP 目录中。目录策略将决定有效的密码策略 （例如最小长度）。

如果不允许对 IMAP 或 HTTP 服务进行密码登录，则不允许基于密码的验证。这时要求用户使用基于证书的登录 （如下节所述）。

为了增加 IMAP 和 HTTP 服务的密码传输的安全性，您可以要求在将密码发送给服务器之前先对其加密。您可以通过选择用于登录的最小加密算法长度要求进行此操作。

- 如果选择 0，则不要求加密。密码以不加密形式发送，或根据客户机策略对其加密。
- 如果选择非零值，客户机将与服务器建立 SSL 会话 （使用其密钥长度不小于指定值的加密算法），从而加密客户机发送的所有 IMAP 或 HTTP 用户密码。

如果将客户机配置为要求加密的密钥长度大于服务器支持的最大长度，或者将服务器配置为要求加密的密钥长度大于客户机支持的长度，则无法进行基于密码的登录。有关设置服务器以支持各种加密算法和密钥长度的信息，请参见第 584 页的“启用 SSL 并选择加密算法的步骤”。

基于证书的登录

除了基于密码的验证之外，Sun Java System 服务器还支持通过检查用户的数字证书对其进行验证。客户机与服务器建立 SSL 会话时将提供用户的证书而不是密码。如果证书有效，则认为用户经过验证。

有关设置 Messaging Server 以接受基于证书的用户登录到 IMAP 或 HTTP 服务的说明，请参见第 586 页的 “设置基于证书的登录的步骤”。

要启用基于证书的登录，无需取消选取 “IMAP 系统”或 “HTTP 系统”表单中的 “允许密码登录”框。如果选择了此框 （默认状态），并且已执行设置基于证书的登录所需的任务，将同时支持基于密码和基于证书的登录。这时，如果客户机建立 SSL 会话并提供证书，将使用基于证书的登录。如果客户机不使用 SSL 或不提供客户机证书，它将发送密码。

性能参数

您可以为 Messaging Server 的 POP、 IMAP 和 HTTP 服务设置一些基本性能参数。您可以根据硬件能力和用户基础调整这些参数，以达到最大服务效率。本节提供的是背景信息；有关完成这些设置所需的步骤，请参见第 121 页的 “配置 POP 服务”、第 123 页的 “配置 IMAP 服务”或第 125 页的 “配置 HTTP 服务”。

进程数量

Messaging Server 可以将工作分为若干个执行进程，在某些情况下这可以提高效率。此功能对于多个处理器的服务器计算机尤其有用，这时调整服务器进程的数量可以将多个任务更有效率地分发给各个硬件处理器。

但是，将任务分配给多个进程以及从一个进程切换到另一个进程时，也会有性能开销。每添加一个新进程，具有多个进程的优势都将减少。对于大多数配置，简单的经验规则是使服务器计算机的每个硬件处理器中有一个进程，最多不超过 4 个进程。最佳配置可能会因情况而异；此经验法则只作为您自己进行分析时的出发点。

注意：在某些平台中，可能需要增加进程数量，以解决该平台特有的对每个进程的特定限制 （例如文件描述符的最大数量），这可能会影响性能。

对于 POP、 IMAP 或 HTTP 服务，默认的进程数量为每项服务 1 个。

每个进程的连接数量

POP、 IMAP 或 HTTP 服务可以维持的同时进行的客户机连接越多，对客户机就越有利。如果客户机由于无可用连接而被拒绝服务，则必需等到其他客户机断开连接。

另一方面，每个打开的连接都要消耗内存资源，并需要使用服务器计算机的 I/O 子系统，因此对于服务器所能支持的同时进行的会话数量是有实际限制的。（您可以通过增加服务器内存或 I/O 容量来放宽此限制。）

IMAP、 HTTP 和 POP 在这方面有不同的需求：

- 与 POP 和 HTTP 连接相比， IMAP 连接的时间通常比较长。用户连接到 IMAP 下载邮件时，连接通常会持续到用户退出或连接超时为止。相反，对 POP 或 HTTP 请求进行服务后， POP 或 HTTP 连接通常就关闭了。
- IMAP 和 HTTP 连接通常比 POP 连接效率更高。每次 POP 重新连接都要求对用户重新验证。相反， IMAP 连接仅要求一次验证，因为在 IMAP 会话期间（从登录到注销）连接将保持打开状态。 HTTP 连接较短暂，但是用户无需在每次连接时重新验证，因为每次 HTTP 会话 （从登录到注销）允许多个连接。因此， POP 连接比 IMAP 或 HTTP 连接需要更多的性能开销。Messaging Server 尤其如此，通过打开但闲置 IMAP 连接以及通过多个 HTTP 连接， Messaging Server 被设计为要求非常低的开销。

注 有关 HTTP 会话安全性的详细信息，请参见第 573 页的 “关于 HTTP 安全性”。

因此，在特定时间，对于特定的用户需求， Messaging Server 可以支持的打开的 IMAP 或 HTTP 连接比 POP 连接多很多。

对于 IMAP，默认值是每个进程 4000 个连接；对于 HTTP，默认值是每个进程 6000 个连接；对于 POP，默认值是 600。这些默认值大致代表典型配置的服务器计算机所能处理的等量需求。最佳配置可能会因情况而异；这些默认值仅作为一般准则。

通常情况下，与活动的 IMAP 连接比较，活动的 POP 连接对服务器资源和带宽的需求更大，这是因为 IMAP 连接多数时间都处于空闲状态，而 POP 连接在不断地下载邮件。拥有较少数量的 POP 会话是正确的。相反， POP 连接的持续时间仅仅是其下载电子邮件所用的时间，因此活动的 POP 用户仅连接了很短的时间，而 IMAP 连接在连续邮件检查期间将保持连接状态。

每个进程的线程数量

除了支持多个进程， Messaging Server 还通过将工作细分给多个线程来进一步提高性能。服务器对线程的使用极大提高了执行效率，因为执行中的命令不会妨碍其他命令的执行。可以根据执行过程中的需要创建和删除线程，多达所设置的最大数量。

具有更多的同时执行的线程意味着可以在没有延迟的情况下处理更多的客户机请求，以便为更多的客户机提供快速服务。但是，在线程间分发任务也有性能开销，因此对于服务器可以使用的线程数量有实际限制。

对于 POP、 IMAP 和 HTTP，默认的最大值为每个进程 250 个线程。尽管 IMAP 和 HTTP 的默认连接数量大于 POP 的默认连接数量，但默认线程数量相等。我们假定，使用与较少但更忙碌的 POP 连接相同的最大线程数量能够高效处理较多的 IMAP 和 HTTP 连接。最佳配置可能因情况而异，但是这些默认值已经足够大，您不大可能需要增加这些值；默认值应该可以为大多数安装提供合理的性能。

切断空闲连接

为了收回无响应客户机的连接所使用的系统资源， IMAP4、 POP3 和 HTTP 协议允许服务器单方面切断已空闲特定时间的连接。

各个协议规范要求服务器在某个最小时间内将空闲连接保持打开状态。对于 POP，默认时间是 10 分钟，对于 IMAP，默认时间是 30 分钟，对于 HTTP，默认时间是 3 分钟。您可以在默认值基础上增加空闲时间，但不能缩短默认时间。

如果切断 POP 或 IMAP 连接，用户必须重新验证才能建立新连接。相反，如果切断 HTTP 连接，用户无需重新验证，因为 HTTP 会话将保持打开状态。有关 HTTP 会话安全性的详细信息，请参见第 573 页的 “关于 HTTP 安全性”。

空闲的 POP 连接通常是由于出现某个问题 （例如崩溃或挂起）致使客户机无法响应而造成的。空闲的 IMAP 连接则属于正常情况。为了避免 IMAP 用户被单方面断开连接，IMAP 客户机通常在小于 30 分钟的某个时间间隔内向 IMAP 服务器定期发送命令。

注销 HTTP 客户机

HTTP 会话可以持续多个连接。切断连接后并不注销 HTTP 客户机。但是，如果 HTTP 会话保持空闲的时间达到指定的时间段，服务器将自动断开 HTTP 会话并注销客户机 （默认时间段是 2 小时）。切断会话后，客户机的会话 ID 将无效，客户机必须重新验证才能建立其他会话。有关 HTTP 安全性和会话 ID 的详细信息，请参见第 573 页的 “关于 HTTP 安全性”。

客户机访问控制

Messaging Server 包含访问控制功能，使您可以决定哪些客户机可以访问 POP、IMAP 或 HTTP 邮件传送服务 （以及 SMTP）。您可以基于多种标准创建灵活的访问过滤器，以允许或拒绝对客户机的访问。

客户机访问控制是 Messaging Server 重要的安全保护功能。有关创建客户机访问控制过滤器及其使用示例的信息，请参见第 591 页的 “配置客户机对 POP、IMAP 和 HTTP 服务的访问”和第 604 页的 “配置客户机对 SMTP 服务的访问”。

配置 POP 服务

您可以通过使用 `configutil` 命令或 Sun ONE Console 对 Messaging Server POP 服务执行基本配置。本章介绍了一些比较常用的 POP 服务选项。在 Sun Java System Messaging Server Administration Reference 中可以查看完整列表。

有关详细信息，另请参见：

- 第 114 页的 “启用和禁用服务”
- 第 116 页的 “设置 POP 客户机的登录分隔符”
- 第 114 页的 “指定端口号”
- 第 118 页的 “每个进程的连接数量”
- 第 120 页的 “切断空闲连接”
- 第 119 页的 “每个进程的线程数量”
- 第 118 页的 “进程数量”

Console 使用 Console 配置 POP 服务：

1. 从 Sun ONE Console 中打开要配置的 Messaging Server。
2. 单击 “配置”选项卡并打开左窗格中的 “服务”文件夹。
3. 选择 “POP”。
4. 单击右窗格中的 “系统”选项卡。
5. 要启用服务，请选取标有 “启用端口处的 POP 服务”的框，然后指定端口号。
6. 指定以下连接设置：
   - 设置每个进程的最大网络连接数量。有关更多信息，请参见第 118 页的 “每个进程的连接数量”。
   - 设置连接的最大空闲时间。有关更多信息，请参见第 120 页的 “切断空闲连接”。

7. 指定以下进程设置：
   - 设置每个进程的最大线程数量。有关更多信息，请参见第 119 页的 “每个进程的线程数量”。
   - 设置最大进程数量。有关更多信息，请参见第 118 页的 “进程数量”。
8. 如果需要，在 POP 服务标题字段中指定服务标题。
9. 单击 “保存”。

注 对于 POP 服务，将自动启用基于密码的登录。

命令行 您可以按照以下方法在命令行中设置 POP 属性的值：

启用或禁用 POP 服务：

```
configutil -o service.pop.enable -v [ yes | no ]
```

指定端口号：

```
configutil -o service.pop.port -v number
```

设置每个进程的最大网络连接数量：

```
configutil -o service.pop.maxsessions -v number
```

设置连接的最大空闲时间：

```
configutil -o service.pop.idletimeout -v number
```

设置每个进程的最大线程数量：

```
configutil -o service.pop.maxthreads -v number
```

设置最大进程数量：

```
configutil -o service.pop.numprocesses -v number
```

启用基于 SSL 的 POP：

```
configutil -o service.pop.enablesslport -v 1
configutil -o service.pop.sslport -v 995
```

请注意，如果正确配置了 SSL，则还支持 TLS。

指定协议欢迎标题：

```
configutil -o service.pop.banner -v banner
```

配置 IMAP 服务

您可以通过使用 `configutil` 命令或 Sun ONE Console 对 Messaging Server IMAP 服务进行基本配置。本节介绍了一些比较常用的 IMAP 服务选项。在 Sun Java System Messaging Server Administration Reference 中可以查看完整列表。有关详细信息，另请参见：

- 第 114 页的 “启用和禁用服务”
- 第 114 页的 “指定端口号”
- 第 117 页的 “基于密码的登录”
- 第 118 页的 “每个进程的连接数量”
- 第 120 页的 “切断空闲连接”
- 第 119 页的 “每个进程的线程数量”
- 第 118 页的 “进程数量”

Console 使用 Console 配置 IMAP 服务：

1. 从 Sun ONE Console 中打开要配置的 Messaging Server。
2. 单击 “配置”选项卡并打开左窗格中的 “服务”文件夹。
3. 选择 “IMAP”。
4. 单击右窗格中的 “系统”选项卡。
5. 要启用服务，请选取标有 “启用端口处的 IMAP 服务”的框，然后指定端口号。
6. 如果需要，启用基于密码的登录。
7. 指定以下连接设置：
   - 设置每个进程的最大网络连接数量。有关更多信息，请参见第 118 页的 “每个进程的连接数量”。
   - 设置连接的最大空闲时间。有关更多信息，请参见第 120 页的 “切断空闲连接”。
8. 指定以下进程设置：
   - 设置每个进程的最大线程数量。有关更多信息，请参见第 119 页的 “每个进程的线程数量”。
   - 设置最大进程数量。有关更多信息，请参见第 118 页的 “进程数量”。
9. 如果需要，在 IMAP 服务标题字段中指定服务标题。

10. 单击 “保存”。

命令行 您可以按照以下方法在命令行中设置 IMAP 属性的值：

启用或禁用 IMAP 服务：

```
configutil -o service.imap.enable -v [ yes | no ]
```

指定端口号：

```
configutil -o service.imap.port -v number
```

为基于 SSL 的 IMAP 启用单独的端口：

```
configutil -o service.imap.enablesslport -v [ yes | no ]
```

为基于 SSL 的 IMAP 指定端口号：

```
configutil -o service.imap.sslport -v number
```

启用或禁用 IMAP 服务的密码登录：

```
configutil -o service.imap.plaintextmincipher -v value
```

其中 *value* 是以下值之一：

```
 -1 — 禁用密码登录
  0 — 启用密码登录而不进行加密
 40 — 启用密码登录并指定加密强度
128 — 启用密码登录并指定加密强度
```

设置每个进程的最大网络连接数量：

```
configutil -o service.imap.maxsessions -v number
```

设置连接的最大空闲时间：

```
configutil -o service.imap.idletimeout -v number
```

设置每个进程的最大线程数量：

```
configutil -o service.imap.maxthreads -v number
```

设置最大进程数量：

```
configutil -o service.imap.numprocesses -v number
```

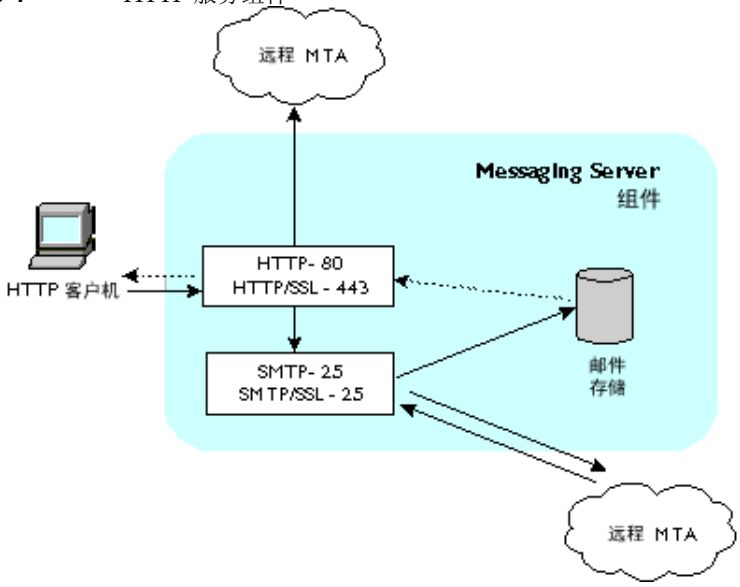
指定协议欢迎标题：

```
configutil -o service.imap.banner -v banner
```

配置 HTTP 服务

POP 和 IMAP 客户机将邮件直接发送给 Messaging Server MTA，以进行路由或传送。相反， HTTP 客户机将邮件发送给专用的 Web Server， Web Server 是 Messaging Server 的一部分。 HTTP 服务随后将邮件发送给本地 MTA 或远程 MTA，以进行路由或传送 （如图 5-1 所示）。如果 Messaging Server 仅用于基于 Web 的电子邮件，请禁用 POP 和 IMAP。

图 5-1 HTTP 服务组件



许多 HTTP 配置参数都与 POP 和 IMAP 服务的可用参数相类似。其中包括用于连接设置和进程设置的参数。本节介绍了一些比较常用的 HTTP 服务选项。在 Sun Java System Messaging Server Administration Reference 中可以查看完整列表。有关详细信息，另请参见：

- 第 114 页的 “启用和禁用服务”
- 第 114 页的 “指定端口号”
- 第 117 页的 “基于密码的登录”
- 第 118 页的 “每个进程的连接数量”
- 第 120 页的 “切断空闲连接”

- 第 120 页的 “注销 HTTP 客户机”
- 第 119 页的 “每个进程的线程数量”
- 第 118 页的 “进程数量”

某些参数是 HTTP 服务特有的；其中包括邮件设置参数和 MTA 设置参数。

邮件设置 HTTP 客户机构建带有附件的邮件时，附件被上载到服务器并存储在文件中。在将邮件发送给 MTA 进行路由或传送之前， HTTP 服务将检索附件并构建邮件。您可以接受默认的附件假脱机目录，也可以指定替换目录。您还可以指定允许的附件最大大小。

MTA 设置 默认情况下， HTTP 服务将外发 Web 邮件发送给本地 MTA，以进行路由或传送。您可能希望把 HTTP 服务配置为将邮件发送给远程 MTA，例如，如果您的站点提供托管服务并且大部分收件人不在与本地主机计算机相同的域中。要将 Web 邮件发送给远程 MTA，您需要指定远程主机名称和远程主机的 SMTP 端口号。

Console 要使用 Sun ONE Console 配置 HTTP 服务，请执行以下操作：

1. 从 Sun ONE Console 中打开要配置的 Messaging Server。
2. 单击 “配置”选项卡并打开左窗格中的 “服务”文件夹。
3. 选择 “HTTP”。
4. 单击右窗格中的 “系统”选项卡。
5. 要启用服务，请选取标有 “启用端口处的 HTTP 服务”的框，然后指定端口号。
6. 如果需要，启用基于密码的登录。
7. 指定以下连接设置：
   - 设置每个进程的最大网络连接数量。有关更多信息，请参见第 118 页的 “每个进程的连接数量”。
   - 设置连接的最大空闲时间。有关更多信息，请参见第 120 页的 “切断空闲连接”。
   - 设置客户机会话的最大空闲时间。有关更多信息，请参见第 120 页的 “注销 HTTP 客户机”。
8. 指定以下进程设置：
   - 设置每个进程的最大线程数量。有关更多信息，请参见第 119 页的 “每个进程的线程数量”。
   - 设置最大进程数量。有关更多信息，请参见第 118 页的 “进程数量”。

9. 指定以下邮件设置：

   - 如果需要，指定附件假脱机目录。
   - 如果需要，指定最大外发邮件大小。请注意，这包括以 base64 编码的所有附件，而 base64 编码要求 33% 的额外空间。因此，控制台中 5 兆字节的限制将导致邮件和附件的最大大小为 3.75 M 左右。

   有关更多信息，请参见第 126 页的 “邮件设置”。

10. 指定以下 MTA 设置：

    - 如果需要，指定替换的 MTA 主机名。
    - 如果需要，指定替换的 MTA 端口。

    有关更多信息，请参见第 126 页的 “MTA 设置”。

11. 单击 “保存”。

命令行 您可以按照以下方法在命令行中设置 HTTP 属性的值 （有关更多信息，请参见位于 http://docs.sun.com/doc/819-0106 的 Sun Java System Messaging Server Administration Reference）：

启用或禁用 HTTP 服务：

```
configutil -o service.http.enable -v [ yes | no ]
```

指定端口号：

```
configutil -o service.http.port -v number
```

为基于 SSL 的 HTTP 启用单独的端口：

```
configutil -o service.http.enablesslport -v [ yes | no ]
```

为基于 SSL 的 HTTP 指定端口号：

```
configutil -o service.http.sslport -v number
```

启用或禁用密码登录：

```
configutil -o service.http.plaintextmincipher -v value
```

其中 *value* 是以下值之一：

```
 -1 — 禁用密码登录
  0 — 启用密码登录而不进行加密
 40 — 启用密码登录并指定加密强度
128 — 启用密码登录并指定加密强度
```

设置每个进程的最大网络连接数量：

```
configutil -o service.http.maxsessions -v number
```

设置连接的最大空闲时间：

```
configutil -o service.http.idletimeout -v number
```

设置客户机会话的最大空闲时间：

```
configutil -o service.http.sessiontimeout -v number
```

设置每个进程的最大线程数量：

```
configutil -o service.http.maxthreads -v number
```

设置最大进程数量：

```
configutil -o service.http.numprocesses -v number
```

指定客户机外发邮件的附件假脱机目录：

```
configutil -o service.http.spooldir -v dirpath
```

指定最大邮件大小：

```
configutil -o service.http.maxmessagesize -v size
```

其中 *size* 是字节数。请注意，这包括以 base64 编码的所有附件，而 base64 编码要求 33% 的额外空间。因此，控制台中 5 兆字节的限制将导致邮件和附件的最大大小为 3.75 M 左右。

指定替换的 MTA 主机名：

```
configutil -o service.http.smtphost -v hostname
```

为替换 MTA 主机名指定端口号：

```
configutil -o service.http.smtpport -v portnum
```

第 6 章

启用单点登录 (SSO)

单点登录是指最终用户进行一次验证 （即使用用户 ID 和密码登录）后即可访问多个应用程序的功能。 Sun Java System Access Manager （请注意，它以前称作 Identity Server）是用于 Sun Java System 服务器的 SSO 的正式网关。也就是说，用户必须登录到 Access Manager 才能访问其他配置了 SSO 的服务器。

例如，如果正确配置了 Messenger Express，用户在 Sun Java System Access Manager 登录屏幕登录后，就可以在其他窗口访问 Messenger Express，而不必再次登录。同样，如果正确配置了 Sun Java System Calendar Server，用户在 Sun Java System Access Manager 登录屏幕登录后，就可以在其他窗口中访问 Calendar Server，而不必再次登录。

请注意， Messaging Server 提供了两种部署 SSO 的方法。第一种方法是通过 Sun Java System Access Manager，第二种方法是通过通信服务器信任的范围技术。使用信任范围是实现 SSO 的传统方法。尽管此方法提供了 Access Manager SSO 所没有的一些功能，但是不建议使用此方法，因为未来所有开发都将使用 Access Manager。但是，在以下各节中对这两种方法都进行了介绍：

- 第 130 页的 “用于 Sun Java System 服务器的 Access Manager SSO”
- 第 132 页的 “信任范围 SSO （传统）”

用于 Sun Java System 服务器的 Access Manager SSO

本节介绍了使用 Access Manager 的 SSO。其中包含以下各节：

- 第 130 页的 “SSO 限制和注意事项”
- 第 130 页的 “将 Messaging Server 配置为支持 SSO”
- 第 132 页的 “SSO 错误诊断”

SSO 限制和注意事项

- Messenger Express 会话仅在 Access Manager 会话有效时才有效。如果用户从 Access Manager 注销， Webmail 会话将自动关闭 （单点注销）。
- 协同工作的 SSO 应用程序必须位于同一 DNS 域中。（也称作 cookie 域）。
- SSO 应用程序必须具有对 Access Manager 验证 URL （命名服务）的访问权限。
- 浏览器必须具有 cookie。

将 Messaging Server 配置为支持 SSO

有四个 `configutil` 参数支持 Messaging Server SSO。对 Messaging Server 启用 SSO 时，只有其中一个参数 `local.webmail.sso.amnamingurl` 是必需的。要启用 SSO，请将此参数设置为 Access Manager 运行命名服务所在的 URL。通常此 URL 是 http://*server*/amserver/namingservice。示例：

```
configutil -o local.webmail.sso.amnamingurl -v
http://sca-walnut:88/amserver/namingservice
```

注 Access Manager SSO 不查看 `local.webmail.sso.enable`，该参数启用旧的 SSO 机制。应该将 `local.webmail.sso.enable` 保留为 `off` 或不对其进行设置，否则将记录关于缺少配置参数的警告消息，而这些配置参数只为旧的 SSO 机制所需。

您可以使用 `configutil` 命令修改表 6-3 所示的 SSO 配置参数。

表 6-1 Access Manager 单点登录参数

参数	说明
`local.webmail.sso.amnamingurl`	Access Manager 运行命名服务所在的 URL。通过 Access Manager 进行单点登录的强制性变量。通常此 URL 是 `http://`*server*`/amserver/namingservice`。 默认值：未设置。
`local.webmail.sso.amcookiename`	Access Manager cookie 名称。如果将 Access Manager 配置为使用其他 cookie 名称，则需要在 Messaging Server 中将该名称配置为 `local.webmail.sso.amcookiename`，以便在进行单点登录时 Messaging Server 知道要查找的内容。默认值是 `iPlanetDirectoryPro`，如果 Access Manager 有默认配置，则不能对其进行更改。 默认值：`iPlanetDirectoryPro`
`local.webmail.sso.amloglevel`	AMSDK 日志记录级别。 Messaging Server 使用的 SSO 库有自己的日志机制，不同于 Messaging Server 的日志机制。其邮件记录在 *msg_svr_base*`/log` 下名为 `http_sso` 的文件中。默认情况下，仅记录具有 *info* 或更高优先级的邮件，但可以通过将日志级别设置为 1 到 5 之间的值 （1 = errors、 2 = warnings、 3 = info、 4 = debug、 5 = maxdebug）来提高日志级别。请注意，库的邮件重要性的概念不同于 Messaging Server，将级别设置为 *debug* 可能会导致大量无意义的数据。另外，`http_sso` 日志文件不由通用的 Messaging Server 日志代码管理，无法清除或翻过此日志文件。将日志级别设置为高于默认级别时，系统管理员将负责将其清除。 默认值：3
`local.webmail.sso.singlesignoff`	从 Messaging Server 到 Access Manager 的单点注销。 Access Manager 是中心验证权威，将始终启用从 Access Manager 到 Messaging Server 的单点注销。此选项允许站点配置 Webmail 中的“**注销**”按钮是否还应将用户从 Access Manager 中注销 （保存某些定制工作）。默认情况下，将启用此选项。如果禁用此选项，从默认的 Webmail 客户机注销的用户将自动重新登录，因为只要 Access Manager cookie 存在并有效，注销将引用文档根目录，而文档根目录将引用收件箱显示。因此，选择禁用此选项的站点需要对 Webmail 注销时的操作进行自定义。 默认值：yes

SSO 错误诊断

如果 SSO 有问题，要做的第一件事情是检查 Webmail 日志文件 *msg_svr_base*/log/http，以查找错误。提高日志级别可能会有帮助 (configutil -o logfile.http.loglevel -v debug)。如果这样做没有帮助，请检查 *msg_svr_base*/log/http_sso 中的 amsdk 消息，然后提高 amsdk 日志记录级别 (configutil -o local.webmail.sso.amloglevel -v 5)。请注意，新的日志级别只有在服务器重新启动后才能生效。

如果 SSO 仍有问题，请确认在登录过程中是否使用了 Access Manager 和 Messaging Server 的全限定主机名。 Cookie 仅在同一域中的服务器之间共享，而浏览器不知道什么域用于本地服务器名称，因此必须在浏览器中使用全限定名称才能使 SSO 工作。

信任范围 SSO （传统）

本节介绍了信任范围 SSO。由于将来所有的开发都将使用 Access Manager，因此不建议使用此种方法的 SSO。但是，信任范围 SSO 的某些可用功能是 Access Manager SSO 现在没有的。本节包含以下几部分：

- 第 132 页的 “信任范围 SSO 概述和定义”
- 第 133 页的 “信任范围 SSO 应用程序”
- 第 134 页的 “信任范围 SSO 限制”
- 第 134 页的 “信任范围 SSO 部署方案示例”
- 第 136 页的 “设置信任范围 SSO”
- 第 140 页的 “Messenger Express 信任 SSO 配置参数”

信任范围 SSO 概述和定义

部署 SSO 之前，请务必了解以下术语。

- **SSO**：单点登录。登录到一个应用程序即可访问其他应用程序的功能。用户身份标识在所有应用程序中相同。
- **信任的应用程序**。共享 SSO 方案 （*SSO* **前缀**）并信任彼此的 cookie 和检验的应用程序。也称为**对等** *SSO* **应用程序**。
- **信任范围**。信任的应用程序的圈子。这些应用程序共享同一个 SSO 前缀。

- **SSO 前缀**。一个字符串， SSO 的部署者定义并告知应用程序，以便应用程序可以使用该字符串查找同一信任范围中其他应用程序生成的 cookie。具有不同前缀的应用程序不在同一圈中，用户在这些应用程序之间移动时需要重新验证。在配置设置中，前缀有时 （但不总是）明确地包含结尾字符 — ("-")。
- **应用程序 ID**。 (appid)。 SSO 部署者为 SSO 圈中每个应用程序定义的唯一字符串。
- **SSO Cookie**。浏览器用于记住用户已经通过某个应用程序验证的标记。Cookie 名称的格式为 *SSO*_ **前缀** — **应用程序** *ID*。 Cookie 的值为 SSO 密钥，通常是应用程序生成的会话 ID。
- **Cookie 域**。应用程序被限制为只能在此域中发送 cookie。这是 DNS 意义的域。
- **验证 URL**。某个应用程序用于向其他应用程序验证其查找到的 cookie 的 URL。

信任范围 SSO 应用程序

实现 SSO 之前，您必须首先考虑哪些应用程序将位于此信任范围中。可位于此信任范围内的应用程序包括 Messenger Express （带有或不带有 Messenger Express Multiplexor）、 Calendar Express 和旧版 iPlanet Delegated Administrator for Messaging （由于仅支持 Sun LDAP Schema 1，因此不建议使用）。

表 6-2 显示了可通过 SSO 彼此访问的应用程序。从用户的角度来看，如果登录到第一列中某个应用程序后，无需重新输入用户 ID 和密码即可访问顶端行中的应用程序，则 SSO 工作。

表 6-2 SSO 互操作性

到: 从:	Calendar Express	Messenger Express	Messenger Express Multiplexor	Delegated Administrator
Calendar Express	SSO	SSO	SSO	SSO
Messenger Express	SSO	N/A	N/A	SSO
Messenger Express Multiplexor	SSO	N/A	N/A	SSO
Delegated Administrator	SSO	SSO	SSO	N/A

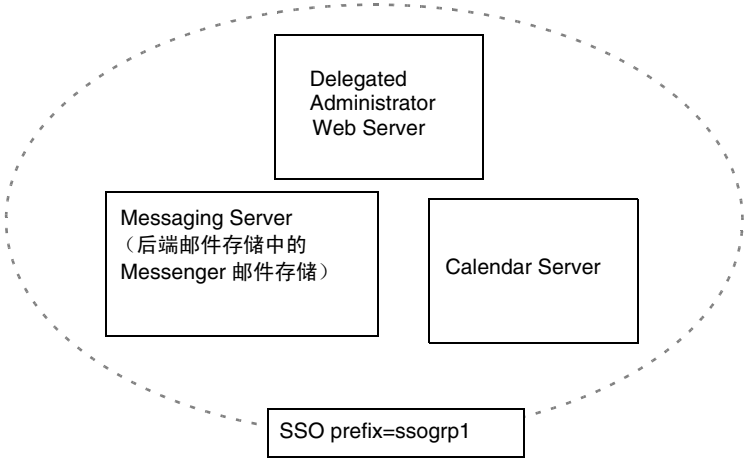
信任范围 SSO 限制

- 协同工作的 SSO 应用程序必须位于同一域中。
- SSO 应用程序必须具有对彼此的 SSO 检验 URL 的访问权限。
- 浏览器必须支持 Cookie。
- 为安全起见，不应该在运行浏览器的计算机中使用 SSO。
- 要切换为其他身份标识，需要重新启动浏览器。
- 假设既在 Messenger Express 中启用了单点注销，又为 Sun Java System Calendar Server 启用了单点注销，如果您从 Sun Java System Calendar Server 注销，则必须重新登录到 Messenger Express。如果您从 Messenger Express 注销，则必须重新登录到 Sun Java System Calendar Server。但是，目前并不是这样工作的。从一个应用程序注销后，您可能仍然在另一个应用程序中保持登录状态。

信任范围 SSO 部署方案示例

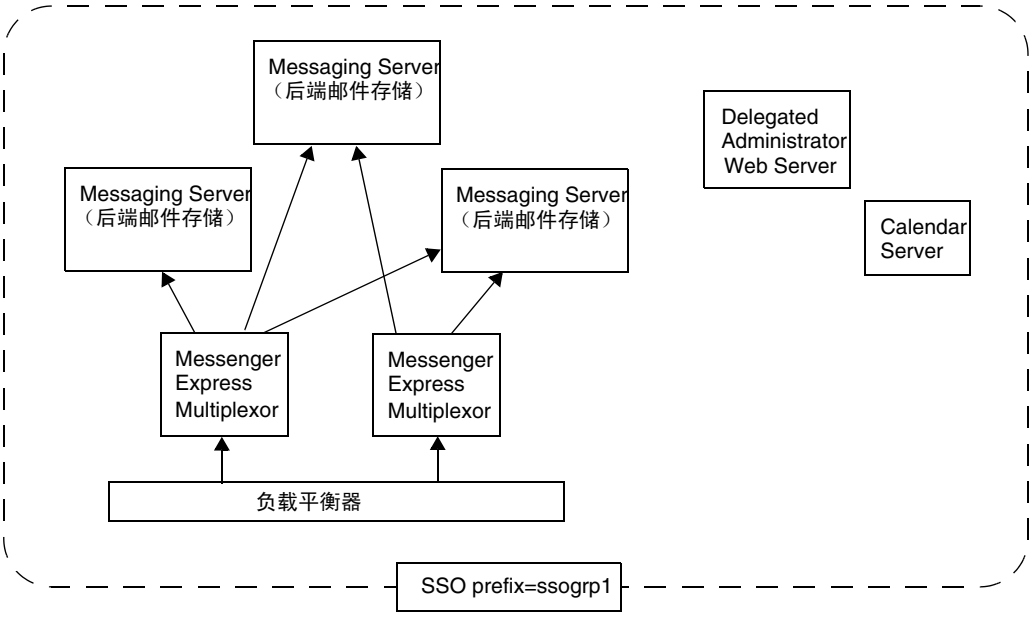
最简单的 SSO 部署方案仅由 Messenger Express 和 iPlanet Delegated Administrator for Messaging 组成。在同一计算机中或不同计算机中添加使用相同 SSO 前缀 （以便其位于同一信任范围中）的 Calendar Express 可以创建较复杂的方案。如图 6-1 所示。

图 6-1 简单 SSO 部署



更复杂的部署将包括 Messenger Express Multiplexors 和负载平衡器。

图 6-2 复杂 SSO 部署



设置信任范围 SSO

本节介绍如何为 Messenger Express、 iPlanet Delegated Administrator for Messaging 和 Calendar Manager 设置 SSO。

1. 配置 Messenger Express 用于 SSO。

   a. 设置适当的 SSO `configutil` 参数。

      要为具有 Delegated Administrator 的 Messenger Express 启用单点登录，请按照以下方法设置配置参数 （假定默认域是 siroe.com）。表 6-3 中介绍了这些参数。您必须是超级用户。使用 `cd` 命令进入到 *instance_root*

```
configutil -o local.webmail.sso.enable -v 1
configutil -o local.webmail.sso.prefix -v ssogrp1
      ssogrp1 是 iDA 使用的默认 SSO 前缀，尽管您可以选择其他前缀，
     但是使用默认前缀可以在配置 iDA 和 iCS 时省去一些键入操作。
configutil -o local.webmail.sso.id -v ims5
     ims5 是您选择用于标识 Messenger Express (ME) 以使其不同于其他应用程序的名称。
configutil -o local.webmail.sso.cookiedomain -v ".siroe.com"
     以上域必须与 ME/ 浏览器客户机使用的域匹配，才能连接到
     服务器。因而，尽管此服务器中的托管域可能被称为 xyz.com，但必须
     使用 DNS 中的真实域。该值必须以句点开头。
configutil -o local.webmail.sso.singlesignoff -v 1
configutil -o local.sso.ApplicationID.verifyurl -v \
     "http://ApplicationHost:port/verifySSO?"
     ApplicationID 是授予 SSO 应用程序的名称 （例如：
     对于 Delegated Administrator 为 ida、对于 Calendar Server 为 ics50）。 ApplicationHost:port 是
     应用程序的主机和端口号。对于每个非 Messaging Server 应用程序，您将有上述行中的其中一行。
例如：
     configutil -o local.sso.ida.verifyurl -v \
       "http://siroe.com:8080/verifySSO?"
```

   b. 更改配置后重新启动 Messenger Express HTTP 服务器。

      ```
      cd instance_root
      ./stop-msg http
      ./start-msg http
      ```

2. 配置 Directory Server 用于 SSO。

a. 在目录中创建代理用户帐户。

代理用户帐户使 Delegated Administrator 可以绑定到 Directory Server 以进行代理验证。使用以下 LDIF 代码 (`proxy.ldif`)，您可以创建使用 `ldapadd` 的代理用户帐户条目。

`ldapadd -h mysystem.siroe.com -D "cn=Directory Manager" -w` *`password`* `-v -f proxy.ldif`

```
dn: uid=proxy, ou=people, o=siroe.com, o=isp
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
uid: proxy
givenname: Proxy
sn: Auth
cn: Proxy Auth
userpassword: proxypassword
```

b. 为代理用户帐户验证创建适当的 ACI。

使用 `ldapmodify` 实用程序为安装 Delegated Administrator 时创建的每个后缀创建一个 ACI。

`osiroot` — 您输入的用于存储用户数据的后缀 （默认值是 `o=isp`）。 `osiroot` 是组织树的根目录。

`dcroot` — 您输入的用于存储域信息的后缀。（默认值是 `o=internet`）

`osiroot` — 您输入的用于存储配置信息的后缀，应当与您输入的用于存储用户数据的值相同。

以下是早期创建的代理用户的 `osiroot` 的 ACI 条目 (`aci1.ldif`) 的示例：

```
dn: o=isp
changetype: modify
add: aci
aci: (target="ldap:///o=isp")(targetattr="*")(version 3.0; acl
"proxy";allow (proxy) userdn="ldap:///uid=proxy, ou=people,
o=siroe.com, o=isp";)
```

ldapmodify -h siroe.com -D "cn=Directory Manager" -w *password* **-v -f aci1.ldif**

为 dcroot 创建类似的 ACI 条目 (aci2.ldif)：

```
dn: o=internet
changetype: modify
add: aci
aci: (target="ldap:///o=internet")(targetattr="*")(version 3.0; acl
"proxy";allow (proxy) userdn="ldap:///uid=proxy, ou=people,
o=siroe.com, o=isp";)
```

ldapmodify -h siroe.com -D "cn=Directory Manager" -w *password* **-v -f aci2.ldif**

3. 配置 Delegated Administrator

   a. 将代理用户证书和上下文的 cookie 名称添加到 Delegated Administrator resource.properties 文件。

      在 Delegated Administrator *iDA_server_root*/nda/classes/netscape/nda/servlet/resource.properties 文件中取消以下条目的注释并对其进行修改：

      LDAPDatabaseInterface-ldapauthdn=*Proxy_Auth_DN*
      LDAPDatabaseInterface-ldapauthpw=*Proxy_Auth_Password*
      NDAAuth-singleSignOnId=*SSO_Prefix*-
      NDAAuth-applicationId=*DelAdminID*

      例如：

      ```
      LDAPDatabaseInterface-ldapauthdn=
         uid=proxy, ou=people, o=siroe.com, o=isp
      LDAPDatabaseInterface-ldapauthpw=proxypassword
      NDAAuth-singleSignOnId=ssogrp1-
      NDAAuth-applicationId=ida
      ```

   b. 添加参与的服务器的检验 URL。

      要检验接收到的单点登录 cookie， Delegated Administrator 必须知道联系的对象。您必须为所有已知的参与的服务器提供检验 URL。

按照示例，假定已安装 Messenger Express 并且其应用程序 ID 是 msg5。编辑 Delegated Administrator *iDA_server_root*/nda/classes/netscape/nda/servlet/resource.properties 文件，并添加一个条目，例如：

```
verificationurl-ssogrp1-msg5=http://webmail_hostname:port/VerifySSO?
verificationurl-ssogrp1-ida=http://iDA_hostname:port/VerifySSO?
verificationurl-ssogrp1-ics50=http://iCS_hostname:port/VerifySSO?
```

4. 添加 Delegated Administrator 单点登录 cookie 信息并启用 UTF8 参数编码。

   a. 定义 Delegated Administrator 的上下文标识符。

      编辑 *Web_Server_Root*/https-*instancename*/config/servlets.properties，并取消包含文本 servlet.*.context=ims50 的所有行的注释。其中 * 表示任意字符串。

   b. 在 Enterprise Server 配置中指定上下文的 cookie 名称。

      编辑 Enterprise Server 文件 *Web_Server_Root*/https-*instancename*/config/contexts.properties，并将以下行添加到文件底部、 #IDACONF-Start 行之前：

      ```
      context.ims50.sessionCookie=ssogrp1-ida
      ```

   c. 为 ims5 上下文启用 UTF8 参数编码。

      要在 Enterprise Server 配置中为 ims5 上下文启用 UTF8 参数编码，请将以下条目添加到 Enterprise Server *WebServer_Root*/https-*instancename*/config/contexts.properties 文件中：

      ```
      context.ims50.parameterEncoding=utf8
      ```

5. 重新启动 Messenger Express。

   按照步骤 1a 至 2c 所述更改了配置后，您必须使用以下命令重新启动 Messenger Express 才能使更改生效：

   WebServer_Root`/https-i`*instance_name*`/stop`
   WebServer_Root`/https-`*instancename*`/start`

6. 如果在此 SSO 组中部署 Calendar Server，请配置 Calendar Server。

   编辑 `ics.conf` 并添加以下内容：

```
sso.appid = "ics50"
sso.appprefix = "ssogrp1"
sso.cookiedomain = ".red.iplanet.com"
sso.enable = "1"
sso.singlesignoff = "true"
sso.userdomain = "mysystem.red.iplanet.com"
sso.ims5.url="http://mysystem.red.iplanet.com:80/VerifySSO?"
sso.ida.url=http://mysystem.red.iplanet.com:8080/VerifySSO?
```

7. 重新启动 Calendar Server

```
start-cal
```

8. 重新启动 Messenger Express HTTP 服务器：

   msg_svr_base/sbin**/stop-msg http**
   msg_svr_base/sbin**/start-msg http**

Messenger Express 信任 SSO 配置参数

您可以使用 `configutil` 命令修改 Messenger Express 的单点登录配置参数（如表 6-3 所示）。有关 `configutil` 的详细信息，请参见 Messaging Server Reference Manual。

表 6-3 信任范围单点登录参数

参数	说明
`local.sso.`*appid*`.verifyurl`	为对等 SSO 应用程序设置验证 URL 值。*appid* 是 SSO cookie 将生效的对等 SSO 应用程序的应用程序 ID。例如， Delegated Administrator 的默认 *appid* 是 `nda45`。其实际值由 Delegated Administrator `resource.properties` 文件条目 `NDAAuth-applicationID` 指定。 应该为每个信任的对等 SSO 应用程序定义一个参数。检验 URL 的标准格式为： `http://`*nda-host:port*`/VerifySSO?` 如果在多个 Messenger Express Multiplexor 和邮件存储服务器 （运行 Messenger Express）前端或日历前端使用负载平衡器，请确保为 `verifyurl` 中带有真实主机名的每个物理系统指定**不同的** `appid`。这将确保使用正确的系统来检验 cookie

表 6-3 信任范围单点登录参数

参数	说明
local.webmail.sso.cookiedomain	此参数的字符串值用于设置由 Messenger Express HTTP 服务器设置的所有 SSO cookie 的 cookie 域值。默认值为空。 该域必须与 Messenger Express 浏览器用于访问服务器的 DNS 域相匹配。它不是托管的域名。
local.webmail.sso.enable	启用或禁用所有单点登录功能，包括获取登录页面后接受和检验客户机提供的 SSO cookie、在成功登录的情况下将 SSO cookie 返回给客户机以及响应来自其他 SSO 同伴的要求检验其 cookie 的请求。 如果设置为任何非零值，服务器将执行所有 SSO 功能。 如果设置为零，服务器将不执行任何 SSO 功能。 默认值为零。
local.webmail.sso.id	对 Messenger Express HTTP 服务器设置的 SSO cookie 进行格式化时，将此参数的字符串值用作应用程序 ID 值。默认值为空。 这可以是任意字符串。它的值必须与您在 Delegated Administrator 的 resource.properties 文件中为其指定的值相匹配。resource.properties 中相应的条目是： Verifycationurl-XXX-YYY=http://webmailhost:webmailport/VerifySSO? 其中 XXX 是上文中设置的 local.webmail.sso.prefix 值，而 YYY 是此处设置的 local.webmail.sso.id 值。
local.webmail.sso.prefix	对 Messenger Express HTTP 服务器设置的 SSO cookie 进行格式化时，将此参数的字符串值用作前缀值。服务器只能识别带有此前缀的 SSO cookie；将忽略其他所有 SSO cookie。 此参数的空值将有效禁用服务器中所有 SSO 功能。 默认值为空。 该字符串必须与 iPlanet Delegated Administrator for Messaging 在其 resource.properties 文件中使用的字符串 （不带有结尾字符 -）相匹配。例如，如果： NDAAuth-singleSignOnID=ssogrp1- 则应该在此处将该值设置为 ssogrp1。
local.webmail.sso.singlesignoff	此参数的整数值 （如果设置为任何非零值）将在客户机注销时清除客户机（如果其前缀值与 local.webmail.sso.prefix 中配置的值相匹配）中的所有 SSO cookie。 如果设置为零，则客户机注销时 Messenger Express 将清除自己的 SSO cookie。 默认值为零。

第 7 章

配置和管理多路复用器服务

本章介绍 Messaging Server 附带的两个多路复用器：用于标准邮件协议 （POP、IMAP 和 SMTP）的 Messaging Multiplexor (MMP) 和用于 Messenger Express Web 接口的 Messenger Express Multiplexor。

本章包含以下主题：

- 第 143 页的 “多路复用器服务”
- 第 145 页的 “关于 Messaging Multiplexor”
- 第 150 页的 “设置 Messaging Multiplexor”
- 第 153 页的 “配置 MMP 以使用 SSL”
- 第 159 页的 “设置故障转移 MMP LDAP 服务器”
- 第 159 页的 “关于 Messenger Express Multiplexor”

多路复用器服务

多路复用器是实现横向可伸缩性 （通过添加更多计算机来支持更多用户的能力）所必需的，因为它提供了可用于间接连接到多个邮件存储的单一域名。多路复用器还可以提供安全性方面的优点。

MMP 是独立于 Messaging Server 进行管理的，而 Messenger Express Multiplexor 则内置于邮件存储和邮件访问安装所附带的 HTTP 服务 (`mshttpd`) 中。

多路复用器的优点

频繁使用的邮件传送服务器上的邮件存储会增长到非常大。因此，将用户邮箱和用户连接分布在多个服务器上可以提高容量和性能。此外，使用多台小型服务器计算机可能比使用一台大型、高容量、多处理器的计算机更划算。

如果您的邮件服务器安装大小要求使用多个邮件存储，则您的组织可以通过使用多路复用器在若干方面受益。用户与其邮件存储之间的间接连接，以及在多个邮件传送服务器上重新配置用户帐户的方便性具有以下优点：

- **简化了用户管理**

  因为所有用户都连接到一个服务器 （或者，如果有分别用于 POP、 IMAP、 SMTP 或 Web 访问的多路复用器计算机，则连接到多个服务器），所以您可以预先配置电子邮件客户机并向所有用户分发统一的登录信息。这简化了您的管理任务并减少了分发错误的登录信息的可能性。

  对于负载特别高的情况，您可以运行具有相同配置的多个多路复用器服务器并通过 DNS 循环或使用负载平衡系统来管理与它们的连接。

  因为多路复用器使用存储在 LDAP 目录中的信息来查找每个用户的 Messaging Server，所以系统管理员可以很容易地将某个用户移动到一个新服务器中，并且这一过程对用户来说是透明的。管理员可以将用户的邮箱从一个 Messaging Server 移动到另一个中，然后更新 LDAP 目录中该用户的条目。该用户的邮件地址、邮箱访问和其它客户机首选项不需要更改。

- **提高了性能**

  如果单个计算机上的邮件存储增长到过分大，则可以通过将某些邮件存储移动到其他计算机上来平衡负载。

  可以将不同的用户类指定到不同的计算机上。例如，可以选择将贵宾用户放在功能更强大的大型计算机上。

  多路复用器将执行某些缓冲，从而使慢速客户机连接 （例如，通过调制解调器）不会降低 Messaging Server 的速度。

- **降低了成本**。因为可以使用一个多路复用器有效地管理多个 Messaging Server，所以可以通过购买多台小型服务器计算机 （其总成本要少于一台大型计算机）来降低整体成本。

- **更好的可伸缩性**。使用多路复用器，可以非常方便地扩展您的配置。您可以在性能和存储容量需要增长时逐渐地添加计算机，而无需替换现有的投入。

- **最短的用户停机时间**。使用多路复用器将一个大型用户库分布在许多小型存储计算机上可以分隔用户的停机时间。当单个服务器出现故障时，只有该服务器的用户会受到影响。

- **提高了安全性**。可以使用安装了多路复用器的服务器计算机作为防火墙计算机。通过此计算机路由所有客户机连接，您可以限制外部计算机对内部邮件存储计算机的访问。多路复用器支持与客户机的未加密和加密的通信。

关于 Messaging Multiplexor

Sun Java System Messaging Multiplexor (MMP) 是专用的邮件传送服务器，用作与多个后端邮件传送服务器的单点连接。使用 Messaging Multiplexor，大规模的邮件传送服务提供商可以将 POP 和 IMAP 用户邮箱分布在许多计算机上以提高邮件存储容量。所有用户都连接到一个多路复用器服务器，该服务器会将每个连接重定向到适当的邮件传送服务器。

如果您为许多用户提供电子邮件服务，则可以安装和配置 Messaging Multiplexor，这样整个邮件传送服务器阵列便可以作为一个单一主机呈现给邮件用户。

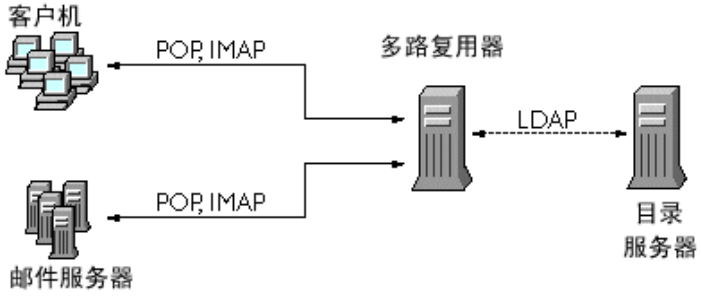
Messaging Multiplexor 是作为 Messaging Server 的一部分提供的。您可以在安装 Messaging Server 或其他 Sun Java System 服务器的同时安装 MMP，也可以在将来某个时候单独安装 MMP。 MMP 支持：

- 与邮件客户机进行未加密和加密的 (SSL) 通信。
- 基于证书的客户机验证，如第 147 页的 “基于证书的客户机验证”中所述。
- 用户预验证，如第 148 页的 “用户预验证”中所述。
- 侦听不同 IP 地址并自动向用户 ID 附加域名的虚拟域，如第 148 页的 “MMP 虚拟域”中所述。
- 在不同服务器上安装多个 MMP （请参见 Sun Java Enterprise System 安装指南）。
- 增强的 LDAP 搜索功能。
- 用于传统 POP 客户机的 “在 SMTP 之前先执行 POP”的服务。有关更多细信息，请参见第 601 页的 “启用 POP Before SMTP”。

Messaging Multiplexor 的工作原理

MMP 是多线程的服务器，它可以协助在多台服务器计算机上分布邮件用户。 MMP 可控制将去往其他服务器计算机 （用户邮箱所在的计算机）的外来客户机连接。客户机将连接到 MMP 本身， MMP 为用户确定正确的服务器，然后连接到该服务器并在客户机和服务器之间传递数据。此功能使 Internet 服务提供商和其他大型安装能够将邮件存储分布在多台计算机上 （可以增加容量），同时为用户和外部客户机呈现了一个单一的邮件主机 （针对用户可以提高效率，针对外部客户机可以提高安全性）。图 7-1 显示了 MMP 安装中服务器和客户机彼此之间的相关方式。

图 7-1 MMP 安装中的客户机和服务器



所有 POP、IMAP 和 SMTP 客户机都可以使用 Messaging Multiplexor。MMP 将接受连接、执行 LDAP 目录查找并适当地路由连接。与其他邮件服务器安装中的典型情况一样，每个用户都被指定一个位于特定 Messaging Server 上的特定地址和邮箱。但是，所有连接都将通过 MMP 来路由。

下面详细介绍了建立用户连接中所涉及的步骤：

1. 用户的客户机连接到 MMP， MMP 将接受初步的验证信息 （用户名）。
2. MMP 查询 Directory Server 以确定包含该用户的邮箱的 Messaging Server。
3. MMP 连接到适当的 Messaging Server，重新进行验证，然后在连接过程中充当通信管道。

加密 (SSL) 选项

Messaging Multiplexor 支持在 Messaging Server 及其邮件客户机之间进行未加密和加密的 (SSL) 通信。 Messaging Server 支持新证书数据库格式 (cert8.db)。

当启用 SSL 时， MMP 支持 STARTTLS，并且还可以配置 MMP 以侦听其他用于 SSL IMAP、 POP 和 SMTP 连接的端口。

要为您的 IMAP、 POP 和 SMTP 服务启用 SSL 加密，请分别编辑 `ImapProxyAService.cfg`、`PopProxyAService.cfg` 和 `SmtpProxyAService.cfg` 文件。还必须编辑 `AService.cfg` 文件中的 `default:ServiceList` 选项以包含所有 IMAP、POP 和 SMTP 服务器端口的列表，而不管它们是否安全。有关详细信息，请参见第 153 页的 “配置 MMP 以使用 SSL”。

默认情况下， SSL 没有被启用，因为 SSL 配置参数被注释掉了。要启用 SSL，必须安装 SSL 服务器证书。然后，应当取消注释并设置 SSL 参数。有关 SSL 参数的列表，请参见 Sun Java System Messaging Server Administration Reference (`http://docs.sun.com/doc/819-0106`)。

基于证书的客户机验证

MMP 可以使用证书映射文件 (`certmap`) 将客户机的证书与用户 / 组 Directory Server 中的正确用户相匹配。

要使用基于证书的客户机验证，还必须启用 SSL 加密，如第 147 页的 “加密 (SSL) 选项”中所述。

还必须配置一个存储管理员。您可以使用邮件管理员，但是建议您为此目的创建一个唯一的用户 ID （例如 `mmpstore`），以便可以根据需要设置权限。

请注意， MMP 不支持 `certmap` 插件，而是接受 `certmap.conf` 文件中增强的 `DNComps` 和 `FilterComps` 属性值条目。这些增强的格式条目使用以下格式：

mapname`:DNComps` *FROMATTR=TOATTR*
mapname`:FilterComps` *FROMATTR=TOATTR*

这样，便可以使用证书的 subjectDN 中的 *FROMATTR* 值来构成一个具有 *TOATTR*=*value* 元素的 LDAP 查询。例如，可以使用以下行将 subjectDN 为 “`cn=Pilar Lorca, ou=pilar, o=siroe.com`”的证书映射到 LDAP 查询 “`(uid=pilar)`”：

mapname`:FilterComps ou=uid`

要为您的 IMAP 或 POP 服务启用基于证书的验证，请执行以下操作：

1. 确定要用作存储管理员的用户 ID。

   虽然可以为此目的使用邮件管理员，但是建议为存储管理员创建一个唯一的用户 ID （例如， `mmpstore`）。

2. 确保启用了（或将启用）SSL 加密，如第 147 页的 “加密 (SSL) 选项”中所述。

3. 通过在您的配置文件中指定 `certmap.conf` 文件的位置来配置 MMP 以使用基于证书的客户机验证。

4. 至少安装一个信任的 CA 证书，如第 581 页的 “安装信任的 CA 证书的步骤”中所述。

用户预验证

MMP 通过作为外来用户绑定到目录并记录结果为您提供了预验证用户的选项。

注	启用用户预验证会降低服务器的性能

日志条目的格式为：

date time `(sid 0x`*hex*`) user` *name* `pre-authenticated - client IP` *address*`, server IP` *address*

其中， *date* 的格式为 `yyyymmdd`； *time* 是在服务器上配置的时间，其格式为 `hhmmss`； *hex* 表示为六位数数字的会话标识符 (`sid`)； `user` *name* 包括虚拟域名（如果有）， IP 地址采用以点分隔的四组数字格式。

MMP 虚拟域

MMP 虚拟域是一组与服务器 IP 地址相关联的配置设置。此功能的主要用途是为每个服务器 IP 地址提供不同的默认域。

用户可以使用简短形式的用户 ID 或全限定的用户 ID （格式为 `user@domain`）来对 MMP 进行验证。提供简短形式的用户 ID 时， MMP 将附加 `DefaultDomain` 设置（如果已指定）。因此，支持多个托管域的站点只需通过将服务器 IP 地址和 MMP 虚拟域与每个托管域相关联便可以允许使用简短形式的用户 ID。

要为给定的托管域查找用户子树，建议通过该域的 LDAP 域树条目中的 inetDomainBaseDN 属性来查找。 MMP 的 LdapUrl 设置不适用于此目的，因为后端邮件存储服务器还需要在 LDAP 中查找用户并且不支持虚拟域。

当启用 Sun LDAP Schema 2 时 （请参见 Sun Java Enterprise System 安装指南和 Sun Java System Communcations Services Schema Reference Manual），指定域的用户子树将是该域的组织节点下的子树中的所有用户。

要启用虚拟域，请编辑实例目录中的 ImapProxyAService.cfg、 PopProxyAService.cfg 或 SmtpProxyAService.cfg 文件，以便 VirtualDomainFile 设置可以指定虚拟域映射文件的全路径。

每个虚拟域文件条目都具有以下语法：

vdmap *name IPaddr*
name:parameter value

其中， *name* 仅用于将 IP 地址与配置参数相关联并且可以是您选择使用的任何名称； *IPaddr* 使用了以点分隔的四组数字格式， *parameter* 和 *value* 对用于配置虚拟域。设置后，虚拟域配置参数值将覆盖全局配置参数值。

下面列出了可以为虚拟域指定的配置参数：

AuthCacheSize 和 AuthCacheSizeTTL
AuthService
BindDN 和 BindPass
CertMap
ClientLookup
CRAMs
DefaultDomain
DomainDelim
HostedDomains
LdapCacheSize 和 LdapCacheTTL
LdapURL
MailHostAttrs
PreAuth
ReplayFormat
RestrictPlainPasswords
StoreAdmin 和 StoreAdminPass
SearchFormat
TCPAccess
TCPAccessAttr

注 除非正确设置了 LdapURL，否则 BindDN、 BindPass、 LdapCacheSize 和 LdapCacheTTL 设置将被忽略。

有关这些配置参数的详细说明，请参见 Messaging Server Reference Manual。

关于 SMTP 代理

MMP 包含一个 SMTP 代理，它在默认情况下被禁用。大多数站点并不需要 SMTP 代理，因为 Internet 邮件标准已经为 SMTP （DNS MX 记录）的横向可伸缩性提供了足够的机制。

SMTP 代理所提供的安全性功能很有用。首先， SMTP 代理与 POP 代理相集成以实现某些传统 POP 客户机所要求的 “在 SMTP 之前先执行 POP”的验证功能。有关更多细信息，请参见第 601 页的 “启用 POP Before SMTP”。此外，通过使用 SMTP 代理可以最大限度地利用在 SSL 加速硬件上的投入。请参见第 587 页的 “如何使用 SMTP 代理服务器优化 SSL 性能”。

设置 Messaging Multiplexor

在 Messaging Server 的初始运行时配置过程中，您确定了是否要在计算机上配置 MMP。您可以将它与 Messaging Server 设置在同一个计算机上，也可以设置在单独的计算机上。

注 MMP 不缓存 DNS 结果。 Messaging Server 的生产部署要求在本地网络上具有高质量的高速缓存 DNS 服务器。

以下各节介绍了如何设置 MMP：

- 第 151 页的 “配置 MMP 之前”
- 第 151 页的 “多路复用器的配置”
- 第 152 页的 “多路复用器文件”
- 第 153 页的 “启动多路复用器”
- 第 153 页的 “修改现有 MMP”

有关 MMP 的详细信息，请参见以下文档：

- Sun Java System Messaging Server Administration Reference 中的 "MMP Syntax and Structure" (http://docs.sun.com/doc/819-0106)

配置 MMP 之前

配置 MMP 之前：

1. 选择要在其上配置 MMP 的计算机。最好使用一台专用于 MMP 的计算机。

注	建议不要在同时还运行了 POP 或 IMAP 服务器的计算机上启用 MMP。 如果将 MMP 和 Messaging Server 安装在同一台计算机上，则必须确保将 POP 和 IMAP 服务器设置到非标准端口。这样， MMP 和 Messaging Server 端口才不会彼此冲突。

2. 在要配置 MMP 的计算机上，创建一个要由 MMP 使用的 UNIX 系统用户。此新用户必须属于一个 UNIX 系统组。请参见第 38 页的 “创建 UNIX 系统用户和组”。
3. 设置要与 Messaging Server 一起使用的 Directory Server 及其主机 （如果尚未设置）。请参见第 39 页的 “为 Messaging Server 配置准备 Directory Server”。
4. 如果在升级后端服务器之前升级 MMP，则用户应设置 `ImapProxyAService.cfg` 中的 `Capability` 选项，才能匹配对还未升级的后端服务器的 `capability` 命令的响应。设置为：

   ```
   IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS CHILDREN LANGUAGE
   XSENDER X-NETSCAPE XSERVERINFO
   ```

   请注意，换行可使编辑清晰，但是配置值必须在一行中。

多路复用器的配置

要配置 MMP，必须使用 Messaging Server 配置程序，该程序为您提供了启用 Messaging Multiplexor 的选项。有关配置程序的详细信息，请参见第 49 页的 “创建初始 Messaging Server 运行时配置”。

要配置 MMP，请执行以下操作：

1. 在要安装和配置 MMP 的计算机上安装 Sun Java System Messaging Server。
2. 通过创建 Messaging Server 初始运行时配置来配置 MMP。请参见第 49 页的 “创建初始 Messaging Server 运行时配置”。

   请注意以下例外情况：安装 Messaging Server 时，仅检查 Messaging Multiplexor 选项。

多路复用器文件

Messaging Multiplexor 文件存储在 *msg_svr_base*/config 配置文件目录中。您必须手动编辑表 7-1 中列出的 Messaging Multiplexor 配置文件中的配置参数。有关所有 MMP 配置参数的完整说明，请参见 Sun Java System Messaging Server Administration Reference。

表 7-1 Messaging Multiplexor 配置文件

文件	说明
PopProxyAService.cfg	指定用于 POP 服务的配置变量的配置文件。
PopProxyAService-def.cfg	POP 服务配置模板。仅在使用 start-msg mmp 启动初始 MMP 之后才存在文件
ImapProxyAService.cfg	指定用于 IMAP 服务的配置变量的配置文件。
ImapProxyAService-def.cfg	IMAP 服务配置模板。仅在初始 MMP 以 start-msg mmp 开头之后，才存在文件
AService.cfg	指定要启动的服务以及一些由 POP 和 IMAP 服务共享的选项的配置文件。
AService-def.cfg	指定要启动的服务以及一些由 POP 和 IMAP 服务共享的选项的配置模板。仅在初始 MMP 以 start-msg mmp 开头之后，才存在文件
SmtpProxyAService.cfg	指定用于 SMTP 代理服务的配置变量的可选配置文件。如果启用“在 SMTP 之前先执行 POP”，则需要该配置文件；它对于最大限度地支持 SSL 硬件很有用，即使没有启用“在 SMTP 之前先执行 POP”。有关“在 SMTP 之前先执行 POP”的详细信息，请参见第 601 页的“启用 POP Before SMTP”。
SmtpProxyAService-def.cfg	指定用于 SMTP 代理服务的配置变量的配置模板。仅在初始 MMP 以 start-msg mmp 开头之后，才存在文件

举例来讲，LogDir 和 LogLevel 参数在所有配置文件中都可以找到。在 ImapProxyAService.cfg 中，它们用于为与 IMAP 相关的事件指定日志记录参数；类似地，这些参数在 PopProxyAService.cfg 中用于为与 POP 相关的事件配置日志记录参数。在 SmtpProxyAService.cfg 中，它们用于为与 SMTP 代理相关的事件指定日志记录。

但是，在 AService.cfg 中，LogDir 和 LogLevel 用于记录 MMP 范围内的故障，例如，无法启动 POP、IMAP 或 SMTP 服务。

注 当配置或升级 MMP 时，配置模板文件将被覆写。

启动多路复用器

要启动、停止或刷新 Messaging Multiplexor 的实例，请使用以下表 7-2 中的命令之一，这些命令位于 *msg_svr_base*/sbin 目录中：

表 7-2 MMP 命令

选项	说明
start-msg mmp	启动 MMP （即使一个 MMP 已在运行）。
stop-msg mmp	停止最近启动的 MMP。
refresh mmp	使一个已在运行的 MMP 刷新其配置而不会中断任何活动连接。

修改现有 MMP

要修改 MMP 的现有实例，请根据需要编辑 ImapProxyAService.cfg 和 / 或 PopProxyAService.cfg 配置文件。这些配置文件位于 *msg_svr_base*/config 子目录中。

配置 MMP 以使用 SSL

要配置 MMP 以使用 SSL，请执行以下操作：

注 假定 MMP 安装在没有邮件存储或 MTA 的计算机上。

1. 如果安装了 Admin Server，请使用管理控制台安装 SSL 服务器证书，或者使用 NSS 工具进行安装。请参见第 587 页的 “网络安全服务工具”。

   请参见 http://docs.sun.com/db/doc/816-5572-10

2. 如果安装了 Admin Server，则在命令行中，进行以下符号链接以简化操作：

   ```
   cd msg_svr_base/config
   ln -s /var/mps/serverroot/alias/admin-serv-instance-cert7.db cert7.db
   ln -s /var/mps/serverroot/alias/admin-serv-instance-key3.db key3.db
   ```

   同时，确保要运行 MMP 的系统 ID 拥有这些文件。 Messaging Server 支持新证书数据库格式 (cert8.db)。

3. 由于 sslpassword.conf 文件是在初始 Messaging Server 运行时配置过程中设置的，因而不需要设置该文件。请参见第 49 页的 “创建初始 Messaging Server 运行时配置”。

注 步骤 1 到 8 的替代方法是从现有 Messaging Server 或 Directory Server 中复制以下文件：cert7.db、 key3.db、 secmod.db 和 sslpassword.conf。这些服务器必须具有服务器证书和适合于已经安装的同一个域的密钥。

4. 编辑 ImapProxyAService.cfg 文件并取消相关的 SSL 设置的注释。
5. 如果需要 SSL 和 POP，请编辑 PopProxyAService.cfg 文件并取消相关的 SSL 设置的注释。

   此外，您还必须编辑 AService.cfg 文件并在 ServiceList 设置中的 110 之后添加 |995。
6. 确保在 ImapProxyAService.cfg 和 PopProxyAService.cfg 文件中设置了 BindDN 和 BindPass 选项。

   您还应当将 DefaultDomain 选项设置为您的默认域 （用于非限定用户名的域）。

如果只需要服务器端的 SSL 支持，则到此就可以完成了。使用 *msg_svr_base*/sbin 目录中的以下命令启动 MMP：

```
start-msg mmp
```

如果希望基于客户机证书进行登录，请执行以下操作：

1. 获取一个客户机证书副本和签署它的 CA 证书。
2. 与以前一样启动 Sun ONE Console （在与 MMP 所在计算机相同的计算机上启动），但是这次导入 CA 证书作为信任的证书授权机构。
3. 使用在安装 Messaging Server 过程中创建的存储管理员。

   有关详细信息，请参见 第 497 页的 “指定管理员对存储的访问权限”。
4. 为 MMP 创建一个 certmap.conf 文件。例如：

   ```
   certmap default  default
   default:DNComps
   default:FilterComps  e=mail
   ```

   这意味着要通过查看 LDAP 服务器中的邮件属性并使用证书 DN 中的 e 字段来搜索一个匹配。

5. 编辑您的 ImapProxyAService.cfg 文件并执行以下操作：

   a. 将 CertMapFile 设置为 certmap.conf

   b. 将 StoreAdmin 和 StorePass 设置为步骤 3 中的值。

   c. 将 UserGroupDN 设置为您的用户和组树的根。

6. 如果需要使用 POP3 的客户机证书，请对 PopProxyAService.cfg 文件重复步骤 5。

7. 如果 MMP 尚未运行，请使用 *msg_svr_base*/sbin 目录中的以下命令来启动 MMP：

   ```
   start-msg mmp
   ```

8. 将客户机证书导入到您的客户机中。在 Netscape™ Communicator 中，单击挂锁 （安全性）图标，选择 “证书”下的 “您的”，然后选择 “导入证书 ...”并按照说明操作。

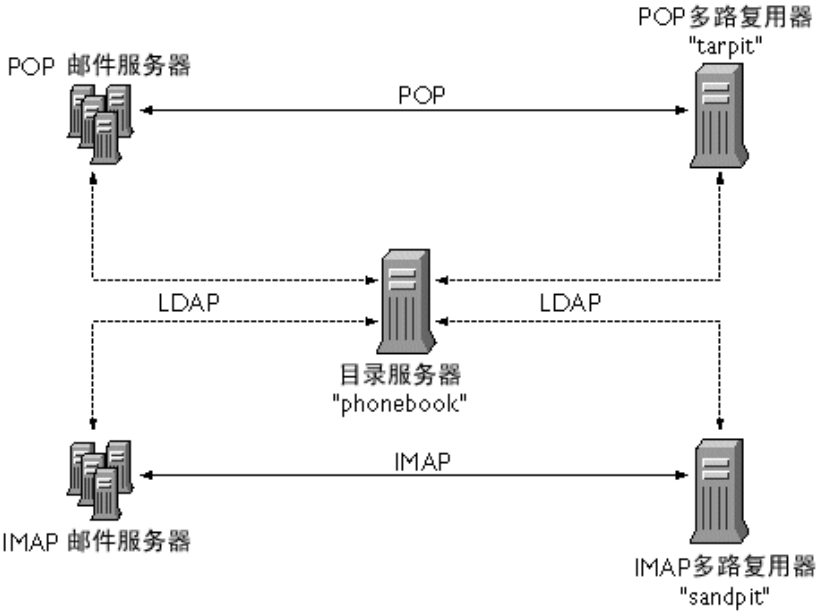
注 如果您要在所有地方都使用客户机证书，则您的所有用户都必须执行此步骤。

样例拓扑

虚构的 Siroe Corporation 分别在两台计算机上具有两个 Messaging Multiplexor，每个都支持若干 Messaging Server。 POP 和 IMAP 用户邮箱被分散在多台 Messaging Server 计算机上，其中每台服务器都专用于 POP 或专用于 IMAP （您可以通过从 ServiceList 设置中删除 ImapProxyAService 条目以单独限制客户机对 POP 服务的访问；类似地，您也可以通过从 ServiceList 设置中删除 PopProxyAService 条目以单独限制客户机对 IMAP 服务的访问。）。此外，每个 Messaging Multiplexor 仅支持 POP 或仅支持 IMAP。 LDAP 目录服务位于单独的专用计算机上。

下面的图 7-2 显示了此拓扑。

图 7-2 多个 MMP 支持多个 Messaging Server



IMAP 配置示例

图 7-2 中的 IMAP Messaging Multiplexor 安装在 `sandpit` 上，这是一台有两个处理器的计算机。此 Messaging Multiplexor 将侦听用于 IMAP 连接的标准端口 (143)。Messaging Multiplexor 与主机 `phonebook` 上的 LDAP 服务器通信以获取用户邮箱信息，然后将连接路由到适当的 IMAP 服务器。它覆盖了 IMAP 功能字符串，提供了一个虚拟域文件，并且支持 SSL 通信。

以下是它的 ImapProxyAService.cfg 配置文件：

```
default:LdapUrl             ldap://phonebook.siroe.com/o=internet
default:LogDir              /opt/SUNWmsgsr/config/log
default:LogLevel            5
default:BindDN              "cn=Directory Manager"
default:BindPass            secret
default:BacksidePort        143
default:Timeout             1800
default:Capability          "IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS CHILDREN
BINARY LANGUAGE XSENDER X-NETSCAPE XSERVERINFO"
default:SearchFormat        (uid=%s)
default:SSLEnable           yes
default:SSLPorts            993
default:SSLSecmodFile       /opt/SUNWmsgsr/config/secmod.db
default:SSLCertFile         /opt/SUNWmsgsr/config/cert7.db
default:SSLKeyFile          /opt/SUNWmsgsr/config/key3.db
default:SSLKeyPasswdFile    ""
default:SSLCipherSpecs      all
default:SSLCertNicknames    Siroe.com Server-Cert
default:SSLCacheDir         /opt/SUNWmsgsr/config
default:SSLBacksidePort     993
default:VirtualDomainFile   /opt/SUNWmsgsr/config/vdmap.cfg
default:VirtualDomainDelim  @
default:ServerDownAlert     "your IMAP server appears to be temporarily out of service"
default:MailHostAttrs       mailHost
default:PreAuth             no
default:CRAMs               no
default:AuthCacheSize       10000
default:AuthCacheTTL        900
default:AuthService         no
default:AuthServiceTTL      0
default:BGMax               10000
default:BGPenalty           2
default:BGMaxBadness        60
default:BGDecay             900
default:BGLinear            no
default:BGExcluded          /opt/SUNWmsgsr/config/bgexcl.cfg
default:ConnLimits          0.0.0.0|0.0.0.0:20
default:LdapCacheSize       10000
default:LdapCacheTTL        900
default:HostedDomains       yes
default:DefaultDomain       Siroe.com
```

POP 配置示例

图 7-2 中的 POP Messaging Multiplexor 示例安装在 tarpit 上，这是一台具有四个处理器的计算机。此 Messaging Multiplexor 将侦听用于 POP 连接的标准端口 (110)。Messaging Multiplexor 与主机 phonebook 上的 LDAP 服务器通信以获取用户邮箱信息，然后将连接路由到适当的 POP 服务器。它还提供了一个欺骗邮件文件。

以下是它的 PopProxyAService.cfg 配置文件：

```
default:LdapUrl             ldap://phonebook.siroe.com/o=internet
default:LogDir              /opt/SUNWmsgsr/config/log
default:LogLevel            5
default:BindDN              "cn=Directory Manager"
default:BindPass            password
default:BacksidePort        110
default:Timeout             1800
default:SearchFormat        (uid=%s)
default:SSLEnable           no
default:VirtualDomainFile   /opt/SUNWmsgsr/config/vdmap.cfg
default:VirtualDomainDelim  @
default:MailHostAttrs       mailHost
default:PreAuth             no
default:CRAMs               no
default:AuthCacheSize       10000
default:AuthCacheTTL        900
default:AuthService         no
default:AuthServiceTTL      0
default:BGMax               10000
default:BGPenalty           2
default:BGMaxBadness        60
default:BGDecay             900
default:BGLinear            no
default:BGExcluded          /opt/SUNWmsgsr/config/bgexcl.cfg
default:ConnLimits          0.0.0.0|0.0.0.0:20
default:LdapCacheSize       10000
default:LdapCacheTTL        900
default:HostedDomains       yes
default:DefaultDomain       Siroe.com
```

MMP 任务

本节说明其他的 MMP 配置任务。这些元字符包含：

- 第 159 页的 “用 MMP 配置邮件访问”
- 第 159 页的 “设置故障转移 MMP LDAP 服务器”

用 MMP 配置邮件访问

因为 MMP 无法自动配置，所以必须进行明确配置。此外， MMP 不使用 `PORT_ACCESS` 映射表。如果希望拒绝来自某些 IP 地址的 SMTP 连接并且正在使用 MMP，则必须使用 `TCPAccess` 选项。该选项的语法与 `mailDomainAllowedServiceAccess` 相同 （请参见位于 `http://docs.sun.com/doc/819-0113` 的 Sun Java System Communcations Services Schema Reference Manual）。该语法也说明在第 592 页的 “过滤器语法”中。

设置故障转移 MMP LDAP 服务器

可以为 MMP 指定多个 LDAP 服务器，以便当一个服务器出现故障时可以使用另一个。请按以下所示修改您的 `PopProxyAservice.cfg` 或 `IMAPProxyAservice.cfg`：

```
default:LdapUrl "ldap://ldap01.yourdomain ldap02.yourdomain/o=INTERNET"
```

关于 Messenger Express Multiplexor

Sun Java System Messenger Express Multiplexor 是一个专用服务器，用作与 HTTP 访问服务的单点连接。 Messenger Express 是 Sun Java System Messaging Server HTTP 服务的客户机接口。所有用户都连接到一个单一的邮件传送代理服务器，该服务器会将用户定向到适当的邮箱。结果，整个邮件传送服务器阵列将作为一个单一的主机呈现给您的邮件用户。

Messagile Messaging Multiplexor (MMP) 连接到 POP 和 IMAP 服务器，而 Messenger Express Multiplexor 则连接到 HTTP 服务器。也就是说， Messenger Express Multiplexor 用于 Messenger Express，而 MMP 则用于 POP 和 IMAP。

与 MMP 类似， Messenger Express Multiplexor 也支持：

- 与邮件客户机进行未加密和加密的 (SSL) 通信

  有关配置 SSL 的更多信息，请参见第 19 章 “配置安全和访问控制”中的 “安全性和访问控制”。

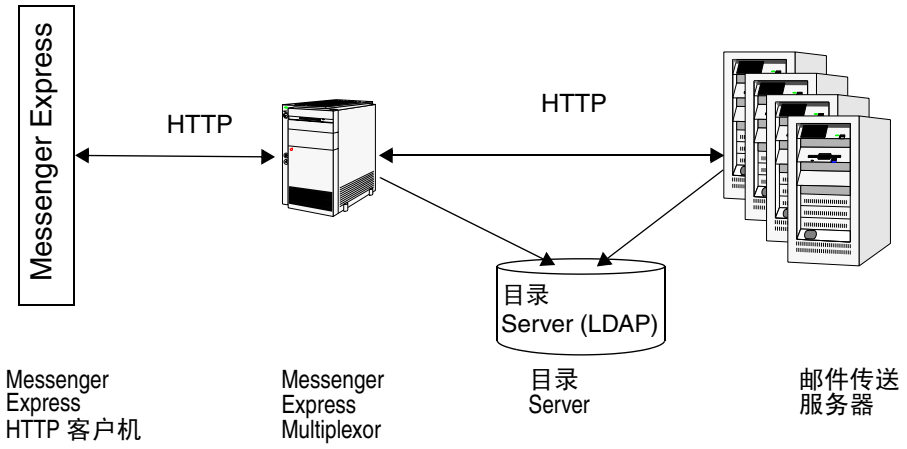
- 托管域

与 MMP 不同的是， Messenger Express Multiplexor 内置于 `mshttpd` 服务中，因此使用了相同的日志记录和配置机制。

Messenger Express Multiplexor 的工作原理

Messenger Express Multiplexor 由作为多路复用器的代理邮件传送服务器构成，它允许您连接到 Messaging Server (Messenger Express) 的 HTTP 服务。 Messenger Express Multiplexor 可以协助在多台服务器计算机上分布邮箱。客户机在登录到 Messenger Express 时将连接到多路复用器， Messenger Express 将为用户确定正确的服务器，然后连接到该服务器并在客户机和服务器之间传递数据。此功能使大型安装可以将邮件存储分散在多台计算机上 （以增加容量），同时向用户和外部客户机呈现了一个单一的邮件主机 （针对用户可以提高效率，针对外部客户机可以提高安全性）。图 7-3 第 160 页 说明了 Messenger Express Multiplexor 在 Messaging Server 安装中驻留的位置。

图 7-3 概述 iPlanet Messenger Express Multiplexor



Messenger Express Multiplexor 在 Messenger Express 客户机和 Messaging Server 之间提供了一个接口，即，接受连接并将它们适当地路由。与其他邮件服务器安装中的典型情况一样，每个用户都被指定一个位于特定邮件传送服务器上的特定地址和邮箱。但是，所有 HTTP 连接都是通过 Messenger Express Multiplexor 路由的。

下面详细介绍了建立用户连接中所涉及的步骤：

1. 用户的客户机连接到 Messenger Express Multiplexor，后者将接受初步验证信息。
2. Messenger Express Multiplexor 将查询 Directory Server 以确定包含用户的邮箱的邮件传送服务器。
3. Messenger Express Multiplexor 连接到相关联的 Messaging Server，重新进行验证，然后在会话过程中充当通信管道。

设置 Messenger Express Multiplexor

本节将介绍设置和配置 Messenger Express Multiplexor 所应遵循的步骤。其中包含以下主题：

- 第 161 页的 “在代理计算机上安装 Messaging Server”
- 第 162 页的 “配置 Messenger Express Multiplexor 参数”
- 第 163 页的 “启用 Messenger Express Multiplexor”

在代理计算机上安装 Messaging Server

第一步是在代理计算机上安装 Messaging Server，该代理计算机将成为 Messenger Express Multiplexor。有关具体的安装说明，请参见 Sun Java Enterprise System 安装指南。

确保将 Messaging Server 配置给指向后端邮件传送服务器的用户和组的目录服务器。此目录服务器将用于通过 Messenger Express Multiplexor 为 Messaging Server 验证用户。

配置 Messenger Express Multiplexor 参数

在代理计算机上完成 Messaging Server 的安装后，请配置 Messenger Express Multiplexor 参数：

1. 收集所需的后端 Messaging Server 信息。

   运行后端邮件传送服务器的目录中的 `configutil` 命令以确定参数的值，本节稍后将介绍这些参数。代理计算机 （将在其上启用多路复用器）的配置必须与后端邮件传送服务器相匹配以确保设置成功。

2. 为 Messenger Express Multiplexor 设置配置参数。

   运行代理计算机邮件传送服务器的 *msg_svr_base*`/sbin/configutil` 目录中的 `configutil` 命令以设置配置值。请注意，这些值应当与后端邮件传送服务器的值相匹配。

以下各节介绍了设置 Messenger Express Multiplexor 所需的 `configutil` 参数：

- 第 162 页的 “LDAP 参数”
- 第 162 页的 “dcroot”
- 第 163 页的 “默认域”
- 第 163 页的 “登录分隔符”

LDAP 参数

您需要确保在启用 Messenger Express Multiplexor 之前正确指定 Directory Server 的参数。要确定您的 LDAP 参数，请运行相应后端 Messaging Server 实例目录中的以下命令：

- `configutil -o local.ugldaphost`

  此参数显示后端邮件传送服务器使用的用户和组 LDAP Directory Server。确保将 `ldaphost` 设置为与后端邮件传送服务器使用的值相同的值 （或是包含相同数据的复制的 LDAP 服务器）。

- ```
  configutil -o local.ugldapbinddn
  configutil -o local.ugldapbindcred
  ```

  这些参数显示用户和组 Directory Server 的 DN 和密码。`ldapbinddn` 和 `ldapbindcred` 必须与在后端邮件传送服务器中指定的值相同。

dcroot

您需要确保正确指定 *dcroot*。要确定您的 *dcroot*，请运行相应邮件传送服务器实例目录中的以下命令：

```
configutil -o service.dcroot
```
```

默认域

您需要确保正确指定邮件传送服务器的默认域 (*defaultdomain*)。要确定您的邮件传送服务器默认域，请运行相应邮件传送服务器实例目录中的以下 configutil 命令：

```
configutil -o service.defaultdomain
```

登录分隔符

确保登录分隔符 (*loginseparator*) 与后端邮件传送服务器使用的登录分隔符一致。要确定您的邮件传送服务器登录分隔符，请运行相应后端邮件传送服务器实例目录中的 configutil 命令：

```
configutil -o service.loginseparator
```

启用 Messenger Express Multiplexor

设置配置参数后，您便可以在代理计算机上启用 Messenger Express Multiplexor。要执行此操作，请运行代理计算机上的邮件传送服务器实例的目录 *msg_svr_base*/sbin/configutil 中的以下 configutil 命令：

```
configutil -o local.service.http.proxy -v 1
```

其中，1 将启用 Messenger Express Multiplexor （默认值为 0）。

当非本地用户 （其邮件主机不在其登录的服务器上的用户）登录且 local.service.http.proxy 的值为 0 时，该用户将被定向到其主机，并且该用户将看到主机名的更改；因此，该多路复用器没有被启用。

如果将 local.service.http.proxy 的值设置为 1，将启用多路复用器，并且主机名不会更改，同时邮件传送服务器的整个阵列将作为一个单一的主机呈现给您的非本地邮件用户。

对于本地用户 （其邮件主机是其登录的服务器的用户），服务器将使用本地邮件存储，而不管 local.service.http.proxy 参数值如何。代理用户和本地用户可以在同一个邮件传送服务器上共存。

测试您的设置

在本节中，您将了解如何测试您的 Messenger Express Multiplexor 设置以及如何在日志文件中查找消息。假定您已经配置和启用了 Messenger Express Multiplexor。

访问 Messenger Express 客户机

在测试您的安装之前，您应当已经熟悉 Messenger Express 产品。此外，您还应当具有一个以前创建的测试帐户。

要测试您的 Messenger Express Multiplexor 代理，请执行以下步骤：

1. 通过 Messenger Express Multiplexor，在浏览器位置中键入以下浏览器位置以连接到 Messenger Express：

   `http://`*`msgserver_name`*。

   例如：

   `http://budgie.sesta.com`

2. 使用以前创建的测试帐户，登录到 Messenger Express。
3. 您应当能够成功登录并从后端邮件传送服务器访问邮件。
4. 如果在您通过 Messenger Express 登录后邮件传送服务器名称发生了变化，请确保将 `local.service.http.proxy` 设置为 `1` 并重新启动邮件传送代理服务器。Messenger Express Multiplexor 应当为您的用户呈现一个单一的邮件主机。

错误消息

如果在输入用户 ID、密码以及单击 “连接”时收到错误消息，应当查看代理计算机的 HTTP 日志文件。要查看错误消息，请转到 *msg_svr_base*`/log` 目录。在大多数情况下，错误消息将包含用于诊断问题的足够信息。在这些实例中，如果没有足够的信息来诊断问题，请与用户支持联系。

管理 Messenger Express Multiplexor

本节介绍 Messenger Express Multiplexor 的基本管理功能。

配置和管理 SSL

要为您的 Messenger Express Multiplexor 配置和管理 SSL （也称为安全套接字层），请参见第 584 页的 “启用 SSL 并选择加密算法的步骤”。

设置多个代理服务器

要设置由一个名称表示的多个 Messenger Express Multiplexor，您可以使用一个能够识别会话的负载平衡设备。使用此设备，可以将所有请求从任何给定的客户机路由到一个唯一的服务器。

管理 Messaging Server 和 Messenger Express Multiplexor 的不同版本

如果为 Messenger Express Multiplexor 和后端邮件主机使用不同版本的 Messaging Server，则需要更新 Messenger Express 静态文件以确保服务器之间的兼容性。

构成 Messenger Express 接口的静态文件是直接从 Messenger Express Multiplexor 提供的，而不是从用户的邮件主机提供的。多路复用器将在 *msg_svr_base*/config/html 目录中查找这些文件。

要更新这些文件以确保服务器之间的兼容性，请用较早版本的 Messaging Server 中的 *msg_svr_base*/config/html 目录的整个内容替换较新版本的 Messaging Server 中的相同目录的整个内容 （其中包含构成 Messenger Express 接口的这些静态文件）。

例如，如果后端邮件传送服务器使用 Messaging Server 6 2003Q4 而您安装了 Messaging Server 6 2005Q1 作为 Messenger Express Multiplexor，则需要将 Messenger Express Multiplexor 的 *msg_svr_base*/config/html 目录的整个内容替换为 Messaging Server 6 2003Q4 后端服务器中相同目录的内容。当最终将 Messaging Server 6 2003Q4 升级到 Messaging Server 6 2005Q1 时，您也可以为 Messenger Express Multiplexor 服务器更新 *msg_svr_base*/config/html 目录中的这些静态文件。

使用 Messenger Express Multiplexor 配置后端邮件传送服务器的端口

如果要使用 Messenger Express Multiplexor 配置后端 HTTP Messaging Server 的端口，请在多路复用器计算机上使用以下 configutil 命令：

local.service.http.proxy.port. **主机名**

其中， *hostname* 是后端 HTTP Messaging Server 的主机。

例如，如果后端邮件传送服务器的主机名为 sesta.com，端口号为 8888，则该命令的格式如下：

```
configutil -o local.service.http.proxy.port.store.sesta.com -v 8888
```

local.service.proxy.port 适用于除拥有自己端口的邮件存储外所有的后端邮件存储（与 local.service.proxy.admin 相同）。

配置单点登录

单点登录必须在 Messenger Express Multiplexor 计算机上按照与邮件传送 (HTTP) 服务器相同的方式进行配置，并且具有以下附加配置：

```
configutil -o local.service.http.proxy.admin -v store_administrator
```

其中， *store_administrator* 是在后端 Messaging Server 安装过程中指定的后端存储管理员。

```
configutil -o local.service.http.proxy.adminpass -v store_admin_password
```

其中， *store_admin_password* 是在后端 Messaging Server 安装过程中指定的后端存储管理员密码。

如果要使用多个后端 Messaging Server （这些服务器使用不同的存储管理员和密码），则可以通过向 Messenger Express Multiplexor 中的每个配置变量附加全限定的主机名来分别配置它们：

```
configutil -o local.service.http.proxy.admin.hostname -v store_administrator
```

```
configutil -o local.service.http.proxy.adminpass.hostname -v
store_admin_password
```

其中， *hostname* 是后端 HTTP Messaging Server 的主机， *store_administrator* 和 *store_admin_password* 是在后端 Messaging Server 安装过程中指定的后端存储管理员和密码。

要将用户登录到后端服务器上， Messenger Express Multiplexor 将使用 `proxyauth` 登录命令。要启用 `proxyauth`，请使用后端邮件存储中的 `configutil` 参数：

```
configutil -o service.http.allowadminproxy -v 1
```

注 如果通过 Messenger Express Multiplexor 启用了单点登录，则不需要在后端 HTTP Messaging Server 上配置它。

要使用 Identity Server 配置 Messenger Express Multiplexor SSO，请启用以下 `configutil` 参数：

```
./configutil -o local.webmail.sso.amcookiename -v iPlanetDirectoryPro
```

```
./configutil -o local.webmail.sso.amnamingurl -v \
        http://identity host:identity port/amserver/namingservice
```

第 8 章

MTA 概念

本章提供了 MTA 的概念性说明。其中包含以下各节：

- 第 167 页的 “MTA 功能”
- 第 171 页的 “MTA 体系结构和邮件流概述”
- 第 172 页的 “分发程序”
- 第 174 页的 “重写规则”
- 第 175 页的 “通道”
- 第 179 页的 “MTA 目录信息”
- 第 179 页的 “作业控制器”

MTA 功能

邮件传输代理 （即 MTA）是 Messaging Server 的组件 （第 169 页的图 8-1 ）。在最基础的级别上， MTA 是邮件路由器。 MTA 从其他服务器接受邮件、读取地址并将其路由到通往最终目的地 （通常是用户邮箱）的过程中的下一个服务器。

这些年来， MTA 已增加了许多功能，其大小、功能和复杂性都有所增加。这些 MTA 功能有重叠，但一般情况下，可以分为以下几类：

- **路由**。接受邮件，在必要 （例如邮件为别名）时扩展或变换邮件，并将邮件路由到下一个服务器、通道、程序、文件或其他位置。路由功能已被扩展为允许管理员指定如何路由邮件的内部和外部结构。例如，可以指定 SMTP 验证之类的功能、使用各种 SMTP 命令和协议、 TCP/IP 或 DNS 查找支持、作业提交、进程控制和邮件排队等等。
- **地址重写**。作为路由进程的一部分，信封地址经常被重写，但是信封或标题地址也可被重写为更想要的或更合适的格式。

- **过滤**。MTA 可以基于地址、域、可能的病毒或垃圾邮件内容、大小、IP 地址、标题内容等过滤邮件。在发送至用户邮箱的过程中，可以放弃、拒绝或修改过滤的邮件，或将其发送给某个文件、程序或下一个服务器。
- **内容修改**。可以修改邮件标题或内容。示例：使邮件对于特定客户机或在特定字符集中可读，或检查垃圾邮件或病毒。
- **审计**。跟踪提交者、提交的内容、地点和时间。

第 170 页的图 8-2 中显示了若干支持这些功能的子组件和进程。本章介绍了这些子组件和进程。此外，还介绍了若干允许系统管理员启用和配置这些功能的工具。这些工具包括 MTA 选项、`configutil` 参数、映射表、关键字、通道和重写规则。将在后面的 MTA 章节中进行介绍：

- 第 9 章 “MTA 地址转换和路由”
- 第 10 章 “关于 MTA 服务和配置”
- 第 11 章 “配置重写规则”
- 第 12 章 “配置通道定义”
- 第 13 章 “使用预定义通道”
- 第 14 章 “将垃圾邮件和病毒过滤程序集成至 Messaging Server”
- 第 15 章 “LMTP 传送”
- 第 16 章 “休假自动邮件回复”
- 第 17 章 “邮件过滤和访问控制”
- 第 19 章 “配置安全和访问控制”
- 第 21 章 “管理日志记录”
- 第 22 章 “MTA 故障排除”
- 第 23 章 “监视 Messaging Server”

图 8-1 Messaging Server，简化的组件视图 （未显示 Messenger Express）

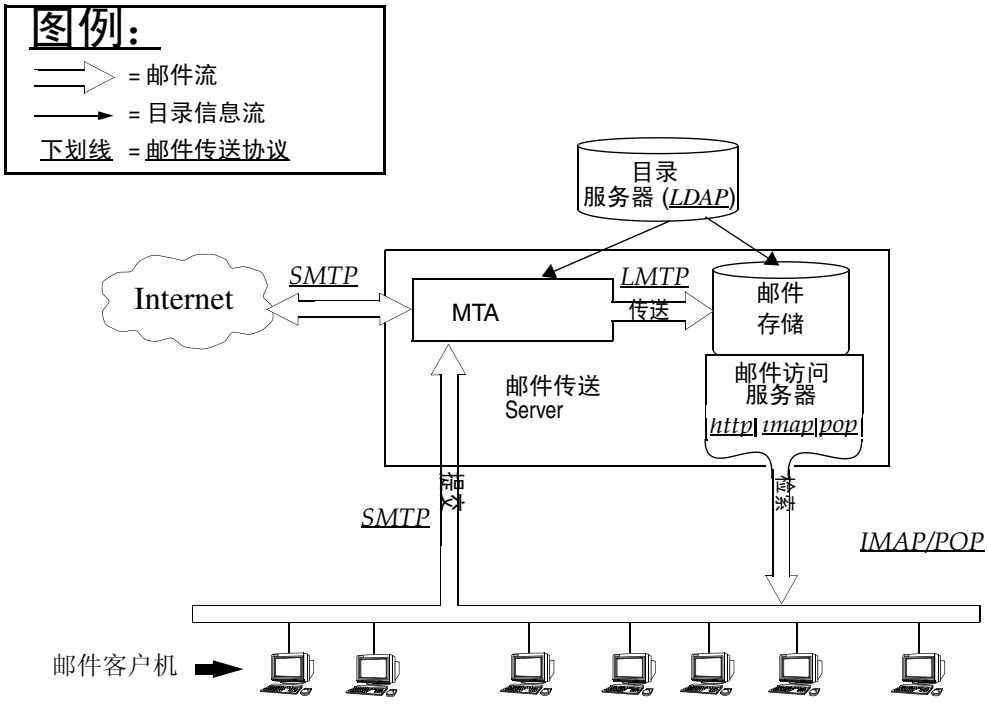
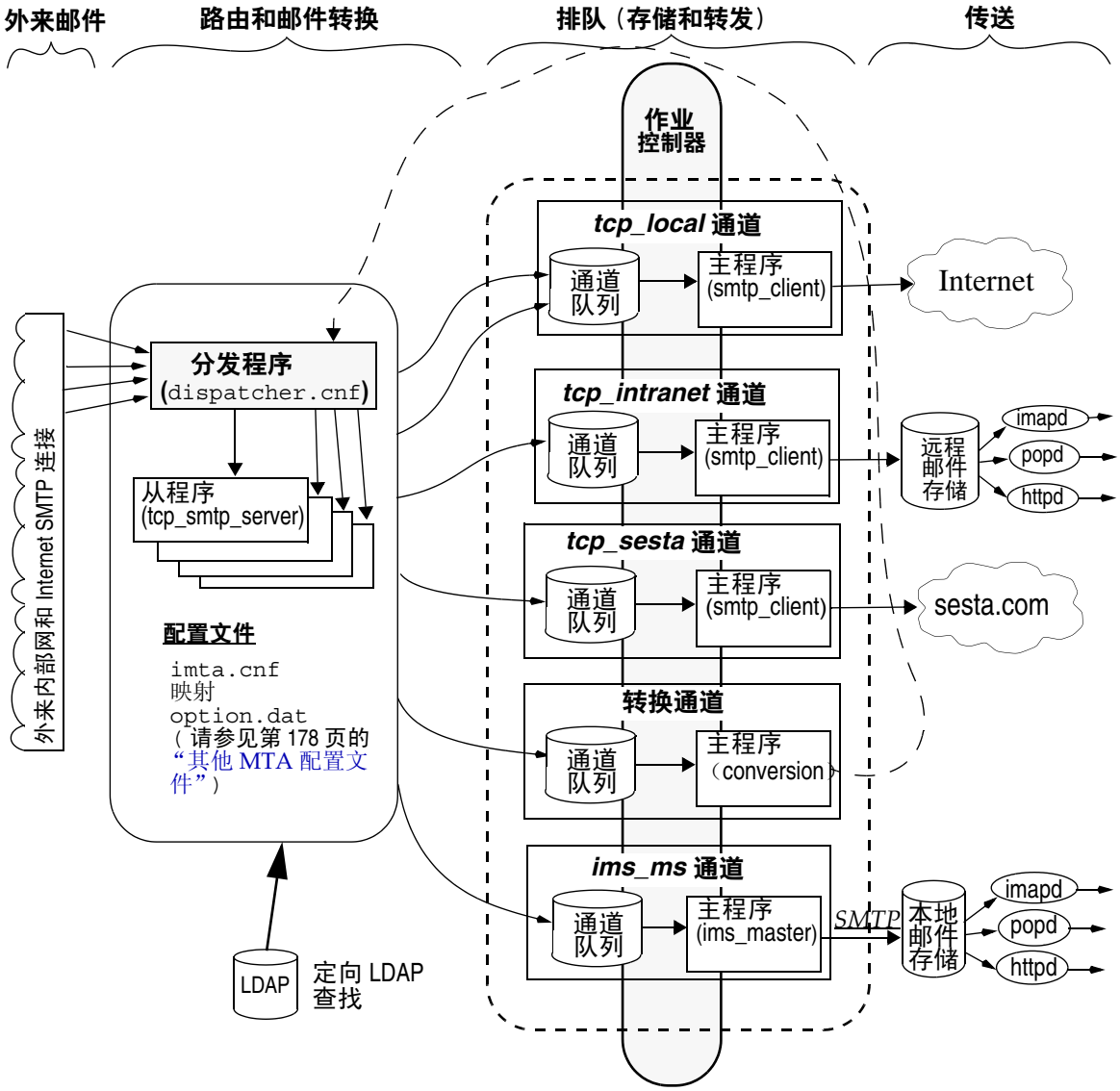


图 8-2 MTA 体系结构


外来邮件
路由和邮件转换
排队（存储和转发）
传送
作业
控制器
tcp_local 通道
通道
队列
主程序
(smtp_client)
Internet
tcp_intranet 通道
通道
队列
主程序
(smtp_client)
远程
邮件
存储
imapd
popd
httpd
tcp_sesta 通道
通道
队列
主程序
(smtp_client)
sesta.com
转换通道
通道
队列
主程序
（conversion）
ims_ms 通道
通道
队列
主程序
(ims_master)
SMTP
本地
邮件
存储
imapd
popd
httpd
外来内部网和 Internet SMTP 连接
分发程序
(dispatcher.cnf)
从程序
(tcp_smtp_server)
配置文件
imta.cnf
映射
option.dat
（请参见第 178 页的
“其他 MTA 配置文
件”）
LDAP
定向 LDAP
查找

MTA 体系结构和邮件流概述

本节简要概述了 MTA 体系结构和邮件流 （图 8-2）。请注意， MTA 是一个非常复杂的组件，而图 8-2 只是流经该系统的邮件的**简要**说明。事实上，此图并不是所有流经该系统的邮件的非常准确的说明。但对于概念性的讨论，这已经足够了。

分发程序和 *SMTP* 服务器 （从程序）

邮件通过 SMTP 会话从 Internet 或内部网进入 MTA。当 MTA 收到要求进行 SMTP 连接的请求时， MTA **分发程序** （多线程连接分发代理）将执行一个**从**程序 (`tcp_smtp_server`) 以处理 SMTP 会话。分发程序将为每个服务维护多线程进程池。请求其他会话时，分发程序将激活一个 SMTP 服务器程序以处理每个会话。分发程序的进程池中的进程可能会同时处理许多连接。分发程序和从程序将一起对每个外来邮件执行许多不同的功能。其中三个主要功能是：

- 邮件阻止 — 可能阻止来自指定的 IP 地址、邮件地址、端口、通道、标题字符串等的邮件 （第 17 章 “邮件过滤和访问控制”）。
- 地址更改。外来 `From:` 地址或 `To:` 地址可能会被重写为其他格式。
- 通道排队。通过重写规则运行地址以确定应将邮件发送到哪个通道。

有关详细信息，请参见第 172 页的 “分发程序”

路由和地址重写

SMTP 服务器和许多其他通道 （包括转换通道和再处理通道）均可将邮件加入队列。虽然此阶段传送期间完成了许多任务，但此阶段传送期间的主要任务是：

- 别名扩展。
- 通过重写规则运行地址以确定应将邮件排入哪个通道以及将地址的域部分重写为正确的或所需的格式。
- 通道关键字处理。
- 向适当的通道队列发送邮件。

通道

通道是用于邮件处理的基本 MTA 组件。通道表示邮件与另一个系统的连接 （例如，另一个 MTA、另一个通道或本地邮件存储）。邮件进入时，根据邮件的源和目的地，不同的邮件需要不同的路由和处理。例如，要传送到本地邮件存储的邮件与要传送到 Internet 的邮件以及要发送到邮件系统内的另一个 MTA 的邮件，将以不同的方式进行处理。通道提供了用于自定义每个连接所需的处理和路由的机制。在默认安装中，大多数邮件转至处理 Internet、内部网和本地邮件的通道。

也可以创建用于特定情况的专门通道。例如，假设某个 Internet 域处理邮件非常缓慢，导致发到此域的邮件阻塞了 MTA。便可以创建一个专门的通道对发到该慢速域的邮件提供特殊处理，从而消除此域中系统的障碍。

地址的域部分将确定邮件要排入哪个通道。用于读取域和确定适当的通道的机制称为重写规则 （请参见第 174 页的 “重写规则”）。

通道通常由一个通道队列和一个通道处理程序 （称为**主程序**）组成。从程序将邮件传送到适当的通道队列后，主程序将执行所需的处理和路由。通道和重写规则一样是在 `imta.cnf` 文件中指定和配置的。以下所示为一个通道条目的示例：

```
tcp_intranet smtp mx single_sys subdirs 20 noreverse maxjobs 7 SMTP_POOL
maytlsserver allowswitchchannel  saslswitchchannel tcp_auth
tcp_intranet-daemon
```

此例中的第一个字 `tcp_intranet` 是通道名称。最后一个字称为通道标记。中间的字称为通道关键字，它们指定了将如何处理邮件。许多不同的关键字允许用许多方式处理邮件。在 Sun Java System Messaging Server Administration Reference 和第 12 章 “配置通道定义”中提供了通道关键字的完整说明。

邮件传送

邮件经过处理后，主程序将邮件沿着邮件的传送路径发送到下一个停靠站。这可能是预期收件人的邮箱、另一个 MTA，甚至也可能是其他通道。虽然图中未显示，但转发到另一个通道的情况经常发生。

请注意，地址的本地部分和接收的字段通常是 7 位字符。如果 MTA 在这些字段中读到 8 位字符，它将把每个 8 位字符替换成星号。

分发程序

分发程序是一个多线程的分发代理，允许多个多线程服务器进程共同分担 SMTP 连接服务。使用分发程序时，可以同时运行若干个多线程 SMTP 服务器进程，并且所有处理均与同一个端口连接。此外，每个服务器可能会有一个或多个活动连接。

分发程序充当在其配置中列出的 TCP 端口的中心接收程序。对于每个已定义的服务，分发程序可能会创建一个或多个 SMTP 服务器进程，在建立了连接之后处理这些连接。

通常，当分发程序接收到已定义的 TCP 端口的连接时，将为该端口上的服务检查可用的工作进程池并为新的连接选择最佳候选池。如果没有合适的候选池，则在配置允许的情况下，分发程序可能会创建一个新的工作进程以处理此连接和以后的连接。分发程序也可能会为预期的将来外来连接创建新的工作进程。有若干配置选项可用于调整各种服务中分发程序的控制，特别是控制工作进程的数量以及每个工作进程所处理的连接的数量。

有关更多信息，请参见第 222 页的 “分发程序配置文件”。

服务器进程的创建和终止

分发程序内的自动内务处理功能控制着新服务器进程的创建和旧的或闲置的服务器进程的终止。控制分发程序性能的基本选项是 MIN_PROCS 和 MAX_PROCS。MIN_PROCS 通过准备就绪若干服务器进程并等待外来连接，提供了一种服务保证级别。另一方面，MAX_PROCS 设置了对于给定服务可以同时活动的服务器进程数量的上限。

当前运行的服务器进程可能不能接收任何连接，因为它处理的连接已经达到其所能处理的最大数量，或者此进程已被安排终止。分发程序可能会创建其他进程以帮助将来的连接。

MIN_CONNS 和 MAX_CONNS 选项提供了一种帮助您在服务器进程之间分发连接的机制。MIN_CONNS 指定了将服务器进程标记为 “足够忙” 的连接的数量，而 MAX_CONNS 指定了服务器进程达到 “最忙” 时连接的数量。

通常，当前服务器进程数量少于 MIN_PROCS 或所有现有服务器进程均为 “足够忙”（每个进程具有的当前活动连接数量至少为 MIN_CONNS）时，分发程序将创建一个新的服务器进程。

如果服务器进程意外中止 （例如，通过 UNIX 系统的 kill 命令），则分发程序仍将在新连接进入时创建新的服务器进程。

有关配置分发程序的信息，请参见第 222 页的 “分发程序配置文件”。

启动和停止分发程序

要启动分发程序，请执行以下命令：

```
start-msg dispatcher
```

此命令将包括并废弃以前用于启动 MTA 组件 （已经配置了分发程序以进行管理）的任何其他 start-msg 命令。特别是，不应再使用 imsimta start smtp 命令。尝试执行任何已废弃的命令将导致 MTA 发出警告。

要关闭分发程序，请执行以下命令：

```
stop-msg dispatcher
```

关闭分发程序时，服务器进程发生的情况取决于基本的 TCP/IP 软件包。如果修改了用于分发程序的 MTA 配置或选项，则必须重新启动分发程序以便使新配置或选项生效。

要重新启动分发程序，请执行以下命令：

```
imsimta restart dispatcher
```

重新启动分发程序与关闭当前运行的分发程序再立即启动新的分发程序具有同样的效果。

重写规则

重写规则可以确定以下问题：

- 如何将地址的域部分重写为正确的或所需的格式。
- 重写地址后应将邮件排入哪个通道。

每个重写规则均由一个**模式**和一个**模板**组成。模式是与地址的域部分匹配的字符串。模板指定了域部分与模式匹配时采取的操作。它由以下两部分组成：1) 一组指定应如何重写地址的说明 （即，一个由控制字符组成的字符串）和 2) 邮件将发送到的通道的名称。重写地址后，邮件将排入目标通道，以传送到预期收件人。

以下所示为一个重写规则的示例：

```
siroe.com           $U%$D@tcp_siroe-daemon
```

`siroe.com` 是域模式。地址包含 `siroe.com` 的任何邮件将按照模板说明 (`$U%$D`) 被重写。 `$U` 指定重写的地址使用相同的用户名。 % 指定重写的地址使用相同的域分隔符。 `$D` 指定重写的地址使用在模式中匹配的相同的域名。 `@tcp_siroe-daemon` 指定将带有重写地址的邮件发送至名为 `tcp_siroe-daemon` 的通道。有关详细信息，请参见第 11 章 “配置重写规则”。

有关配置重写规则的更多信息，请参见第 206 页的 “MTA 配置文件”和第 11 章 “配置重写规则”。

通道

通道是处理邮件的基本 MTA 组件。通道表示与另一个计算机系统或系统组的连接。各个通道中实际的硬件连接或软件传输或者这两者，可能大大不同。

通道执行以下功能：

- 将邮件传输到远程系统，并在发送邮件后将其从队列中删除。
- 从远程系统接收邮件，并将其放入适当的通道队列。
- 将邮件传送到本地邮件存储。
- 将邮件传送到用于特殊处理的程序。

邮件在进入 MTA 的过程中由通道排队，离开 MTA 的过程中被取消排队。通常，邮件经由一个通道进入，然后通过另一个通道离开。通道可以将邮件取消排队、处理邮件或将邮件排入另一个 MTA 通道。

主程序和从程序

通常 （并非总是），通道与两个程序相关联：主程序和从程序。从程序从其他系统接收邮件并将其添加至通道的邮件队列中。主程序将邮件从通道传输到其他系统。

例如， SMTP 通道有一个用来传输邮件的主程序和一个用来接收邮件的从程序。分别为 SMTP 客户机和服务器。

主通道程序通常在 MTA 已启动操作的地方负责外发的连接。主通道程序：

- 响应本地的处理请求时运行。
- 使邮件从通道邮件队列中取消排队。
- 如果目的地格式不同于排入的邮件的格式，则根据需要执行地址、标题和内容的转换。
- 启动邮件的网络传输。

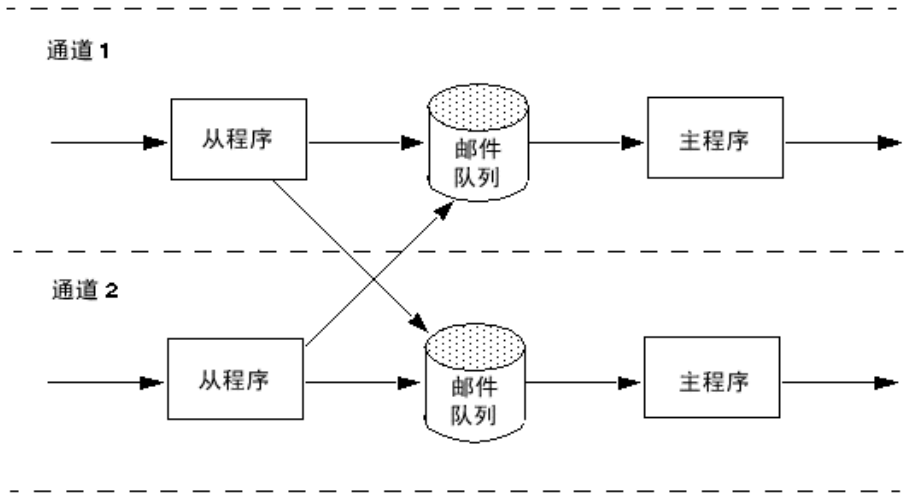
从通道程序通常在 MTA 响应外部请求的地方接受外来连接。从通道程序：

- 响应外部事件或本地请求时运行。
- 将邮件排入通道。通过重写规则传送信封地址确定目标通道。

例如，图 8-3 显示了两个通道程序 Channel 1 和 Channel 2。 Channel 1 中的从程序从远程系统接收了一封邮件。它将查看地址，根据需要应用重写规则，然后基于重写的地址将邮件排入适当的通道邮件队列。

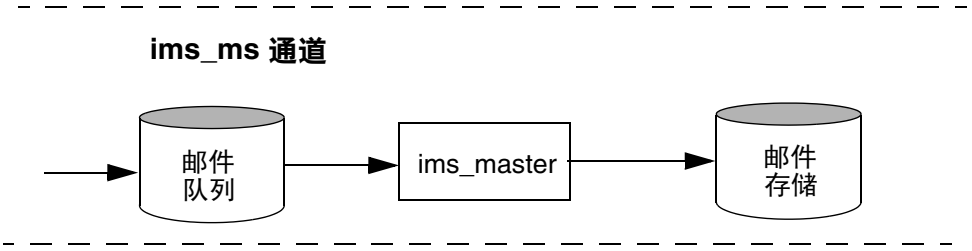
主程序从队列中将邮件取消排队并启动邮件的网络传输。请注意，主程序只能将邮件从其自己的通道队列中取消排队。

图 8-3 主程序和从程序



虽然典型通道有一个主程序和一个从程序，但也有可能一个通道仅包含一个从程序或一个主程序。例如， Messaging Server 提供的 `ims-ms` 通道仅包含一个主程序，因为此通道仅负责将邮件取消排队并退到本地邮件存储，如图 8-4 中所示。

图 8-4 ims-ms 通道



通道邮件队列

所有通道均有关联的邮件队列。邮件进入邮件传送系统时，从程序确定将此邮件排入哪个邮件队列。排入的邮件存储在通道队列目录的邮件文件中。默认情况下，这些目录存储在以下位置：*msg_svr_base*/data/queue/*channel*/*。

注意 请勿在 MTA 队列目录 （即 imta_tailor 文件中 IMTA_QUEUE 的值）中添加任何文件或目录，因为这样会出现问题。将单独的文件系统用于 MTA 队列目录时，请在该装入点下创建一个子目录并指定该子目录为 IMTA_QUEUE 的值。

通道定义

通道定义显示在 MTA 配置文件 (imta.cnf) 的下半部分，在重写规则之后 （请参见第 206 页的 “MTA 配置文件”）。显示在文件中的第一个空白行表示重写规则部分的结束和通道定义的开始。

通道定义包含通道的名称，后跟一个定义通道配置的可选关键字列表，和一个在重写规则中使用以将邮件路由到通道的唯一的通道标记。通道定义由单个空白行分隔。通道定义内可能包括注释，但没有空白行。

```
[blank line]
! sample channel definition
Channel_Name  keyword1  keyword2
Channel_Tag
[blank line]
```

总体而言，通道定义被称为通道主机表。单个通道定义称为通道块。例如，在以下示例中通道主机表包含三个通道定义（块）。

```
! test.cnf - An example configuration file.
!
! Rewrite Rules
      .
      .
      .

! BEGIN CHANNEL DEFINITIONS
! FIRST CHANNEL BLOCK
l
local-host

! SECOND CHANNEL BLOCK
a_channel defragment charset7 usascii
a-daemon

! THIRD CHANNEL BLOCK
b_channel noreverse notices 1 2 3
b-daemon
```

典型的通道条目类似如下：

```
tcp_intranet smtp mx single_sys subdirs 20 noreverse maxjobs 7 SMTP_POOL
maytlsserver allowswitchchannel  saslswitchchannel tcp_auth
tcp_intranet-daemon
```

此例中的第一个字 `tcp_intranet` 是通道名称。此例中的最后一个字 `tcp_intranet-daemon` 称为**通道标记**。通道标记是重写规则用来定向邮件的名称。通道名称和通道标记之间的字称为通道**关键字**，指定将如何处理邮件。许多不同的关键字允许用许多方式处理邮件。在 Sun Java System Messaging Server Administration Reference 和第 12 章 “配置通道定义”中列出并介绍了通道关键字的完整列表。

通道主机表定义了 Messaging Server 可以使用的通道以及与每个通道相关联的系统的名称。

在 UNIX 系统上，文件中的第一个通道块总是介绍本地通道 `l`。（例外情况是可能会在本地通道之前显示一个 `defaults` 通道。）本地通道用于决定路由和发送由 UNIX 邮件工具发送的邮件。

也可以在 MTA 选项文件 option.dat 中为通道设置全局选项，或在通道选项文件中为特定通道设置选项。有关选项文件的详细信息，请参见第 224 页的 “选项文件”和第 222 页的 “TCP/IP (SMTP) 通道选项文件”。有关配置通道的详细信息，请参见第 12 章 “配置通道定义”。有关创建 MTA 通道的详细信息，请参见第 206 页的 “MTA 配置文件”。

MTA 目录信息

对于 MTA 处理的每封邮件， MTA 均需要访问有关其支持的用户、组和域的目录信息。此信息存储在一个 LDAP 目录服务中。 MTA 直接访问 LDAP 目录。第 9 章 “MTA 地址转换和路由”中对此进行了全面说明。

作业控制器

每次将邮件排入通道时，作业控制器均确保有一个运行的作业以传送该邮件。这可能涉及启动一个新作业进程、添加一个线程或只是通知一个作业已经在运行。如果因为已达到通道或池的作业限制而不能启动作业，则作业控制器将等待直到其他作业退出。不再超出作业限制时，作业控制器将启动其他作业。

通道作业在作业控制器内的处理池中运行。可以认为池是一个运行通道作业的 “地方”。池提供了一个计算区域，一组作业可以在其中运行而不与池外的作业竞争资源。有关池的更多信息，请参见第 225 页的 “作业控制器文件”和第 322 页的 “用于通道执行作业的处理池”。

通道的作业限制由 maxjobs 通道关键字确定。池的作业限制由池的 JOB_LIMIT 选项确定。

Messaging Server 通常尝试立即传送所有邮件。如果第一次尝试不能传送邮件，则将延迟该邮件一段时间，该时间由相应的 backoff 关键字确定。一旦 backoff 关键字中指定的时间过后，就可以传送延迟的邮件，并且如果需要将启动通道作业以处理该邮件。

当前正在处理和等待处理的邮件的作业控制器的内存中数据结构，通常反映了存储在 MTA 队列区域的磁盘上的全部邮件文件。但是，如果磁盘上待处理的邮件文件累计超出了作业控制器的内存中数据结构大小的限制，则作业控制器仅在内存中跟踪磁盘上的邮件文件总数的一部分。作业控制器仅处理那些它正在内存中跟踪的邮件。传送足够数量的邮件，释放足够的内存中存储空间后，作业控制器将通过扫描 MTA 队列区域以更新其邮件列表来自动刷新其内存中存储。然后作业控制器开始处理其他刚从磁盘检索的邮件文件。作业控制器自动执行对 MTA 队列区域的这些扫描。

如果您的站点日常要处理大量邮件，则您需要通过使用 MAX_MESSAGES 选项调整作业控制器。通过增大 MAX_MESSAGES 选项值来允许作业控制器使用更多内存，可以减少待处理邮件溢出作业控制器的内存中高速缓存情况的次数。这减少了作业控制器必须扫描 MTA 队列目录时有关的系统开销。但是请记住，当作业控制器必须要重建内存中高速缓存时，由于高速缓存增大，进程将花费更长时间。也请注意，因为每次启动或重新启动作业控制器时，它必须扫描 MTA 队列目录，所以大的待处理邮件意味着作业控制器的启动或重新启动将比没有此类待办事项存在时需要更多开销。

有关池和配置作业控制器的详细信息，请参见第 225 页的 “作业控制器文件”和第 318 页的 “配置邮件处理和传送”。

启动和停止作业控制器

要启动作业控制器，请执行以下命令：

```
start-msg job_controller
```

要关闭作业控制器，请执行以下命令：

```
stop-msg job_controller
```

要重新启动作业控制器，请执行以下命令：

```
imsimta restart job_controller
```

重新启动作业控制器与关闭当前运行的作业控制器再立即启动新的作业控制器具有同样效果。

第 9 章

MTA 地址转换和路由

低于 Messaging Server 6 2003Q4 的 Messaging Server 通过由 LDAP 服务器中存储的信息编译得到的数据库来访问所有用户、域和组数据。 LDAP 服务器中的目录信息更新时，数据库信息通过称为 `dirsync` 的程序同步更新。现在，Messaging Server MTA 可以直接访问 LDAP 目录。本章介绍使用直接 LDAP 数据访问时 MTA 中的数据流。本章包含以下各节：

- 第 181 页的 “直接 LDAP 算法和实现”
- 第 201 页的 “地址反向”
- 第 203 页的 “异步 LDAP 操作”
- 第 204 页的 “设置摘要”

直接 LDAP 算法和实现

以下各节介绍直接 LDAP 处理。

域位置确定

启动 *user@domain* 格式的地址时，地址转换和路由进程将首先检查以查看 *domain* 是否是本地域。

重写规则机制

MTA 重写规则机制添加了新的功能，用于检查给定字符串是否为需要在本地进行处理的域。通过 $V 或 $Z 元字符可以激活此新增功能。从句法上来说，这些新增元字符类似于现有的 $N、$M、$Q 和 $C 元字符，即这些元字符之后都跟一个模式字符串。就 $N、$M、$Q 和 $C 而言，此模式与源通道或目标通道相匹配。就 $V 和 $Z 而言，此模式是一个域，将检查以查看其是否为本地域。$V 导致非本地域的规则失败，$Z 导致本地域的规则失败。

按以下过程可以实现对这些元字符的处理：

1. Messaging Server 检查以查看当前域与目录中的有效域条目是否匹配。如果不存在该条目，则转至步骤 3。
2. 如果该域在目录中有条目，将从域条目中检索到由 LDAP_DOMAIN_ATTR_ROUTING_HOSTS MTA 选项 （默认值为 mailRoutingHosts）指定的属性。如果存在该属性，它将列出能够处理该域中的用户的一组主机。该列表将与通过 local.hostname configutil 参数指定的主机以及通过 local.imta.hostnamealiases configutil 参数指定的主机列表相比较。可以通过 LDAP_LOCAL_HOST 和 LDAP_HOST_ALIAS_LIST MTA 选项分别覆盖这些选项。如果存在匹配或者域中不存在该属性，则该域为本地域。如果未出现匹配，则该域为非本地域。

   由于 mailRoutingHosts 属性取决于 ROUTE_TO_ROUTING_HOST MTA 选项的设置，因此将这些域作为非本地域对其进行处理。如果将选项设置为 0 （默认设置），地址将仅被视为非本地地址， MTA 重写规则用于确定路由。如果将选项设置为 1，地址前置了源路由 （包含 LDAP_DOMAIN_ATTR_ROUTING_HOSTS MTA 选项中列出的第一个值）。
3. 如果找不到任何域条目，则从域的左侧删除组件，然后转至步骤 1。如果没有剩余组件，则继续执行步骤 4。

   这种回溯域树的结果就是如果 domain.com 被识别为本地域，则 domain.com 的所有子域将被识别为本地子域。可能会出现某些料想不到的情况，因此提供了 MTA 选项 DOMAIN_UPLEVEL 来控制该性能。特别是，如果将 DOMAIN_UPLEVEL 的位 0 （值 = 1）清除，则会禁用删除域组件的重试操作。 DOMAIN_UPLEVEL 的默认值为 0。

4. 现在需要执行虚名域检查。虚名域没有域条目，而是通过将特定的域属性附加到一个或多个用户条目指定的。使用通过 DOMAIN_MATCH_URL MTA 选项指定的 LDAP URL 来执行 LDAP 搜索可以完成虚名域检查。应该将该选项的值设置为：

   ```
   ldap:///$B?msgVanityDomain?sub?(msgVanityDomain=$D)
   ```

   $B 将替换 local.ugldapbasedn configutil 参数的值；这是目录中用户树的基目录。 LDAP_USER_ROOT MTA 选项可用于专为 MTA 覆盖该 configutil 选项的值。

   该搜索的实际返回值并不重要。重要的是是否会返回值。如果返回值，该域将被视为本地域；如果未返回值，该域将被视为非本地域。

域位置的域映射确定

提醒您注意在目录中查找有效域条目执行哪些步骤。这些步骤是特定于模式级别的。就 Sun LDAP Schema 1 而言，这些步骤包括：

1. 将域转换为域树中的基本 DN。通过将域转换为一系列 dc 组件，然后添加域根后缀可以完成此操作。默认后缀可通过 service.dcroot configutil 参数获得。默认后缀为 o=internet。因此 a.b.c.d 格式的域通常被转换为 dc=a,dc=b,dc=c,dc=d,o=internet。通过设置 LDAP_DOMAIN_ROOT MTA 选项可以覆盖 service.dcroot configutil 参数。
2. 查找具有在步骤 1 中找到的基本 DN 的条目，以及对象类为 inetDomain 或 inetDomainAlias 的条目。通过设置 LDAP_DOMAIN_FILTER_SCHEMA1 MTA 选项 （默认设置为 (|(objectclass=inetDomain)(objectclass=inetdomainalias)) ）可以覆盖用于此目的的搜索过滤器。
3. 如果未找到任何条目，则以失败退出。
4. 如果找到条目的对象类为 inetDomain，请检查以确保该条目具有与域条目相关联的 inetDomainBaseDn 属性。如果存在该属性，系统会将其保存以供后续搜索用户条目以及终止处理时使用。如果不存在该属性，则假定该条目为域别名并继续处理步骤 5。 MTA 选项 LDAP_DOMAIN_ATTR_BASEDN 可用于覆盖 inetDomainBaseDN 的使用。
5. 条目必须为域别名；查找 aliasedObjectName 属性所引用的新条目，然后返回至步骤 4。如果 aliasedObjectName 属性不存在，处理将因出现故障而终止。使用 aliasedObjectName 属性的替代方法可以通过 MTA 选项 LDAP_DOMAIN_ATTR_ALIAS 指定。

   请注意，处理最多只能返回步骤 4 一次；不允许使用指向域别名的域别名。

在 Sun LDAP Schema 2 中，所采取的操作更简单：搜索目录，查找具有对象类 sunManagedOrganization 的条目，其中域显示为 sunPreferredDomain 或 associatedDomain 属性的值。如果需要使用用于此目的的 sunPreferredDomain 和 associatedDomain 属性，则可以使用 MTA 选项 LDAP_ATTR_DOMAIN1_SCHEMA2 和

LDAP_ATTR_DOMAIN2_SCHEMA2 分别覆盖这两个属性。在由 service.dcroot configutil 参数指定的根目录下执行搜索。通过设置 LDAP_DOMAIN_ROOT MTA 选项可以覆盖 service.dcroot configutil 参数。此外， Schema 2 中的域条目不需要有 inetDomainBaseDn 属性；如果没有这些属性，用户树的基目录将被假定为域条目本身。

缓存域位置信息

由于执行域重写操作很频繁并且目录查询 （尤其是虚名域检查）很耗时，因此需要缓存有关域的负向和正向指示。使用内存中的开放链的动态扩展散列表可以实现此操作。通过 DOMAIN_MATCH_CACHE_SIZE MTA 选项 （默认值为 100000）可以设置高速缓存的最大大小，通过 DOMAIN_MATCH_CACHE_TIMEOUT MTA 选项 （默认值为 600 秒）可以设置高速缓存中的条目的超时值。

错误处理

必须小心处理在此进程中出现的临时服务器故障，发生这些故障以后，系统将无法知道给定域是否为本地域。在这种情况下，基本上会出现两种结果：

1. 将临时 (4*xx*) 错误返回到客户机，通知其稍后重试该地址。
2. 接受该地址，但将其排入到重新处理的通道，这样可以在本地稍后重试该地址。

这些选项并不适合所有的情况。例如，当与远程 SMTP 中继通话时，则对应于结果 1。但处理来自本地用户的 SMTP 提交时，则对应于结果 2。

虽然从理论上来说，可以通过在同一模式下使用多个规则来处理临时故障，但是，即使具备高速缓存，由于重复进行此类查询所带来的系统开销也无法接受。由于这些原因，域重写的简单成功 / 失败转到下一规则匹配的模型都是不足的。而在域查找失败的情况下，可以使用通过 MTA 选项 DOMAIN_FAILURE 指定的特殊模板。 $V 操作失败后，该模板将替换要处理的当前重写规则模板的剩余部分。

域检查重写规则的模式

在有可能运行其他重写规则操作之前，需要先执行该域检查。通过在规则的左侧使用特殊的 $* 可以确保此排序。在检查所有其他规则之前，先检查 $* 模式。

汇总所有机制

在帐户中采用到目前为止所述的所有机制时， imta.cnf 中所需的新重写规则将为：

```
$*        $E$F$U%$H$V$H@localhost
```

并且 option.dat 文件中的 DOMAIN_FAILURE MTA 选项的值需要为：

```
reprocess-daemon$Mtcp_local$1M$1~-error$4000000?Temporary lookup failure
```

在此重写规则中， localhost 是与本地通道相关联的主机名。此处所示的 DOMAIN_FAILURE 选项的值是默认值，因此在一般环境下不需要将该值显示在 option.dat 中。

此处的排序特别需要慎重对待。 MTA 检查 $V 应在重建地址后但在添加路由之前进行。在临时查找失败的情况下， MTA 将更改路由。在任何时候插入点发生了更改，就可以应用待定通道匹配检查，以便第二个 $H 之后的 @ 调用检查。如果检查成功，将应用模板的剩余部分并重写处理结论。如果检查失败，重写就会失败，重写将继续执行下一个适用的重写规则。如果由于临时故障无法执行检查，模板处理将使用通过 DOMAIN_FAILURE MTA 选项指定的值继续操作。首先，该模板的值将路由主机设置为 reprocess-daemon。然后，模板将检查以查看 MTA 是否正在处理某类重新处理通道或 tcp_local。如果 MTA 正在处理此类通道，则规则将继续，因此使路由主机非法并将临时故障指定为结果。如果 MTA 没有处理此类通道，则规则将被截断并成功终止，因此将地址重写到重新处理通道。

本地地址的别名扩展

确定地址与本地通道相关联后，该地址将自动进行别名扩展。别名扩展处理将检查若干信息源，包含：

1. 别名文件 （已编译配置的一部分）。
2. 别名数据库。
3. 别名 URL。

检查确切别名源以及检查这些源的顺序取决于 option.dat 文件中的 ALIAS_MAGIC MTA 选项的设置。对于直接 LDAP，将选项设置为 8764。这表示首先检查通过 ALIAS_URL0 MTA 选项指定的 URL，再检查通过 ALIAS_URL1 MTA 选项指定的 URL，接着检查通过 ALIAS_URL2 MTA 选项指定的 URL，最后检查别名文件。此设置有效时，将不检查别名数据库。

使用 LDAP URL 检查别名

通过将两个特殊 LDAP URL 指定为别名 URL，可以实现检查 LDAP 中的别名。上述第一个 URL 处理常规用户和组；后续别名 URL 处理虚名域。第一个 URL 被指定为 ALIAS_URL0：

```
ALIAS_URL0=ldap:///$V?*?sub?$R
```

$V 元字符

元字符扩展发生在 URL 查找之前。在 ALIAS_URL0 值中使用的两个元字符为 $V 和 $R。

$V 元字符将地址的域部分转换为基本 DN。这与前面的标题为 “重写规则机制”一节中所述的 $V 重写规则元字符所执行的初始步骤类似。$V 处理包含以下步骤：

1. 获取当前域中用户条目的基本 DN。
2. 获取与当前域相关联的规范域。在 Sun LDAP Schema 1 中，如果存在 inetCanonicalDomainName 属性，域条目的该属性将给出规范域名。如果不存在该属性，规范域名则是通过实际域条目的 DN 以明显的方式构建的。如果当前域是一个别名，这将与当前域不同。可以使用 option.dat 文件中的 LDAP_DOMAIN_ATTR_CANONICAL MTA 选项覆盖用于存储规范名称的名称属性。

   在 Sun LDAP Schema 2 中，规范名称只是 SunPreferredDomain 属性的值。
3. 如果存在基本 DN，则使用该 DN 替换 URL 中的 $V。
4. 现在确定了该条目的所有可用托管域。通过将规范域 （如果清除了 DOMAIN_UPLEVEL 的位 2 [值 = 4]）或当前域 （如果设置了 DOMAIN_UPLEVEL 的位 2 [值 = 4]）与 service.defaultdomain configutil 参数相比较，可以完成此操作。如果不匹配，则该条目是托管域的成员。通过设置 option.dat 文件中的 LDAP_DEFAULT_DOMAIN MTA 选项可以覆盖 service.defaultdomain configutil 参数。
5. 如果基本 DN 确定失败，则从域的左侧删除组件，然后转至步骤 1。如果没有剩余任何组件，则替换将失败。

$V 还接受可选数字变量。如果将其设置为 1 （例如 $1V），将忽略解析域树中的域时出现的失败，并返回由 local.ugldapbasedn configutil 选项指定的用户树的基目录。

如果尝试检索域的基本 DN 成功， MTA 还将检索稍后会需要的若干有用的域属性。检索到的属性的名称通过 option.dat 文件中的以下 MTA 选项进行设置：

- LDAP_DOMAIN_ATTR_UID_SEPARATOR （默认值为 domainUidSeparator）
- LDAP_DOMAIN_ATTR_SMARTHOST （默认值为 mailRoutingSmartHost）
- LDAP_DOMAIN_ATTR_CATCHALL_ADDRESS （默认值为 mailDomainCatchallAddress）
- LDAP_DOMAIN_ATTR_BLOCKLIMIT （默认值为 mailDomainMsgMaxBlocks）
- LDAP_DOMAIN_ATTR_REPORT_ADDRESS （默认值为 mailDomainReportAddress）
- LDAP_DOMAIN_ATTR_STATUS （默认值为 inetDomainStatus）
- LDAP_DOMAIN_ATTR_MAIL_STATUS （默认值为 mailDomainStatus）
- LDAP_DOMAIN_ATTR_CONVERSION_TAG （默认值为 mailDomainConversionTag）

- LDAP_DOMAIN_ATTR_FILTER （默认值为 mailDomainSieveRuleSource）
- LDAP_DOMAIN_ATTR_DISK_QUOTA （没有默认值）
- LDAP_DOMAIN_ATTR_MESSAGE_QUOTA （没有默认值）
- LDAP_DOMAIN_ATTR_AUTOREPLY_TIMEOUT （没有默认值）
- LDAP_DOMAIN_ATTR_NOSOLICIT （没有默认值）
- LDAP_DOMAIN_ATTR_OPTIN （没有默认值）
- LDAP_DOMAIN_ATTR_RECIPIENTLIMIT （没有默认值）
- LDAP_DOMAIN_ATTR_RECIPIENTCUTOFF （没有默认值）
- LDAP_DOMAIN_ATTR_SOURCEBLOCKLIMIT （没有默认值）

从 URL 调用映射

以某些其他方式完成从域到基本 DN 的映射时可能会出现一些特殊情况。为了容纳此类设置， URL 解析过程可以调用 MTA 映射。使用以下通用格式的元字符序列完成此操作：

$|/*mapping-name*/*mapping-argument*|

双引号 (") 将启动和终止调用。紧跟在 $ 后的字符是映射名称和变量之间的分隔符；应该选择与映射名称或变量中使用的期望字符值不发生冲突的字符。

$R 元字符

$R 元字符为 URL 提供了适当的过滤器。目的在于生成一个过滤器，该过滤器可以搜索可能包含特定用户或组的电子邮件地址的所有属性。要搜索的属性的列表来自于 configutil 参数 local.imta.mailaliases。如果未设置此参数，则会检验 local.imta.schematag configutil 参数，并根据此参数的值，选择一组相应的默认属性，如下所示：

```
sims401         mail, rfc822mailalias

nms41           mail,mailAlternateAddress

ims50           mail,mailAlternateAddress,mailEquivalentAddress
```

local.imta.schematag 的值可以是以逗号分隔的列表。如果支持多种模式，则使用消除了复制功能的属性的组合列表。LDAP_SCHEMATAG MTA 选项可用于专为 MTA 覆盖 local.imta.schematag 的设置。

此外，过滤器不但搜索原来提供的地址，而且还搜索具有相同本地部分但实际上是在域树 （该域树是在标题为 “$V 元字符”一节中的步骤 2 中保存的）中找到域的地址。域树查找的重复性意味着两个地址可能不同。此附加检查由 option.dat 文件中的 DOMAIN_UPLEVEL MTA 选项的位 1 （值 = 2）来控制。设置位将启用附加地址检查。 DOMAIN_UPLEVEL 的默认值为 0。

例如，假定域 siroe.com 显示在域树中。假设 Sun LDAP Schema 1 有效，要查找的地址是

```
u@host1.siroe.com
```

扩展 $R 和 ims50 schematag 得到的过滤器将类似于：

```
(|(mail=u@siroe.com)
     (mail=u@host1.siroe.com)
     (mailAlternateAddress=u@siroe.com)
     (mailAlternateAddress=u@host1.siroe.com)
     (mailEquivalentAddress=u@siroe.com)
     (mailEquivalentAddress=u@host1.siroe.com))
```

另一方面，如果将 DOMAIN_UPLEVEL 设置为 1 而不是 3，则过滤器将为：

```
(|(mail=u@host1.siroe.com)
     (mailAlternateAddress=u@host1.siroe.com)
     (mailEquivalentAddress=u@host1.siroe.com))
```

确定要获取的属性

如果 URL 为要返回的属性的列表指定 * 号，我们将用 MTA 能够使用的属性的列表替换星号。此列表是由指定 MTA 所使用选项的各个 MTA 选项设置动态生成的。

处理 LDAP 错误

此时，所得到的 URL 用于执行 LDAP 搜索。如果出现某种 LDAP 错误，处理将终止于临时故障指示 （SMTP 中的 4xx 错误）。如果 LDAP 操作成功，但无法生成结果，将检查通过 LDAP_DOMAIN_ATTR_CATCHALL_ADDRESS MTA 选项检索到的域的替换邮件地址属性。如果设置了该属性，则该属性的值将替换当前地址。

如果未设置替换邮件地址属性，将检查通过 LDAP_DOMAIN_ATTR_SMARTHOST MTA 选项检索到的域的智能主机属性。如果设置了该属性，则创建

@smarthost:user@domain

格式的地址，并且别名处理将以此结果成功终止。此外，通过 LDAP_DOMAIN_ATTR_CONVERSION_TAG MTA 选项获得的域的转换标记 （如果存在）将被附加到地址中，以便在转发给智能主机之前可以先完成转换操作。如果该域不存在替换邮件地址或智能主机，则此别名 URL 的处理将不会成功终止。

对 LDAP 结果的正常性检查

LDAP 搜索返回了结果之后，它将验证其中是否只有一个条目。如果具有多个条目，则检查每个条目以确定其是否具有用户或组的正确对象类、不可删除的状态以及具有用户的 UID。忽略未通过此检查的条目。如果通过此检查将多个条目的列表减少到只有一个条目，则处理将继续进行。如果没有减少，将返回一个复制或模糊目录错误。

支持虚名域

ALIAS_URL0 检查是针对常规用户或托管域中的用户的。如果此检查失败，还会进行虚名域检查。使用以下别名 URL 可以完成此操作：

```
ALIAS_URL1=ldap:///$B?*?sub?(&(msgVanityDomain=$D)$R)
```

支持替换邮件地址

最后，需要在 mailAlternateAddress 属性中进行 @*host* 格式的替换邮件地址检查。此格式的通配符允许在托管域和虚名域中使用，因此地址的正确别名 URL 为：

```
ALIAS_URL2=ldap:///$1V?*?sub?(mailAlternateAddress=@$D)
```

注 在直接 LDAP 模式中，+* 子地址替换机制始终用于处理替换邮件地址，但被替换的字符串仅为子地址，而非整个本地部分。这种情况已改变，使用这种构造时原始地址的整个本地部分将作为子地址插入替换邮件地址。

例如，给定形式为 foo+bar@domain.com 的地址 （domain.com 域中没有本地用户 foo）以及 domain.com 的替换邮件地址 bletch+*@example.com，最终得到的地址为 bletch+foo+bar@example.com。而原来是 bletch+bar@example.com。

处理 LDAP 结果

可以通过若干顺序独立的阶段完成 LDAP 别名结果的处理。以下各节介绍了这些阶段。

对象类检查

如果别名搜索成功，将检查条目的对象类以确保其包含用户或组的一组相应的对象类。通常，用户和组的所需对象类的可能设置由有效的模式来确定。这由 local.imta.schematag 设置确定。

表 9-1 显示了从各个 schematag 值得到的用户和组对象类。

表 9-1 从各个 schematag 值得到的对象类

schematag	用户对象类	组对象类
sims40	inetMailRouting+inetmailuser	inetMailRouting+inetmailgroup
nms41	mailRecipient + nsMessagingServerUser	mailGroup
ims50	inetLocalMailRecipient+inetmailuser	inetLocalMailRecipient+inetmailgroup

很难编码该表中的信息（如处理其余的模式标记）。但是，在 option.dat 文件中还有两个 MTA 选项 LDAP_USER_OBJECT_CLASSES 和 LDAP_GROUP_OBJECT_CLASSES，可以设置这两个选项以分别指定用户和组的对象类的不同设置。

例如， ims50,nms41 模式标记的设置将等价于以下选项设置：

```
LDAP_USER_OBJECT_CLASSES=inetLocalMailRecipient+inetmailuser,
mailRecipient+nsMessagingServerUser
```

```
LDAP_GROUP_OBJECT_CLASSES=inetLocalMailRecipient+inetmailgroup,mailGroup
```

如果 LDAP 结果不具有适用于用户或组的一组正确的对象类，将只会忽略该结果。MTA 还确定其是否处理用户或组，并保存该信息。稍后将重复使用此处保存的信息。

请注意，此处所述的对象类设置还用于构建实际的 LDAP 搜索过滤器，该过滤器可用于检查以查看条目是否具有用户或组的正确对象类。可以通过 $K 元字符访问该过滤器。该过滤器还存储在 MTA 的配置内，以备通道程序使用，并作为 LDAP_UG_FILTER 选项（在使用命令 imsimta cnbuild -option 时）写入到 MTA 选项文件 option.dat 中。该选项只写入到文件中。 MTA 不通过选项文件读取该选项。

条目状态检查

接下来检查条目的状态。有两个状态属性，一个用于常规条目，另一个专用于邮件服务。

表 9-2 介绍了在不同的 schematag 中， schematag 条目中用于作为检验标准的普通用户或组属性和特定于邮件的用户或组属性

表 9-2 要进行检查的属性

schematag	类型	常规	邮件特定
sims40	用户	inetsubscriberstatus	mailuserstatus
sims40	组	无	inetmailgroupstatus
nms41	用户	无	mailuserstatus
nms41	组	无	无
Messaging Server 5.0	用户	inetuserstatus	mailuserstatus
Messaging Server 5.0	组	无	inetmailgroupstatus

如果需要，option.dat 文件中的 LDAP_USER_STATUS 和 LDAP_GROUP_STATUS MTA 选项可分别用于选择用户和组的备用常规状态属性。邮件特定的用户和组状态属性由 LDAP_USER_MAIL_STATUS 和 LDAP_GROUP_MAIL_STATUS MTA 选项控制。

起控制作用的另一个因素是域本身的状态 （LDAP_DOMAIN_ATTR_STATUS 和 LDAP_DOMAIN_ATTR_MAIL_STATUS）。总共有四种状态属性。以下列顺序考虑这些属性的组合：

1. 域状态
2. 域邮件状态
3. 用户或组状态
4. 邮件用户或邮件组状态

指定了除 “活动”状态以外的状态的这些属性中的第一个属性优先于所有其他属性。允许的其他状态值包括 “不活动”、“已删除”、“已移除”、“已禁用”、“保留”和 “超过配额”。只能将 “保留”、“已禁用”和 “已移除”状态指定给邮件域、邮件用户或邮件组。只能将 “超过配额”状态指定为邮件域或邮件用户状态。

如果不存在特定状态属性，则所有状态都默认为 “活动”。未知状态值被解释为 “不活动”。

组合使用四种状态时，可能出现用户或组的下列状态：“活动”、“不活动”、“已删除”、“已移除”、“已禁用”、“保留”和 “超过配额”。活动状态会使别名处理继续进行。不活动或超过配额状态将会立即拒绝具有 4xx （临时）错误的地址。已删除、已移除和已禁用状态将会立即拒绝具有 5xx （永久）错误的地址。就状态处理而言，可以将保留状态视为活动状态，但它设置了内部标志，以便以后考虑传送选项，所有被覆盖的选项都具有包含一个 “保留”条目的选项列表。

UID 检查

下一步将考虑条目的 UID。 UID 可用于各种目的，它必须是所有用户条目的一部分，并且可以包含在组条目中。不具有 UID 的用户条目将被忽略，并且该别名 URL 的处理也会不成功终止。托管域中条目的 UID 可以包含实际 UID、分隔符以及域。如果目前使用通过 option.dat 文件中的 LDAP_DOMAIN_ATTR_UID_SEPARATOR MTA 选项获得的域分隔符，则 MTA 只希望使用实际 UID，因此删除其余部分。

万一使用某个属性而不是 uid 来存储 UID，LDAP_UID MTA 选项则可用于强制使用其他属性。

邮件捕获

接下来检查用于指定一个或多个邮件捕获地址的 LDAP 属性。必须使用 LDAP_CAPTURE MTA 选项指定用于此目的的属性。没有默认值。该属性的值将被视为地址，生成一个特殊的 “捕获” 通知，并将该通知发送到以附件方式包含当前邮件的这些地址。此外，如果捕获地址用于初始化地址反向高速缓存，该地址以后将显示为信封 from: 地址。

初始化反向高速缓存

接下来将考虑主地址和附加到用户条目的所有别名。该信息可用于初始化地址反向高速缓存。此操作在当前地址转换进程中不起作用。首先，考虑主地址、个人名称、收件人限制、收件人截止日期和源块限制属性。主地址通常存储于 "mail" 属性中；其他属性可以通过相应设置 LDAP_PRIMARY_ADDRESS MTA 选项来指定。（当然，主地址的反向结果与其自身相同。）所有其他属性都没有默认属性。如果要使用这些属性，您必须通过 LDAP_PERSONAL_NAME （请参见第 453 页的 “休假自动回复属性”）、LDAP_RECIPIENTLIMIT、LDAP_RECIPIENTCUTOFF （请参见第 349 页的 “对邮件收件人进行限制”）和 LDAP_SOURCEBLOCKLIMIT （请参见第 346 页的 “指定绝对邮件大小限制”） MTA 选项指定这些属性。此时还要考虑相应的域级别收件人限制、收件人截止日期和源块限制属性。用户级别设置将完全覆盖所有域级别设置。

接下来，将考虑所有次地址，并为每个地址设置一个高速缓存条目。次地址包括两类：一类进行地址反向，另一类则不进行。必须考虑这两类地址以便正确初始化地址反向高速缓存，因为在所有情况下都需要检查邮件捕获请求。

进行反向的次地址通常存储于 mailAlternateAddress 属性中。通过设置 LDAP_ALIAS_ADDRESSES MTA 选项可以指定其他属性。不进行反向的次地址通常存储于 mailEquivalentAddress 属性中。使用 LDAP_EQUIVALENCE_ADDRESSES MTA 选项可以指定其他属性。

邮件主机和路由地址

现在来考虑 mailhost 和 mailRoutingAddress 属性。可以考虑使用 LDAP_MAILHOST 和 LDAP_ROUTING_ADDRESS MTA 选项分别覆盖实际属性。这些属性协同工作以确定此时这些属性是否应作用于地址或转发给其他系统。

第一步要确定 mailhost 对于该条目是否有意义。执行作用于条目的有效传送选项的初步检查，以查看该条目是否为邮件主机特定的。如果不是，则省略 mailhost 检查。要了解该检查的执行方式，请查看第 195 页的 “传送选项处理”的说明 （尤其是 # 标志）。

就用户条目而言， mailhost 属性必须标识本地系统才能使该属性作用于本地系统。将 mailhost 属性与 local.hostname configutil 参数的值相比较，并与 local.imta.hostnamealiases configutil 参数指定的值的列表相比较。如果出现任一匹配，则 mailhost 属性将被视为标识本地主机。

成功匹配意味着别名可以在本地起作用，并且别名处理将继续进行。不成功匹配则意味着需要将邮件转发给邮件主机才能起作用。将构建格式为

@mailhost:*user@domain*

的新地址，该地址将成为别名扩展操作的结果。

根据该条目是用户还是组，对缺少 mailhost 属性的处理有所不同。就用户而言，邮件主机是重要的，因此如果不存在 mailhost 属性，则格式为

@smarthost:*user@domain*

的新地址将会使用通过 LDAP_DOMAIN_ATTR_SMARTHOST MTA 选项确定的域的智能主机来构建。如果该域不存在智能主机，则会报告错误。

另一方面，组不需要邮件主机，因此缺少邮件主机将被解释为意味着可以随处扩展组。因此别名处理将继续进行。

mailRoutingAddress 属性将添加一个最终难题。如果该问题存在，则别名处理将终止，结果为 mailRoutingAddress。但是，如果邮件主机存在，会将该问题添加到作为源路由的 mailRoutingAddress 中。

其他属性支持

接下来，将考虑 mailMsgMaxBlocks 属性。首先，使用通过 LDAP_DOMAIN_ATTR_BLOCKLIMIT MTA 选项返回的域块限制将其最小化。如果已知当前邮件的大小超过限制，别名处理将终止，产生一个超过大小的错误。如果大小未知或未超过限制，则会存储该限制并在稍后检查邮件自身时重新检查限制。用 LDAP_BLOCKLIMIT MTA 选项可以覆盖使用 mailMsgMaxBlocks。

下一步将访问并保存若干属性。最终，这些属性将被写入到队列文件条目中以供 ims_master 通道程序使用，然后该程序将使用这些属性来更新存储的用户信息高速缓存。如果未找到单个用户的属性，可以使用域级别属性设置默认属性。

如果 LDAP 条目适用于组而不适用于用户，或者如果 LDAP 条目来自别名高速缓存而不是来自 LDAP 目录，则跳过此步骤。后一个标准的逻辑是不需要经常更新此信息，如果需要更新，应使用别名高速缓存提供合理的标准。检索到的属性的名称由各个 MTA 选项设置。

表 9-3 显示了设置检索到的磁盘配额和邮件配额属性的 MTA 选项。

表 9-3 设置检索到的磁盘配额和邮件配额属性的 MTA 选项

MTA 选项	属性
LDAP_DISK_QUOTA	mailQuota
LDAP_MESSAGE_QUOTA	mailMsgQuota

接下来，将存储若干属性，以备稍后可能与元字符替换结合使用。

表 9-4 显示了 MTA 选项、默认属性和元字符。

表 9-4 MTA 选项、默认属性和元字符

MTA 选项	默认属性	元字符
LDAP_PROGRAM_INFO	mailProgramDeliveryInfo	$P
LDAP_DELIVERY_FILE	mailDeliveryFileURL	$F
LDAP_SPARE_1	没有默认属性	$1E $1G $E
LDAP_SPARE_2	没有默认属性	$2E $2G $G
LDAP_SPARE_3	没有默认属性	$3E $3G
LDAP_SPARE_4	没有默认属性	$4E $4G
LDAP_SPARE_5	没有默认属性	$5E $5G

还包含用于其他属性的备用插槽，以便您可以使用这些插槽构建自定义地址扩展设备。

接下来，将与 mailconversiontag 属性相关联的所有值添加到一组当前的转换标记中。可以用 LDAP_CONVERSION_TAG MTA 选项更改该属性的名称。如果将所有值与域的 mailDomainConversionTag 属性相关联，也会附加这些值。

传送选项处理

接下来，将检查 mailDeliveryOption 属性。可以用 LDAP_DELIVERY_OPTION MTA 选项更改该属性的名称。这是一个多值选项，该选项的各个值确定了由别名转换进程生成的地址。此外，用于用户和组的允许值是不同的。通用允许值包括 program、forward 和 hold。仅限用户使用的值包括 mailbox、 native、 unix 和 autoreply。仅限组使用的值包括 members、 members_offline 和 file。

mailDeliveryOption 属性到相应地址的转换由 DELIVERY_OPTIONS MTA 选项来控制。该选项不仅指定每个允许的 mailDeliveryOption 值生成哪些地址，而且还指定允许的 mailDeliveryOption 值包括哪些以及每个值是否适用于用户、组或者用户和组。

该选项的值由 deliveryoption=template 对的以逗号分隔的列表组成，每对具有一个或多个可选单字符前缀。

DELIVERY_OPTIONS 选项的默认值为：

```
DELIVERY_OPTIONS=*mailbox=$M%$\\$2I$_+$2S@ims-ms-daemon,  \
     &members=*,                                          \
     *native=$M@native-daemon,                            \
     /hold=@hold-daemon:$A,                               \
     *unix=$M@native-daemon,                              \
     &file=+$F@native-daemon,                             \
     &@members_offline=*,                                 \
     program=$M%$P@pipe-daemon,                           \
     #forward=**,                                         \
     *^!autoreply=$M+$D@bitbucket
```

每个传送选项对应于可能的 mailDeliveryOption 属性值，相应的模板使用与 URL 处理使用的相同元字符替换方案来指定得到的地址。

表 9-5 显示了可用于 DELIVERY_OPTIONS 选项的单字符前缀。

表 9-5 用于 DELIVERY_OPTIONS MTA 选项中的选项的单字符前缀。

字符前缀	说明
@	设置一个标志，表明需要将邮件重定向至重新处理通道。放弃处理当前用户 / 组。忽略源自重新处理通道的邮件的标志。
*	传送选项应用于用户。
&	传送选项应用于组。

表 9-5 用于 DELIVERY_OPTIONS MTA 选项中的选项的单字符前缀。

字符前缀	说明
$	设置一个标志，表明要延迟该用户或组的扩展。
^	设置一个标志，表明应检查休假开始时间和结束时间以查看此传送选项是否真正有效。
#	设置一个标志，表明在条目指定的邮件主机中不需要进行此传送选项的扩展。即后面的条目独立于邮件主机。这使 MTA 可以进行检查，以查看给定的用户或组的所有传送选项是否均独立于邮件主机。如果满足此条件，则 MTA 可以立即操作此条目，而无需将此邮件转发给邮件主机。
/	设置一个标志，该标记会保留由该传送选项生成的所有地址。包含这些收件人地址的邮件文件将具有 .HELD 扩展名。
!	设置一个标志，表明自动回复操作应该由 MTA 进行内部处理。只有在自动回复选项中使用此前缀才有意义。选项的值应将邮件定向到 bitbucket 通道。

如果 * 或 & 都不存在，则采用传送选项应用于用户和组中。

传送选项中使用的附加元字符

已经添加了若干附加元字符以支持使用此 MTA 的 URL 模板的新增功能。这些元字符包含：

表 9-6 显示了附加元字符以及在传送选项中使用这些元字符的说明。

表 9-6 传送选项中使用的附加元字符

元字符	说明
$\	强制后续文本转为小写。
$^	强制后续文本转为大写。
$_	不对后续文本执行大小写转换。
$*n*A	插入地址的第 *n* 个字符。第一个字符是字符 0。如果省略 *n*，则替换整个地址。这适用于构建自动回复目录路径。
$D	插入地址的域部分。
$*n*E	插入第 *n* 个备用属性的值。如果省略 *n*，则使用第一个属性。
$F	插入传送文件的名称 （mailDeliveryFileURL 属性）。
$*n*G	插入第 *n* 个备用属性的值。如果省略 *n*，则使用第二个属性。
$*n*H	在从 0 计数的原地址中插入域的第 *n* 个组件。如果省略 *n*，则默认值为 0。
$*n*I	插入与别名相关联的托管域。该元字符接受整数参数 *n*，其语义如表 9-7 所述。
$*n*J	插入从 0 计数的托管域的第 *n* 部分。 *n* 的默认值为 0。

表 9-6 传送选项中使用的附加元字符 （续）

元字符	说明
$*n*O	插入与当前地址关联的源路由。该元字符接受整数参数 n，其语义如表 9-7 所述。
$K	插入与用户或组的对象类相匹配的 LDAP 过滤器。请参见 LDAP_UG_FILTER 仅用于输出的 MTA 选项的说明。
$L	插入地址的本地部分。
$*n*M	插入 UID 的第 *n* 个字符。第一个字符是字符 0。如果省略 n，则替换整个 UID。
$P	插入程序名称 （mailProgramDeliveryInfo 属性）
$*n*S	插入与当前地址相关联的子地址。该元字符接受整数参数 n，其语义如表 9-7 所述。
$*n*U	插入当前地址的邮箱部分的未用引号引起格式的第 n 个字符。第一个字符是字符 0。如果省略 n，则替换整个未用引号引起的邮箱。
$*n*X	插入邮件主机的第 *n* 个组件。如果省略 *n*，则插入整个邮件主机。

表 9-7 说明了整数参数如何修改 $nI 和 $nS 元字符的性能。

表 9-7 控制 $nI 和 $nS 元字符的性能修改的整数

整数	性能说明
0	如果没有可用的值，则失败 （默认值）。
1	如果有可用的值，则插入该值。如果没有，则不插入任何值。
2	如果有可用的值，则插入该值。如果没有可用值，则不插入任何值，并删除前面的字符 （ims-ms 通道需要此特殊性能）。
3	如果有可用的值，则插入该值。如果没有可用值，则不插入任何值并忽略后面的字符。

除了元字符，表 9-8 还显示了两个特殊的模板字符串。

表 9-8 特殊的模板字符串

特殊的模板字符串	说明
*	执行组扩展。该值对于用户条目无效。
**	扩展由 LDAP_FORWARDING_ADDRESS MTA 选项命名的属性。这将默认设置为 mailForwardingAddress。

以组扩展为例，如果将用户的 mailDeliveryOption 值设置为 mailbox，将形成一个新地址，该地址由以下几部分组成：已拆开的 UID、百分比符号 （后面跟托管域，如果托管域可用）、加号 （后面跟子地址，如果指定了子地址）、最后是 @ims-ms-daemon。

传送选项默认设置

如果此时活动传送选项列表为空，则为用户激活列表中的第一个选项 （通常为邮箱），并为组激活列表中的第二个选项 （通常为成员）。

开始和结束日期检查

读取传送选项列表后，将检查开始和结束日期。有两个属性，其名称分别由 LDAP_START_DATE （默认值为 vacationStartDate）和 LDAP_END_DATE （默认值为 vacationEndDate） MTA 选项控制。如果一个或多个活动传送选项指定了 ^ 前缀字符，将针对当前日期检查这些选项的值。如果当前日期超出这些选项所指定的范围，将从活动集中删除带有 ^ 前缀的传送选项。有关更多信息，请参见第 453 页的“休假自动回复属性”。

Optin 和 Presence 属性

LDAP_OPTIN MTA 选项可用于指定包含垃圾邮件过滤器选定值的列表的 LDAP 属性。如果指定了该选项并且存在该属性，则将其附加到当前垃圾邮件过滤器选定列表中。 LDAP_DOMAIN_ATTR_OPTIN MTA 选项设置的域级别属性所设置的所有值也将附加到列表中。

LDAP_PRESENCE MTA 选项可用于指定 URL，可以解析此 URL 以返回有关用户的存在信息。如果指定了该选项并且存在该属性，则会保存该属性的值以备与 Sieve 存在测试结合使用。如果不存在用户条目的值，则会将 LDAP_DOMAIN_ATTR_PRESENCE MTA 选项所设置的域级别属性用作此 URL 的来源。

Sieve 过滤器处理

接下来将检查应用于此条目的 Sieve 过滤器的 mailSieveRuleSource 属性。如果存在该属性，此时将分析并保存该属性。该属性的值的两种可能的格式为包含一个完整 Sieve 脚本的单个值或每个值包含一段 Sieve 脚本的多个值。后一种格式由 Web 过滤器构造界面生成。特殊代码用于对这些值进行排序并将其正确组合在一起。

通过使用 LDAP_FILTER MTA 选项可以特别覆盖使用 mailSieveRuleSource 属性。

延迟的处理控制

接下来，将检查 mailDeferProcessing 属性。通过使用 LDAP_REPROCESS MTA 选项可以更改该属性。如果存在该属性并将其设置为 no，通常处理将继续进行。但如果将该属性设置为 yes，并且当前源通道不是重新处理通道，则该条目的扩展将被终止并且原 *user@domain* 地址将只是排入到重新处理通道中。如果不存在该属性，将检查与传送选项处理相关联的延迟处理字符前缀的设置。（有关示例，请参见 “传送选项处理”一节。）如果已设置，将延迟处理。如果未设置，用户的默认设置将为 no。组的默认设置由 MTA 选项 DEFER_GROUP_PROCESSING 控制，其默认值为 1（是）。此时将结束用户条目的别名处理。

组扩展属性

一系列附加属性与组扩展相关联，并且此时必须对这些属性进行处理。这些属性的名称都可以通过各个 MTA 选项进行配置。

表 9-9 列出了默认属性名、要设置属性名的 MTA 选项和 MTA 处理属性的方式。此表中元素的排序显示了处理各个组属性的顺序。该排序对于正确操作极为重要。

表 9-9 组扩展默认属性和用于设置属性名称的 MTA 选项

默认属性	（用于设置属性名称的 MTA 选项）处理属性的方法
mgrpMsgRejectAction	(LDAP_REJECT_ACTION) 单个值的属性，用于控制当后续访问检查失败时会如何操作。只定义了一个值：TOMODERATOR，如果设置该值，将指示 MTA 把所有访问失败重定向到 mgrpModerator 属性所指定的中介人。默认值 （以及该属性的所有其他值）将会报告一个错误并拒绝邮件。
mailRejectText	(LDAP_REJECT_TEXT) 将保存存储于该属性的第一个值中的文本的第一行。如果以下任一验证属性使邮件被拒绝，将返回此文本。这意味着文本可以显示在 SMTP 响应中，因此只能将值限定为 US-ASCII 才能符合当前的邮件传送标准。
mgrpBroadcasterPolicy	(LDAP_AUTH_POLICY) 指定发送到组所需的验证级别。可能的标记为 SMTP_AUTH_REQUIRED 或 AUTH_REQ，这两个值都表示 SMTP AUTH 命令必须用于标识发件人以便发送到组； PASSWORD_REQUIRED、 PASSWD_REQUIRED 或 PASSWD_REQ 都表示由 mgrpAuthPassword 属性指定的列表的密码必须显示在邮件的 Approved: 标题字段中； OR 用于将此列表的 OR_CLAUSES MTA 选项设置改为 1； AND 用于将此列表的 OR_CLAUSES MTA 选项设置改为 0； NO_REQUIREMENTS 为 no-op。允许多值。每个值由以逗号分隔的标记列表组成。 如果调用 SMTP AUTH，它还表示所有后续验证检查将针对 SASL 层所提供的电子邮件地址而不是 MAIL FROM 地址来完成。
mgrpAllowedDomain	(LDAP_AUTH_DOMAIN) 域允许将邮件提交到该组中。OR_CLAUSES MTA 设置为 0（默认值）时匹配失败，表明访问检查已失败且将避开所有后续测试。 OR_CLAUSES MTA 设置为 1 时匹配失败，将设置 “失败暂挂”标志；其他访问检查必须都成功才能使访问检查成功。如果提交者已经与 LDAP_AUTH_URL 匹配，则将避开此检查。可具有多个值，并允许使用全局样式通配符。

表 9-9 组扩展默认属性和用于设置属性名称的 MTA 选项 （续）

默认属性	（用于设置属性名称的 MTA 选项）处理属性的方法
mgrpDisallowedDomain	(LDAP_CANT_DOMAIN) 域不允许将邮件提交到该组中。出现匹配就表示访问检查已失败且将避开所有后续检查。如果提交者已经与 LDAP_AUTH_URL 匹配，则将避开此检查。可具有多个值，并允许使用全局样式通配符。
mgrpAllowedBroadcaster	(LDAP_AUTH_URL) 标识邮件地址的 URL 允许将邮件发送到该组中。可具有多个值。每个 URL 都扩展为地址列表，并针对当前信封 From: 地址检查每个地址。 OR_CLAUSES MTA 设置为 0 （默认值）时匹配失败，表明访问检查已失败且将避开所有后续测试。 OR_CLAUSES MTA 设置为 1 时匹配失败，将设置 “失败暂挂”标志；其他允许的访问检查必须都成功才能使访问检查成功。出现匹配还将禁用后续的域访问检查。执行的扩展类似于禁用所有访问控制检查的 SMTP EXPN。
mgrpDisallowedBroadcaster	(LDAP_CANT_URL) 标识邮件地址的 URL 不允许将邮件发送到该组中。可具有多个值。每个 URL 都扩展为地址列表，并针对当前信封 From: 地址检查每个地址。出现匹配就表示访问检查已失败且将避开所有后续检查。执行的扩展类似于禁用所有访问控制检查的 SMTP EXPN。
mgrpMsgMaxSize	(LDAP_ATTR_MAXIMUM_MESSAGE_SIZE) 可以发送给组的最大邮件大小 （以字节为单位）。该属性作废，但仍支持向下兼容性；而应该使用新的 mailMsgMaxBlocks 属性。
mgrpAuthPassword	(LDAP_AUTH_PASSWORD) 指定发送到列表所需的密码。mgrpAuthPassword 属性的出现将强制执行重新处理传送。邮件被重新排入到重新处理通道时，将从标题中获取密码并把密码放置在信封中。然后，在进行重新处理时，将从信封中获取密码并针对该属性检查密码。另外，只能从标题字段中删除实际使用的密码。 OR_CLAUSES MTA 选项将按照其操作其他访问检查属性的同一种方法来操作此属性。
mgrpModerator	(LDAP_MODERATOR_URL) 该属性给出的 URL 列表扩展为一系列地址。该地址列表的解释取决于 LDAP_REJECT_ACTION MTA 选项的设置。如果将 LDAP_REJECT_ACTION 设置为 TOMODERATOR，该属性将邮件要发送到的中介人地址指定为所有访问检查都应失败。如果缺少 LDAP_REJECT_ACTION 或具有任何其他值，则将地址列表与信封源地址相比较。如果出现匹配，处理将继续进行。如果未出现匹配，则邮件将被重新发送到该属性所指定的所有地址。通过将属性的值设为组的 URL 列表，可以实现该属性的扩展。清除与该组相关联的 RFC822 地址或 DN 的所有列表，并将该组的传送选项设置为 members。最后，忽略该表中列出的后续组属性。
mgrpDeliverTo	(LDAP_GROUP_URL1) 扩展 URL 列表时，该列表将提供邮递列表成员地址的列表。
memberURL	(LDAP_GROUP_URL2) 扩展 URL 的另一个列表时，该列表将提供邮递列表成员地址的另一个列表。
uniqueMember	(LDAP_GROUP_DN) 组成员 DN 的列表。 DN 可以指定整个子树。通过将唯一成员 DN 嵌入到 LDAP URL 中可以扩展这些 DN。要使用的确切 URL 由 GROUP_DN_TEMPLATE MTA 选项指定。此选项的默认值为：ldap:///$A?mail?sub?(mail=*) $A 指定了 uniqueMember DN 的插入点。
mgrpRFC822MailMember	(LDAP_GROUP_RFC822) 该列表的成员的邮件地址。

表 9-9 组扩展默认属性和用于设置属性名称的 MTA 选项 （续）

默认属性	（用于设置属性名称的 MTA 选项）处理属性的方法
rfc822MailMember	(LDAP_GROUP_RFC822) rfc822MailMember 支持向下兼容性。 rfc822MailMember 或 mgrpRFC822MailMember （但不能同时）可以用于任何给定组。
mgrpErrorsTo	(LDAP_ERRORS_TO) 将信封创始者 (MAIL FROM) 地址设置为属性指定的内容。
mgrpAddHeader	(LDAP_ADD_HEADER) 将在属性中指定的标题变为标题剪裁 ADD 选项。
mgrpRemoveHeader	(LDAP_REMOVE_HEADER) 将指定的标题变为标题剪裁 MAXLINES=-1 选项。
mgrpMsgPrefixText	(LDAP_PREFIX_TEXT) 将指定的文本添加到邮件文本 （如果有）的开头。
mgrpMsgSuffixText	(LDAP_SUFFIX_TEXT) 将指定的文本添加到邮件文本 （如果有）的结尾。
No Default	(LDAP_ADD_TAG) 检查指定文本的主题；如果没有主题，将把文本添加到主题字段的开头。

在组扩展作为 SMTP EXPN 命令一部分的特殊情况下，将检查一个最终属性：mgmanMemberVisibility 或可扩展。 LDAP_EXPANDABLE MTA 选项可用于选择不同的属性来进行检查。可能的值包括：anyone，表示任何人都可以扩展组； all 或 true，表示用户必须先通过 SASL 成功验证后才允许扩展； none，表示不允许扩展。不可识别的值被解释为 none。如果不存在该属性， EXPANDABLE_DEFAULT MTA 选项将控制是否允许扩展。

以此方式缓存的别名条目类似于域条目。控制别名高速缓存的 MTA 选项为 ALIAS_ENTRY_CACHE_SIZE （默认值为 1000 个条目）和 ALIAS_ENTRY_CACHE_TIMEOUT （默认值为 600 秒）。给定别名的整个 LDAP 返回值保留在高速缓存中。

条目的负缓存由 ALIAS_ENTRY_CACHE_NEGATIVE MTA 选项控制。非零值启用别名匹配的缓存失败。零值将其禁用。默认情况下，禁用别名条目的负缓存。理论上可以重复说明无效地址，实际上不可能经常发生。此外，负缓存可能会影响及时识别已添加到目录中的新用户。但是，在频繁使用虚名域的情况下，站点应该考虑重新启用别名的负缓存。由 ALIAS_URL0 中指定的 URL 执行的搜索不可能会成功。

地址反向

使用直接 LDAP 的地址反向以 USE_REVERSE_DATABASE 值 4 开始，该值禁用所有反向数据库。然后，它将构建于先前讨论过的路由设备上。特别是，在以前的版本中，它以反向 URL 说明的格式开始：

```
REVERSE_URL=ldap:///$V?mail?sub?$Q
```

The $V 元字符已在别名 URL 的上下文中进行了介绍。但是， $Q 元字符 （在功能上与在别名 URL 中使用的 $R 元字符非常类似）专用于地址反向。与 $R 不同，它会生成一个过滤器，该过滤器搜索包含地址 （为地址反向的候选项）的属性。要搜索的属性的列表来自 MTA 选项 LDAP_MAIL_REVERSES。如果未设置该选项，将检查 local.imta.schematag configutil 参数，并根据该参数的值选择一组相应的默认属性。

表 9-10 显示了所选择的 local.imta.schematag 值和默认属性。

表 9-10 local.imta.schematag 值和属性

模式标记值	属性
sims40	mail,rfc822mailalias
nms41	mail,mailAlternateAddress
ims50	mail,mailAlternateAddress

但是，使用 $Q 将不再适合。为了使邮件捕获和其他功能可以正常工作，已增强了地址反向功能以注意除了出现匹配的事实之外所匹配的属性。这表示 $R 应该用于指定过滤器而不是 $Q。此外，还添加了 $N 元字符，该字符将返回地址反向感兴趣的属性的列表。得到的选项值为：

```
REVERSE_URL=ldap:///$V?$N?sub?$R
```

通常， local.imta.schematag 可以为以逗号分隔的列表。如果支持多种模式，则使用消除了复制功能的属性的组合列表。

此外，过滤器不但搜索原来提供的地址，而且还搜索具有相同本地部分实际上是在域树 （保存在第 182 页的步骤 2 中）中找到域的地址。域树查找的重复性意味着两个地址可能不同。

例如，假定域 siroe.com 显示在域树中，并且 MTA 查找地址：

```
u@host1.siroe.com
```

扩展 $R 和 ims50 schematag 得到的过滤器将类似于：

```
(|(mail=u@siroe.com)
(mail=u@host1.siroe.com)
(mailAlternateAddress=u@siroe.com)
(mailAlternateAddress=u@host1.siroe.com)
(mailEquivalentAddress=u@siroe.com)
(mailEquivalentAddress=u@host1.siroe.com))
```

请注意，反向 URL 明确指定该属性包含规范的地址。通常，该属性将是邮件属性。

构建 URL 之后，将执行 LDAP 搜索。如果搜索成功，返回的第一个属性值将替换原始地址。如果搜索不成功或出现错误，则保留原始地址不变。

由于执行地址反向操作的频率，特别是给出可以显示在邮件标题中的一系列地址，以及目录查询所涉及的损耗，因此负和正结果都需要被缓存。使用内存中的开放链的动态扩展散列表可以实现此操作。通过 REVERSE_ADDRESS_CACHE_SIZE MTA 选项（默认值为 100000）可以设置高速缓存的最大大小，通过 REVERSE_ADDRESS_CACHE_TIMEOUT MTA 选项 （默认值为 600 秒）可以设置高速缓存中的条目的超时值。高速缓存实际上存储地址本身，而不存储 LDAP URL 和 LDAP 结果。

异步 LDAP 操作

异步查找无需在内存中存储完整的大量 LDAP 结果，从而避免在一些情况下可能出现的性能问题。 MTA 提供了通过 MTA 异步完成执行各种类型的查找的能力。

使用异步 LDAP 查找由 MTA 选项 LDAP_USE_ASYNC 来控制。此选项是按位编码的值。每一位 （如果设置）可结合 MTA 中具体的 LDAP 使用方法来进行 LDAP 异步查找。

表 9-11 显示了 option.dat 文件中的 LDAP_USE_ASYNC MTA 选项的位和值设置。

表 9-11 LDAP_USE_ASYNC MTA 选项的设置

位	值	LDAP 的具体使用
0	1	LDAP_GROUP_URL1 (mgrpDeliverTo) URL
1	2	LDAP_GROUP_URL2 (memberURL) URL
2	4	LDAP_GROUP_DN (UniqueMember) DN
3	8	auth_list、moderator_list、sasl_auth_list 和 sasl_moderator_list 非位置列表参数 URL
4	16	cant_list 和 sasl_cant_list 非位置列表参数 URL
5	32	originator_reply 非位置列表参数 URL
6	64	deferred_list、direct_list、hold_list 和 nohold_list 非位置列表参数 URL
7	128	username_auth_list、username_moderator_list、username_cant_list 非位置列表参数 URL
8	256	别名文件列表 URL
9	512	别名数据库列表 URL

表 9-11 LDAP_USE_ASYNC MTA 选项的设置 （续）

位	值	LDAP 的具体使用
10	1024	LDAP_CANT_URL (mgrpDisallowedBroadcaster) 外层 URL
11	2048	LDAP_CANT_URL 内层 URL
12	4096	LDAP_AUTH_URL (mgrpAllowedBroadcaster) 外层 URL
13	8192	LDAP_AUTH_URL 内层 URL
14	16384	LDAP_MODERATOR_URL (mgrpModerator) URL

LDAP_USE_ASYNC MTA 选项的默认值为 0，表示默认情况下禁用异步 LDAP 查找。

设置摘要

为了启用直接 LDAP，需要设置以下 MTA 选项：

```
ALIAS_MAGIC=8764
ALIAS_URL0=ldap:///$V?*?sub?$R
USE_REVERSE_DATABASE=4
USE_DOMAIN_DATABASE=0
REVERSE_URL=ldap:///$V?mail?sub?$Q
```

如果要支持虚名域，必须设置以下附加选项：

```
DOMAIN_MATCH_URL=ldap:///$B?msgVanityDomain?sub?(msgVanityDomain=$D)
ALIAS_URL1=ldap:///$B?*?sub?(&(msgVanityDomain=$D)$R)
ALIAS_URL2=ldap:///$1V?*?sub?(mailAlternateAddress=@$D)
```

请注意，这些选项中的最后一个选项还处理托管域以及虚名域中的通配符的本地部分的情况。如果需要支持通配符的本地部分，但不需要支持虚名域，则应该使用以下选项：

```
ALIAS_URL1=ldap:///$V?*?sub?&(mailAlternateAddress=@$D)
```

需要将 filter ssrd:$A 子句从 MTA 配置文件 (imta.cnf) 中的 ims-ms 通道定义中删除。

第 10 章

关于 MTA 服务和配置

本章介绍常规的 MTA 服务和配置。其他章节中包含更具体和详细的说明。其中包含以下各节：

- 第 206 页的 “编译 MTA 配置”
- 第 206 页的 “MTA 配置文件”
- 第 208 页的 “映射文件”
- 第 220 页的 “其他 MTA 配置文件”
- 第 231 页的 “别名”
- 第 233 页的 “命令行实用程序”
- 第 233 页的 “SMTP 安全性和访问控制”
- 第 233 页的 “日志文件”
- 第 234 页的 “将地址由内部格式转换为公用格式”
- 第 240 页的 “控制传送状态通知邮件”
- 第 252 页的 “控制邮件处理通知”

编译 MTA 配置

修改了 MTA 配置文件 （例如 imta.cnf、 mappings、 aliases 或 option.dat）之后，必须使用 imsimta refresh 命令重新编译配置 （请参见 Sun Java System Messaging Server Administration Reference）。此命令将配置文件编译成共享内存 （在 UNIX 上）或动态链接库 (NT) 中的单个映像。

经过编译的配置中包含静态和动态可重新装入的部分。如果动态部分被更改，并且运行 imsimta reload，则正在运行的程序将重新装入动态数据。动态部分为映射表、别名和查找表。

编译配置信息的主要原因是为了提高性能。使用经过编译的配置的另一个功能是可以更方便地测试配置更改，因为当经过编译的配置处于使用状态时，配置文件本身并不是 “活动的”。

当 MTA 组件 （例如通道程序）必须读取配置文件时，它首先会查看经过编译的配置是否存在。如果存在，则将映像附加到正在运行的程序。如果映像附加操作失败，则 MTA 会返回使用原先读取文本文件的方法。

MTA 配置文件

主 MTA 配置文件为 imta.cnf。默认情况下，此文件位于 *msg_svr_base*/config/imta.cnf。此文件包含 MTA 通道定义及通道重写规则。与重写目标地址关联的通道成为目标通道。该系统使用默认的 imta.cnf 时，通常会运行良好。

本节简要介绍了 MTA 配置文件。有关配置构成 MTA 配置文件的重写规则和通道定义的详细信息，请参见第 11 章 “配置重写规则”和第 12 章 “配置通道定义”。

通过修改 MTA 配置文件，可以建立在站点中使用的通道，并且可以通过重写规则确定哪些通道负责哪类地址。配置文件通过指定可用的传输方法 （通道）及将地址类型与相应的通道关联的传输路线 （重写规则），建立电子邮件系统的布局。

配置文件由两部分组成：域重写规则和通道定义。域重写规则最先显示在文件中，并由空行与通道定义分隔开。通道定义统称为通道表。一个单独的通道定义构成一个通道块。

以下 imta.cnf 配置文件示例显示了如何使用重写规则将邮件路由到正确的通道。其中不使用域名，以尽可能使其简化。重写规则显示在配置文件的上半部分，下半部分是通道定义。

```
! test.cnf - An example configuration file. (1)
!
! This is only an example of a configuration file. It serves
! no useful purpose and should not be used in a real system.
!
! Part I: Rewrite rules
a     $U@a-daemon (2)
b     $U@b-daemon
c     $U%c@b-daemon
d     $U%d@a-daemon
            (3)
! Part II: Channel definitions
l              (4)
local-host

a_channel defragment charset7 usascii (5)
a-daemon

b_channel noreverse notices 1 2 3
b-daemon

</opt/SUNWmsgsr/msg-tango/table/internet.rules (6)
```

下表说明了先前配置文件中的关键项 （标有黑体数字，括在括号中）：

1. 感叹号 (!) 用于包含注释行。感叹号必须显示在第一列。显示在其他任何位置的感叹号均被当作**文字**感叹号。
2. 重写规则显示在配置文件的上半部分。重写规则的行间不能出现空行。允许出现具有注释的行 （以第一列中的感叹号开始）。
3. 文件中显示的第一个空行表示重写规则部分的结束和通道块的开始。这些定义统称为**通道主机表**，用于定义 MTA 可以使用的通道和与每个通道关联的名称。
4. 显示的第一个通道块通常是本地通道或 l 通道。然后空行将各个通道块彼此分隔开。（defaults 通道例外，它可以出现在 l 通道之前）。
5. 典型的通道定义由通道名称 (a_channel)、定义通道配置的若干关键字 (defragment charset7 usascii) 以及也被称为**通道标记**的路由系统 (a-daemon) 组成。

6. 配置文件中可以包含其他文件的内容。如果第一列的某一行中包含小于号 (<)，则该行中的剩余内容被视为文件名；文件名应始终为绝对和完整文件路径。打开文件时，在该点将其内容并入配置文件。包含的文件最多可以嵌套三层。配置文件中包含的所有文件必须与配置文件一样，可由所有人读取。

表 10-1 显示了先前的配置如何路由某些示例地址。

表 10-1 地址和关联的通道

地址	排队到通道
u@a	a_channel
u@b	b_channel
u@c	b_channel
u@d	a_channel

有关 MTA 配置文件的更多信息，请参阅第 174 页的 “重写规则”，第 177 页的 “通道定义”和第 11 章 “配置重写规则”。

注 只要更改了 imta.cnf 文件，就必须重新编译 MTA 配置。请参见第 206 页的 “编译 MTA 配置”。

映射文件

MTA 的许多组件都使用面向表查找的信息。这类表用来将输入字符串转换 （即，**映射**）为输出字符串。这类表称为**映射表**，通常显示为两列。第一 （左边的）列提供对其进行匹配的可能输入字符串 （模式），第二 （右边的）列给出了映射输入字符串的结果输出字符串 （模板）。

大多数 MTA 数据库 — 包含不同类型的 MTA 数据，并且不应与映射表混淆的数据库 — 都是此类表的实例。但是， MTA 数据库文件不具备通配符查找功能，因为其具有内在局限性，必须要扫描整个数据库才能找到匹配的通配符。

MTA 映射文件支持多个映射表。它具备通配符功能以及多步和迭代映射方法。此方法的计算量比使用数据库要大，特别是条目很多时。但是，其灵活性带来的好处是您不需要等效数据库中的大多数条目，从而可能使总体开销较低。

映射表保存在 MTA mappings 文件中。这是使用 MTA tailor 文件中的 IMTA_MAPPING_FILE 选项指定的文件。默认情况下，该文件为 *msg_svr_base*/config/mappings。mappings 文件的内容将作为可重新装入的部分并入经过编译的配置中 （请参见第 206 页的 “编译 MTA 配置”）。mappings 文件应该可以由所有人读取。如果无法让所有人都能读取，则将导致错误行为。只要更改了 mappings 文件，就必须重新编译 MTA 配置。请参见第 206 页的 “编译 MTA 配置”。

表 10-2 列出了本指南中所介绍的映射表。

表 10-2 Messaging Server 映射表

映射表	页	说明
AUTH_REWRITE	316	与 authrewrite 关键字配合使用，以使用从验证操作 (SASL) 中获得的寻址信息修改标题和信封地址。
CHARSET-CONVERSION	383	用于指定应该执行哪些类型的通道到通道字符集转换和邮件重新格式化。
COMMENT_STRINGS	334	用于修改地址标题注释 （括在括号中的字符串）。
CONVERSIONS	367	用于为转换通道选择邮件通信。
FORWARD	237	用于执行转发，与使用别名文件或别名数据库执行的转发类似。
FROM_ACCESS	457	用于基于信封源地址过滤邮件。如果 To 地址是不相关的地址，请使用该表。
INTERNAL_IP	470	用于识别内部系统和子网。
MAIL_ACCESS	457	用于根据 SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息阻塞外来的连接。
NOTIFICATION_LANGUAGE	240	用于自定义或本地化通知邮件。
ORIG_MAIL_ACCESS	457	用于根据 ORIG_SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息阻塞外来的连接。
ORIG_SEND_ACCESS	457	用于根据信封源地址、信封目标地址、源通道和目标通道阻塞外来的连接。
PERSONAL_NAMES	335	用于修改个人名称 （尖括号分隔的地址前的字符串）。
PORT_ACCESS	457	用于根据 IP 编号阻塞外来的连接。
REVERSE	234	用于将地址从内部格式转换为公用的公布格式。
SEND_ACCESS	457	用于根据信封源地址、信封目标地址、源通道和目标通道阻塞外来的连接。
*SMS_Channel*_TEXT	783	用于站点定义的文本转换。
X-ATT-NAMES	375	用于从映射表中检索参数值。
X-REWRITE-SMS-ADDRESS	782	用于本地 SMS 地址有效性检查。

映射文件中的文件格式

mappings 文件由一系列单独的表组成。每个表的开头都是表名称。名称在第一列中始终为字母字符。表名称后面必须有一个空行，然后是表中的条目。条目由零个或多个缩进行组成。每个条目行包含两列，由一个或多个空格或制表符分隔。条目中的所有空格都必须用 $ 字符括起。每个映射表之后以及各映射表之间必须有一个空行；单个表中的条目之间不允许出现空行。注释用第一列中的感叹号 (!) 表示。

结果格式与以下格式类似：

```
TABLE1_NAME

    pattern1-1      template1-1
    pattern1-2      template1-2
    pattern1-3      template1-3
        .               .
        .               .
        .               .
    pattern1-n      template1-n

TABLE2_NAME

    pattern2-1      template2-1
    pattern2-2      template2-2
    pattern2-3      template2-3
        .               .
        .               .
        .               .
    pattern2-n      template2-n

            .
            .
            .

TABLE3_NAME

            .
            .
            .
```

使用映射表 TABLE2_NAME 的应用程序会将字符串 pattern2-2 映射为由 template2-2 指定的任何内容。每种模式或模板最多可以包含 252 个字符。映射中可以显示的条目数量没有限制 （尽管条目数量过多可能会消耗大量的 CPU 资源，并且会消耗过多的内存）。较长的行 （超过 252 个字符）可以使用反斜杠 (\) 结束，以在下一行继续。两列之间及第一列之前的空格不可省略。

mappings 文件中不允许出现重复的映射表名称。

将其他文件包含到映射文件中

可以将其他文件包含到 mappings 文件中。这可以通过以下格式的行来实现：

```
<file-spec
```

它可以有效地使文件 file-spec 的内容替换到 mappings 文件中包内容出现的位置。文件规范应指定一个完整文件路径 （目录等）。以此方式包括的所有文件都必须可由所有用户读取。此类包括的 mappings 文件中还允许具有注释。包括最多可以嵌套三层。装入 mappings 文件的同时会装入包括的文件 — 它们不是按需装入的，因此使用包括的文件时不涉及性能或内存节约。

映射操作

mappings 文件中的所有映射都以一致的方式应用。从一个映射到下一个映射的唯一变化就是输入字符串的源和映射输出的用途。

映射操作始终以输入字符串和映射表开始。按照条目在映射表中显示的顺序，从上到下每次扫描一个条目。每个条目的左侧都用作模式，并使用该模式以不区分大小写的方式比较输入字符串。

映射条目模式

模式可以包含通配符。特别地，允许使用通常的通配符：星号 (*) 匹配零个或多个字符，每个百分比符号 (%) 匹配一个字符。可以在星号、百分比符号、空格和制表符前加一个美元符号 ($) 来引用它们。引用星号或百分比符号将使其不具有特殊意义。必须引用空格和制表符以防止它们过早地结束模式或模板。文字美元符号字符应该采用双写的形式 ($$)，第一个美元符号引用第二个美元符号。

表 10-3 映射模式通配符

通配符	**说明**
%	只匹配一个字符。
*	匹配零个或多个字符，最长 （或最多）可匹配从左至右的全部字符
向后匹配	**说明**
$ n*	匹配第 n 个通配符或全局通配符。
修饰符	**说明**
$_	使用最少或 “最短”的从左至右匹配。
$@	关闭后续通配符或全局通配符的 “保存”。
$^	打开后续通配符或全局通配符的 “保存”；这是默认设置。
全局通配符	**说明**
$A%	匹配一个字母字符 （A-Z 或 a-z）。
$A*	匹配零或多个字母字符 （A-Z 或 a-z）。
$B%	匹配一个二进制数字 （0 或 1）。
$B*	匹配零个或多个二进制数字 （0 或 1）。
$D%	匹配一个十进制数字 (0-9)。
$D*	匹配零个或多个十进制数字 (0-9)。
$H%	匹配一个十六进制数字 （0-9 或 A-F）。
$H*	匹配零个或多个十六进制数字 （0-9 或 A-F）。
$O%	匹配一个八进制数字 (0-7)。
$O*	匹配零个或多个八进制数字 (0-7)。
$S%	匹配一个符号集字符 （例如， 0-9、 A-Z、 a-z、 _、 $）。
$S*	匹配零个或多个符号集字符 （即 0-9、 A-Z、 a-z、 _、 $）。
$T%	匹配一个制表符或垂直制表符，或空格字符。
$T*	匹配零个或多个制表符或垂直制表符，或空格字符。
$X%	$H% 的同义词。
$X*	$H* 的同义词。
$[c]%	匹配字符 c。
$[c]*	匹配任意出现的字符 c。
$[c_1 c_2 ... c_n]%	只匹配 c_1、 c_2 或 c_n 中出现的一个字符。
$[c_1 c_2 ... c_n]*	匹配 c_1、 c_2 或 c_n 中出现的任意字符。

表 10-3 映射模式通配符 （续）

$[c_1 -c_n]%	匹配 c_1 到 c_n 范围内的任一字符。
$[c_1 -c_n]*	匹配 c_1 到 c_n 范围内出现的任意字符。
$< IPv4>	匹配一个 IPv4 地址 （忽略位）。
$(IPv4)	匹配一个 IPv4 地址 （保留前缀位）。
${IPv6}	匹配一个 IPv6 地址。

在全局结构内 （即 `$[...]` 结构内）反斜杠字符 \ 是引用字符。要表示文字连字符 - 或右方括号]，则在全局结构内必须用反斜杠引用连字符或右方括号。

模式中的所有其他字符仅表示并匹配自身。特别地，在映射模式或模板中，单引号和双引号字符以及括号都没有特殊意义，它们只是一些普通的字符。这样一来，便很容易写入与非法地址或部分地址对应的条目。

要指定多个修饰符或指定修饰符和向后匹配，语法中只能使用一个美元字符。例如，要向后匹配初始通配符，而不保存向后匹配自身，则使用 $@0，而不是 $@$0。

注意， `imsimta test -match` 实用程序可用于测试映射模式，尤其是测试模式中的通配符行为。

星号通配符通过从左至右处理模式，最大程度地匹配字符。例如，将字符串 `a/b/c` 与模式 `*/*` 进行比较时，左边的星号与 `a/b` 匹配，右边的星号匹配剩余部分 `c`。

`$_` 修饰符使得通配符匹配最小化，将最小匹配看作匹配，从左到右处理模式。例如，将字符串 `a/b/c` 与模式 `$_*/$_*` 进行比较时，左边的 `$_*` 匹配 `a`，右边的 `$_*` 匹配 `b/c`。

IP 匹配

使用 IPv4 前缀匹配，要指定 IP 地址或子网，后跟斜杠和距离前缀的位数 （可选），在比较匹配时，位数很重要。例如，以下行匹配 `123.45.67.0` 子网中的所有地址：

```
$(123.45.67.0/24)
```

使用 IPv4 忽略位匹配，要指定 IP 地址或子网，后跟斜杠或检查匹配时忽略的位数（可选）。例如，以下行匹配 `123.45.67.0` 子网中的所有地址：

```
$<123.45.67.0/8>
```

以下示例匹配 `123.45.67.4` 到 `123.45.67.7` 范围中的所有地址：

```
$<123.45.67.4/2>
```

IPv6 匹配匹配一个 IPv6 地址或子网。

映射条目模板

如果给定条目中的模式比较失败，则不执行任何操作，继续扫描下一个条目。如果比较成功，条目的右侧将用作模板以生成输出字符串。该模板会将输入字符串有效地替换为根据模板给出的说明构造的输出字符串。

模板中几乎所有的字符都只是在输出中生成它们自身。只有美元符号 ($) 例外。

美元符号后跟美元符号、空格或制表符将在输出字符串中生成美元符号、空格或制表符。注意，必须引用所有这些字符串，才能将其插入输出字符串中。

美元符号后跟数字 *n* 代表替换，美元符号后跟字母字符被称为 “元字符”。元字符本身并不显示在由模板生成的输出字符串中，而是生成一些特殊的替换或处理。有关特殊替换和标准处理元字符的列表，请参见表 10-4。所有其他的元字符都保留用于特定于映射的应用程序。

注意，任意一个元字符 `$C`、`$E`、`$L` 或 `$R` 出现在匹配模式的模板中时，都会影响映射进程并控制进程是终止还是继续。即，可以设置迭代映射表条目，使一个条目的输出成为另一个条目的输入。如果匹配模式的模板不包含任一元字符 `$C`、`$E`、`$L` 或 `$R`，则假设为 `$E` （立即终止映射进程）。

为防止无限循环，将限制通过映射表的迭代数量。每次重新启动通过的字符串 （长度等于或大于上一个通过的字符串）时，计数器的数量都会增加。如果该字符串的长度比上一个字符串短，则系统会将计数器重置为零。计数器超过 10 以后，将不接受重新迭代映射的请求。

表 10-4 映射模板替换和元字符

替换序列	替换
`$n`	从 0 开始从左至右计数的第 *n* 个通配符字段。
`$#...#`	序列号替换。
$]...[	LDAP 搜索 URL 查找；在结果中替换。
`$|...|`	将指定的映射表应用于所提供的字符串。
${...}	常规的数据库替换。
$}*domain*,*attribute*{	添加该功能以访问基于域的属性。 *domain* 是有问题的域， *attribute* 是与该域相关联的属性。如果该域存在并具有属性，则它的初始值将被替换为映射结果；如果属性或域两者中有一个不存在，则映射条目将失败。 *attributes* 可以为域 LDAP 属性或为下面定义的特殊属性： `_base_dn_` — 域中用户条目的基本 DN `_domain_dn_` — 域条目自身的 DN `_domain_name_` — 域名 （与之相对的是别名） `_canonical_name_` — 与域相关联的规范名称
`$[...]`	调用由站点提供的例程；在结果中替换。

表 10-4 映射模板替换和元字符 （续）

替换序列	替换
元字符	**说明**
$C	从下一个表条目开始继续执行映射进程；将此条目的输出字符串用作映射进程的新的输入字符串。
$E	立即结束映射进程；将此条目的输出字符串用作映射进程的最终结果。
$L	从下一个表条目开始继续执行映射进程；将此条目的输出字符串用作新的输入字符串；表中所有条目都耗尽之后，从第一个表条目开始再执行一次传递。后续的匹配可以用 $C、 $E 或 $R 元字符覆盖此条件。
$R	从映射表的第一个条目开始继续执行映射进程；将此条目的输出字符串用作映射进程的新的输入字符串。
$nA	插入从位置 0 开始的当前地址左侧第 n 个字符，如果省略 n，则将插入整个地址。
$nX	插入从 0 开始的邮件主机左侧第 n 个组件，如果省略 n，则将插入整个邮件主机。
$?x?	映射条目百分之 x 的时间成功。
$\	强制后续文本为小写。
$^	强制后续文本为大写。
$_	使后续文本保留其原有大小写形式。
$=	强制后续替换字符经适当引用插入到 LDAP 搜索过滤器中。材料为大写。
$:*x*	仅在设置了指定的标志后才匹配。
$;*x*	仅在清除了指定的标志后才匹配。

通配符字段替换 *($n)*

后跟数字 n 的美元符号将被替换为与模式中的第 *n* 个通配符匹配的内容。通配符从 0 开始编号。例如，以下条目将匹配输入字符串 PSI%A::B 并生成结果输出字符串 b@a.psi.siroe.com:

```
PSI$%*::*     $1@$0.psi.siroe.com
```

输入字符串 PSI%1234::USER 也将匹配，并生成 USER@1234.psi.siroe.com 作为输出字符串。输入字符串 PSIABC::DEF 不会匹配此条目中的模式，也不执行任何操作，即，不会从此条目生成输出字符串。

控制文本的大小写 *($\, $^, $_)*

元字符 $\ 强制后续文本为小写，$^ 强制后续文本为大写，$_ 使后续文本保留其原先的大小写。例如，使用映射对区分大小写的地址进行转换时，这些元字符可能会十分有用。

进程控制 *($C, $L, $R, $E)*

$C、 $L、 $R 和 $E 元字符可以影响映射进程，控制是否终止以及何时终止映射进程。元字符：

- $C 使映射进程继续处理下一个条目，将当前条目的输出字符串用作映射进程的新的输入字符串。
- $L 使映射进程继续处理下一个条目，将当前条目的输出字符串用作映射进程的新的输入字符串，并且如果没有找到映射条目，则从第一个表条目开始在表中再次进行传递。具有 $C、 $E 或 $R 元字符的后续匹配条目将覆盖此条件。
- $R 使映射进程从表的第一个条目开始继续执行，将当前条目的输出字符串用作映射进程的新的输入字符串。
- $E 使映射进程终止，此条目的输出字符串为最终输出。 $E 为默认值。

映射表模板是从左到右进行扫描的。要为可能 “成功” 也可能 “失败” 的条目（例如，常规数据库替换或随机值控制的条目）设置 $C、$L 或 $R 标志，请将 $C、$L 或 $R 元字符置于可能成功也可能失败的条目部分的左侧，否则，如果条目的剩余部分失败，则不显示标志。

检查特殊标志

某些映射探测设置了特殊标志。这些标志可以设置，并可以使用 $:, $; 测试的常规映射表功能进行存在 / 不存在测试。 $:x 使条目仅在设置了标志 x 的情况下匹配。 $;x 使条目仅在清除标志 x 的情况下匹配。有关可以应用于该表的任何特殊标志，请参见特定映射表说明。（请参见表 17-2 第 458 页中的 $A、 $T、 $S、 $F 和 $D。）

如果希望在标志检查成功时条目应成功并终止，而在标志检查失败时映射进程应继续，则条目应在标志检查的左侧使用 $C 元字符，在标志检查的右侧使用 $E 标志。

条目随机成功或失败 *($?x?)*

映射表条目中的元字符 $?x? 使该条目的 “成功” 时间达到百分之 *x* ；剩余时间内条目 “失败”，并且将映射条目以原样输出。（注意，取决于映射，条目失败的效果不一定与首先不匹配的条目相同。） *x* 应该是一个指定成功百分比的真实数字。

例如，假设 IP 地址为 123.45.6.78 的系统向您的站点发送了太多的 SMTP 电子邮件，您希望使其放慢速度，您可以以下方式使用 PORT_ACCESS 映射表。假设您只允许 25% 的连接尝试，拒绝剩余 75% 的连接尝试。以下 PORT_ACCESS 映射表使用 $?25? 使具有 $Y （接受连接）的条目仅在 25% 的时间内成功；在剩余 75% 的时间内，当此条目失败时，该条目上初始的 $C 将使 MTA 继续从下一个条目执行映射，导致连接尝试被拒绝，同时显示 SMTP 错误和消息：Try again later （请稍后重试）。

```
PORT_ACCESS

  TCP|*|25|123.45.6.78|*          $C$?25?$Y
  TCP|*|25|123.45.6.78|*          $N45s$ 4.40$ Try$ again$ later
```

序列号替换 *($#...#)*

$#...# 替换会增加 MTA 序列文件中存储的值并将该值替换为模板。当映射表输出中需要有唯一的限定符时，则可以使用此模板生成唯一的递增字符串，例如，使用映射表生成文件名时。

允许使用以下语法形式中的任何一种：

$#*seq-file-spec*|*radix*|*width*|*m*#

$#*seq-file-spec*|*radix*|*width*#

$#*seq-file-spec*|*radix*#

$#*seq-file-spec*#

必需的 *seq-file-spec* 参数是已有的 MTA 序列文件的完整文件规范。可选的 *radix* 和 *width* 参数将分别指定用于输出序列值的基数 （基）和输出的位数。默认的基数为 10。基数也可以在范围 -36 到 36 之间，例如，基数 36 给出由数字 0 到 9、A 到 Z 表示的值。默认情况下，序列值以原有宽度打印，但是如果指定的宽度代表更大的位数，则输出结果的左边将用 0 补齐，从而获得正确的位数。注意，如果明确指定了宽度，则必须同时明确指定基数。

可选的 *m* 参数是模量。如果指定了第四个参数，则插入的值是从文件模量 *m* 中检索到的序列号。默认情况下，不执行任何模量操作。

如上所述，映射中所引用的 MTA 序列文件必须已存在。要创建 MTA 序列文件，请使用以下 UNIX 命令：

```
touch seq-file-spec
```

或

```
cat >seq-file-spec
```

使用映射表访问的序列号文件必须可由所有人读取，才能保证正确操作。您还必须具有 MTA 用户帐户 （在 imta_tailor 文件中配置为 nobody）才能使用这类序列号文件。

LDAP 查询 *URL* 替换， *$]...[*

$]*ldap-url*[格式的替换是特殊处理的。 *ldap-url* 被翻译为 LDAP 查询 URL，并且该 LDAP 查询的结果将被替换。使用标准的 LDAP URL 时，会省略主机和端口，主机和端口是使用 LDAP_HOST 和 LDAP_PORT 选项指定的。即，应将 LDAP URL 指定为：

ldap:///*dn*[?*attributes*[?*scope*?*filter*]]

其中，以上显示的方括号字符 [和] 表示 URL 的可选部分。 *dn* 是必需的独特名称，用于指定搜索基准。 URL 可选的 *attributes*、*scope* 和 *filter* 部分进一步完善了要返回的信息。即， *attributes* 指定要从匹配此 LDAP 查询的 LDAP 目录条目中返回的属性。 *scope* 可以是 base （默认）、one 或 sub 中的任何一个。 *filter* 描述了匹配条目的特征。

某些 LDAP URL 替换序列可以在 LDAP 查询 URL 中使用。

映射表替换 *($|...|)*

$|*mapping*;*argument*| 格式的替换是特殊处理的。 MTA 在 MTA mappings 文件中查找名为 *mapping* 的辅助映射表，并使用 *argument* 作为该命名的辅助映射表的输入。该命名的辅助映射表必须存在，并且必须在其输出中设置了 $Y 标志 （如果成功）；如果命名的辅助映射表不存在，或没有设置 $Y 标志，则该辅助映射表替换将失败，并且原始的映射条目也将被看作失败：原始的输入字符串将被用作输出字符串。

请注意，当您要在执行映射表替换的映射表条目中使用进程控制元字符 （例如 $C、$R 或 $L）时，应将进程控制元字符置于映射表模板中的映射表替换的左侧；否则，如果映射表替换 “失败”，则意味将不显示进程控制元字符。

常规查找表或数据库替换 *(${...})*

${*text*} 格式的替换是特殊处理的。 *text* 部分用作访问常规查找表或数据库的密钥。数据库是使用 imsimta crdb 实用程序生成的。如果在表中找到了 *text*，则将替换表中对应的模板。如果 *text* 与表中的条目都不匹配，则输入字符串将原样用作输出字符串。

如果您使用的是常规查找表，则需要设置低顺序位的 MTA 选项 use_text_databases。即，将其设置为奇数。需要将对 general.txt 的更改编译到 MTA 配置中 （使用 imsimta cnbuild 进行编译并使用 imsimta reload 重新装入可重新装入的数据）。

如果正在使用常规数据库，则该数据库应该可由所有人读取，才能保证它正确操作。

当您要在执行常规表替换的映射表条目中使用进程控制元字符 （例如， $C、$R 或 $L）时，应将进程控制元字符置于映射表模板中的常规表替换的左侧；否则，如果常规表替换 “失败”，则意味着将不显示进程控制元字符。

由站点提供的例程替换 *($[...])*

$[*image*,*routine*,*argument*] 格式的替换是特殊处理的。 image、 routine、 argument 部分用于查找和调用由用户提供的例程。在 UNIX 上运行时， MTA 使用 dlopen 和 dlsym 从共享库 *image* 中动态装入和调用 *routine* 例程。然后将使用以下变量列表将 *routine* 例程作为函数调用：

```
status = routine (argument, arglength, result, reslength)
```

argument 和 result 是长度为 252 个字节的字符串缓冲区。 argument 和 result 将作为指针传递到字符串 （例如，在 C 中，作为 char*）。 arglength 和 reslength 是由引用传递的带有符号的长整数。输入时， argument 包含来自映射表模板的 *argument* 字符串， arglength 中包含该字符串的长度。返回时，结果字符串应放在 result 中，其长度应放在 reslength 中。然后，此结果字符串将替换映射表模板中的 $[image,routine,argument]。如果映射表替换失败，则 *routine* 例程返回 0，如果映射表替换成功则返回 ñ1。如果替换失败，则正常情况下，原始输入字符串将原样用作输出字符串。

如果要在执行由站点提供的例程替换的映射表条目中使用进程控制元字符 （例如， $C、 $R 或 $L），应将进程控制元字符置于映射表模板中由站点提供的例程替换的左侧；否则，如果映射表替换 “失败”，则意味着将不显示进程控制元字符。

由站点提供的例程调用机制可以使用各种复杂的方式来扩展 MTA 的映射进程。例如，在 PORT_ACCESS 或 ORIG_SEND_ACCESS 映射表中，可以执行对某类装入监视服务的调用，其结果可用于确定是否接受连接或邮件。

由站点提供的共享库映像 image 应可由所有人读取。

生成 *UTF-8* 字符串

您可以从常规映射表功能中的 Unicode 字符值生成 UTF-8 字符串。以下格式的 Unicode 元字符序列：

```
$&A0A0,20,A1A1&
```

将生成一个 UTF-8 字符串，其中包含位于 A0A0、 20 和 A1A1 位置的字符。

其他 MTA 配置文件

除了 imta.cnf 文件， Messaging Server 还提供了其他几个帮助您配置 MTA 服务的配置文件。表 10-5 中汇总了这些文件。请注意，修改了 MTA 配置文件 （例如， imta.cnf、 mappings、 aliases 或 option.dat）之后，必须重新编译该配置 （请参见 Sun Java System Messaging Server Administration Reference 中的 imsimta refresh 命令）。

表 10-5 MTA 配置文件

文件	说明
别名文件 （强制）	实现目录中不存在的别名。 *msg_svr_base*/config/aliases
TCP/IP (SMTP) 通道选项文件 （也称为 SMTP 选项文件）	设置特定于通道的选项。 *msg_svr_base*/config/*channel*_option
转换文件	由转换通道使用，用于控制邮件正文部分的转换。 *msg_svr_base*/config/conversions
分发程序配置文件 （强制）	分发程序的配置文件。 *msg_svr_base*/config/dispatcher.cnf
作业控制器文件 （强制）	作业控制器所使用的配置文件。 /*msg_svr_base*/config/job_controller.cnf
MTA 配置文件 （强制）	用于地址重写、路由以及通道定义。 /*msg_svr_base*/config/imta.cnf
映射文件 （强制）	映射表的系统信息库。 /*msg_svr_base*/config/mappings
选项文件	全局 MTA 选项文件。 /*msg_svr_base*/config/option.dat
调整文件 （强制）	用于指定位置和某些优化参数的文件。 /*msg_svr_base*/config/imta_tailor
常规查找表 （可选）	常规查找工具与常规数据库等效。可重新装入的经过编译的配置的一部分。 用于指定位置和某些优化参数的文件。 /*msg_svr_base*/config/general.txt
正向查找表 （可选）	To: 地址的查找。与正向数据库等效。可重新装入的经过编译的配置的一部分。 /*msg_svr_base*/config/forward.txt
反向查找表 （可选）	From: 地址的反向查找。与反向数据库等效。可重新装入的经过编译的配置的一部分。 /*msg_svr_base*/config/reverse.txt

别名文件

别名文件 aliases 可用来设置目录中未设置的别名。特别地，根的地址是一个很好的示例。如果目录中存在同一别名，则将忽略在此文件中设置的别名。有关别名和 aliases 文件的详细信息，请参见第 231 页的 “别名”。

对 aliases 文件进行更改后，必须重新启动 MTA 或发布命令 imsimta reload。

TCP/IP (SMTP) 通道选项文件

TCP/IP 通道选项文件可以控制 TCP/IP 通道的各种特征。通道选项文件必须存储在 MTA 配置目录中，并命名为 *x*_option，其中 *x* 是通道的名称。例如，*msg_svr_base*/config/imta/tcp_local_option。有关详细信息，请参见第 300 页的“配置 SMTP 通道选项”。有关所有通道选项关键字和语法的完整信息，请参见 Messaging Server Reference Manual。

转换文件

转换文件 conversions，指定了转换通道如何对通过 MTA 的邮件执行转换。可以选择转换任何 MTA 通信子集，并可以使用任何一组程序或命令过程来执行转换处理。MTA 将查看转换文件，以便为每个正文部分选择适当的转换。

有关此文件的语法的详细信息，请参见第 365 页的 “转换通道”。

分发程序配置文件

分发程序配置文件 dispatcher.cnf，指定了分发程序配置信息。安装时将创建一个默认的配置文件，它可以不作更改，直接使用。但是，如果出于安全性或性能原因，需要修改默认配置文件，则可以通过编辑 dispatcher.cnf 文件来实现此操作。（有关概念性的信息，请参见第 172 页的 “分发程序”。）

分发程序配置文件的格式与其他 MTA 配置文件的格式类似。指定选项的行具有以下格式：

option=value

option 是选项的名称， *value* 是选项被设置成的字符串或整数。如果 *option* 可以接受整数*值*，则可以使用 *b*%*v* 格式的记数法指定基数，其中 *b* 是以 10 为基础表示的基数， *v* 是以基数 *b* 表示的实际值。此类选项规范根据应用以下选项设置的服务，使用以下格式的行分组成几个部分：

[SERVICE=*service-name*]

service-name 是服务的名称。显示在任何此类部分标记之前的初始选项规范将全局地应用于所有部分。

以下是一个样例分发程序配置文件 (dispatcher.cnf)。

```
! The first set of options, listed without a [SERVICE=xxx]
! header, are the default options that will be applied to all
! services.
!
MIN_PROCS=0
MAX_PROCS=5
MIN_CONNS=5
MAX_CONNS=20
MAX_LIFE_TIME=86400
MAX_LIFE_CONNS=100
MAX_SHUTDOWN=2
!
! Define the services available to Dispatcher
!
[SERVICE=SMTP]
PORT=25
IMAGE=msg_svr_base/lib/tcp_smtp_server
LOGFILE=msg_svr_base/log/tcp_smtp_server.log
```

有关此文件参数的详细信息，请参见 Messaging Server Reference Manual。

映射文件

mappings 文件定义了 MTA 如何将输入字符串映射为输出字符串。

MTA 的许多组件都使用面向表查找的信息。一般说来，此类表格可用于将输入字符串转换 （即映射）为输出字符串。此类表 （称为映射表），通常显示为两列，第一（或左边的）列给出了可能的输入字符串，第二 （或右边的）列给出了与输入关联的结果输出字符串。大多数 MTA 数据库都是此类映射表的实例。但是， MTA 数据库文件不具备通配符查找功能，因为其具有内在局限性，必须要扫描整个数据库才能找到匹配的通配符。

mappings 文件为 MTA 提供了支持多个映射表的工具。它提供了完整的通配符工具，并同时提供了多步和迭代映射方法。此方法的计算量比使用数据库要大，特别是条目很多时。但是，其灵活性带来的好处是实际上您不需要等效数据库中的大多数条目，从而可能使实际总体开销较低。

您可以使用 imsimta test -mapping 命令来测试映射表。有关 mappings 文件和 test -mapping 命令的更多信息，请参见第 208 页的 “映射文件”和 Messaging Server Reference Manual。

对 mappings 文件进行更改后，必须重新启动 MTA 或发布命令 imsimta reload。

选项文件

选项文件 option.dat，指定了与特定于通道的选项相反的全局 MTA 选项。

您可以使用选项文件覆盖作为整体应用于 MTA 的各种参数的默认值。特别地，选项文件可用于建立读入配置和别名文件的各种表的大小。您还可以使用选项文件限制 MTA 接收的邮件的大小、指定 MTA 配置中允许的通道数量、设置允许的重写规则的数量，等等。

在 option.dat 中，以 #、 ! 或 ; 开头的行将被视为注释行 （即使前一行带有后缀 \ 表示该行待续）。这就说明必须留意包含这些字符的长选项 （特别是传送选项）。

传送选项在自然布局中可能会出现以 # 或 ！ 开头的继续行。对于这种问题，有一种安全而巧妙的解决方法。

有关选项文件语法的详细信息，请参见 Messaging Server Reference Manual。

调整文件

调整文件 imta_tailor，可以设定各种 MTA 组件的位置。为使 MTA 正常工作，imta_tailor 文件必须始终位于 *msg_svr_base*/config 目录中。

尽管您可以编辑此文件以反映在特定安装中的更改，但是您必须谨慎地执行此操作。对此文件进行更改后，必须重新启动 MTA。最好是在 MTA 停止时进行更改。

注	除非绝对必要，否则请勿编辑此文件。

有关此文件完整信息，请参见 Messaging Server Reference Manual。

作业控制器文件

作业控制器可以创建并管理传送邮件的通道作业。这些通道作业在作业控制器内的进程池中运行。可以认为池是一个运行通道作业的 “地方”。池提供了一个计算区域，一组作业可以在其中运行而不与池外的作业竞争资源。（有关作业控制器概念和通道关键字配置的信息，请参见第 179 页的 “作业控制器”、第 322 页的 “用于通道执行作业的处理池”和第 322 页的 “服务作业限制”。）

作业控制器文件 job_controller.cnf 指定了以下通道处理信息：

- 定义各种池
- 为所有通道指定主程序名和从程序名 （如果适用）

在 imta.cnf 文件中，您可以使用 pool **关键字**指定进程池的名称 （已在 job_controller.cnf 中定义）。例如，以下 job_controller.cnf 样例文件的片段定义了池 MY_POOL：

```
[POOL=MY_POOL]
job_limit = 12
```

以下 imta.cnf 样例文件的片段指定了通道块中的池 MY_POOL：

```
channel_x pool MY_POOL
channel_x-daemon
```

如果要修改与默认池配置关联的参数或添加附加池，则可以通过编辑 job_controller.cnf 文件，然后停止并重新启动作业控制器来实现此操作。

作业控制器配置文件中的第一个池用于不指定池名称的所有请求。在 MTA 配置文件 (imta.cnf) 中定义的 MTA 通道可以通过使用后跟池名称的 pool 通道关键字将它们的处理请求定向到特定的池。池名称必须与作业控制器配置中的池名称匹配。如果作业控制器不能识别请求的池名称，则将忽略请求。

在初始配置中，定义了以下池：DEFAULT、 LOCAL_POOL、 IMS_POOL、 SMTP_POOL。

使用示例

通常情况下，如果您需要将某些通道的处理与其他通道的处理区分开，则可以在作业控制器配置中添加附加的池定义。您也可以选择使用具有不同特征的池。例如，您可能需要控制某些通道可以处理的同时进行的请求的数量。通过创建具有作业限制的新池，您可以执行此操作，然后可以使用 pool 通道关键字将这些通道定向到新的更适合的池。

除了池定义以外，作业控制器配置文件还包含 MTA 通道表，以及作业控制器处理每个通道的请求所必须使用的命令。两类请求分别称为 “主”类型和 “从”类型。通常情况下，通道的 MTA 邮件队列中存储了邮件时，便会调用通道主程序。主程序会使邮件退出队列。

调用从程序的目的是为了轮询通道并选取进入该通道的所有邮件。尽管几乎所有的 MTA 通道都有主程序，但是很多通道却没有或不需要从程序。例如，通过 TCP/IP 处理 SMTP 的通道不使用从程序，因为网络服务和 SMTP 服务器将通过 SMTP 服务器发出的请求接收外来的 SMTP 邮件。 SMTP 通道的主程序是 MTA 的 SMTP 客户机。

如果与通道关联的目标系统无法一次处理多个邮件，则需要创建一种新类型的池，其作业限制为一个池：

```
[POOL=single_job]
job_limit=1
```

反之，如果目标系统具有足够的并行处理能力，则可以将作业限制设置为较高的值。

代码示例 10-1 显示了样例作业控制器配置文件。表 10-6 显示了可用的选项。

代码示例 10-1 UNIX 中的样例作业控制器配置文件

```
!MTA Job Controller configuration file
!
!Global defaults
tcp_port=27442          (1)
secret=never mind
slave_command=NULL      (2)
max_life_age=3600       (3)
!
!
!Pool definitions
!
[POOL=DEFAULT]          (4)
job_limit=10            (5)
!
[POOL=LOCAL_POOL]
job_limit=10
!
[POOL=IMS_POOL]
job_limit=1
!
[POOL=SMTP_POOL]
job_limit=1
!
!Channel definitions
!
!
[CHANNEL=l]              (6)
master_command=msg_svr_base/lib/l_master
!
[CHANNEL=ims-ms]
master_command=msg_svr_base/lib/ims_master
!
[CHANNEL=tcp_*]          (7)
anon_host=0
master_command=msg_svr_base/lib/tcp_smtp_client
```

前述示例中的关键项 （带有编号、括在括号中，且为粗体）为：

1. 此全局选项定义了作业控制器在其上侦听请求的 TCP 端口号。
2. 为后续的 [CHANNEL] 部分设置默认值 SLAVE_COMMAND。
3. 为后续的 [CHANNEL] 部分设置默认值 MAX_LIFE_AGE。
4. [POOL] 部分定义了名为 DEFAULT 的池。
5. 将池的 JOB_LIMIT 设置为 10。
6. [CHANNEL] 部分应用于名为 l 的通道，即 UNIX 本地通道。此部分中所需的唯一定义是 master_command，作业控制器发布该命令来运行此通道。由于通道名称中没有显示通配符，所以通道必须完全匹配。
7. [CHANNEL] 部分应用于名称以 tcp_* 开始的任何通道。由于此通道名称中包含通配符，所以它将与名称以 tcp_ 开头的任何通道匹配。

添加附加池的示例

作业控制器可以创建并管理传送邮件的通道作业。这些通道作业在作业控制器内的进程池中运行。可以认为池是一个运行通道作业的 “地方”。池提供了一个计算区域，一组作业可以在其中运行而不与池外的作业竞争资源。注意，在 job_controller 中设置的作业限制将应用于单个池。例如，如果您将 SMTP_POOL 的 job_limit 定义为 10，那么在任一给定时刻，只能有 10 个 tcp_smtp 客户机进程可以在该池中运行。

某些情况下，用户可能需要创建附加的 tcp_* 通道 （例如，用于特别缓慢的邮件站点的 tcp 通道）。最好是使这些通道在不同的池中运行。这样做的原因在于，如果我们创建了十个不同的 tcp_* 通道，并且它们全运行在 SMTP_POOL 中，那么在给定时刻在每个 tcp_* 通道上很可能只有一个 tcp_smtp 客户机在运行 （取决于所有的 tcp_* 通道上是否有邮件，并假设将 SMTP_POOL 的 job_limit 定义为 10）。假设系统负载很重，并且所有队列中都有邮件等待通过各个 tcp_* 通道发送，则这样会效率很低。用户很可能会为附加的 tcp_* 通道定义附加的池，以便不会出现竞争槽的情况。

例如，假设我们设置了以下 tcp_* 通道：

```
tcp_yahoo smtp mx pool yahoo_pool keyword keyword keyword
tcp-yahoo-daemon

tcp_aol smtp mx keyword keyword keyword pool aol_pool
tcp-aol-daemon

tcp_hotmail smtp mx pool hotmail_pool keyword keyword keyword tcp-hotmail-daemon

...

tcp_sun smtp mx pool sun_pool keyword keyword keyword
tcp-sun-daemon
```

为了使每个新的通道有十个 tcp_smtp_client 进程，我们要在 job_controller.cnf 文件中添加以下行：

```
[POOL=yahoo_pool]
job_limit=10

[POOL=aol_pool]
job_limit=10

[POOL=hotmail_pool]
job_limit=10

...

[POOL=sun_pool]
job_limit=10
```

有关池的详细信息，请参见第 322 页的 “用于通道执行作业的处理池”。有关作业控制器文件语法的详细信息，请参见 Messaging Server Reference Manual。

表 10-6 作业控制器配置文件选项

选项	说明
常规选项	**说明**
INTERFACE_ADDRESS=*adapter*	指定应绑定作业控制器的 IP 地址接口。指定的值（适配器）可以是 ANY、ALL、LOCALHOST 之一，也可以是一个 IP 地址。默认情况下，作业控制器绑定到所有的地址（相当于指定 ALL 或 ANY）。指定 INTERFACE_ADDRESS=LOCALHOST，表示作业控制器仅接受来自本地计算机内的连接。这不会影响正常操作，因为作业控制器不支持任何计算机之间的操作。但是，这对于 HA 代理可能正在检查作业控制器是否响应的 HA 环境可能并不适合。如果运行 Messaging Server 的计算机处于 HA 环境中，具有一个“内部网络”适配器和一个“外部网络”适配器，您不能确信您的防火墙可以阻塞到高端口号的连接，您应考虑指定“内部网络”适配器的 IP 地址。
MAX_MESSAGES=*integer*	作业控制器以内存内结构保留有关邮件的信息。在较大的待办事项构建的事件中，可能需要限制此结构的大小。如果待办事项中的邮件数量超过了此处指定的参数，则有关后续邮件的信息将不会保留在内存中。因为邮件消息始终会被写入磁盘，所以邮件不会丢失，但是在作业控制器所知道的邮件数量降至此数量的一半之前，不会发送邮件。此时，作业控制器将模拟 imsimta cache -sync 命令，扫描队列目录。 默认值为 100000。
SECRET=*file_spec*	用于保护已发送至作业控制器的请求的共享机密。
SYNCH_TIME=*time_spec*	作业控制器会偶尔扫描磁盘上的队列文件，以检查是否有丢失的文件。默认情况下，此操作在作业控制器启动四小时后开始，每四小时进行一次。 *time_spec* 的格式为 *HH*:*MM*/*hh*:*mm* 或 /*hh*:*mm*。变量 *hh*.*mm* 是事件之间的间隔（以小时 [*h*] 和分钟 [*m*] 为单位）。变量 *HH*:*MM* 是事件在一天中第一次发生的时间。例如，指定 15:45/7:15，则表示事件在 15:45 开始，并从此刻起每隔 7 小时 15 分钟就会再次发生。
TCP_PORT=*integer*	指定作业控制器应在其上侦听请求软件包的 TCP 端口。除非默认设置与系统上的其他 TCP 应用程序冲突，否则不要更改此选项。如果确实要更改此选项，请更改 MTA 调整文件（位于 *msg_svr_base*/config/imta_tailor）中相应的 IMTA_JBC_SERVICE 选项，以使其匹配。 TCP_PORT 选项将应用于全局，如果它显示在 [CHANNEL] 或 [POOL] 部分中，则该选项将被忽略。

表 10-6 作业控制器配置文件选项 （续）

选项	说明
池选项	**说明**
JOB_LIMIT=*integer*	指定池可同时 （并行）使用的最大进程数。 JOB_LIMIT 将单独应用到每个池；作业的最大总数是所有池的 JOB_LIMIT 参数的和。如果在某部分之外设置此选项，则它会被未指定 JOB_LIMIT 的任何 [POOL] 部分用作默认选项。在 [CHANNEL] 部分中会忽略此选项。
通道选项	**说明**
MASTER_COMMAND=*file_spec*	指定指向作业控制器创建的 UNIX 系统进程要执行的命令的完整路径，该命令用于运行通道并将通过该通道外发的邮件退出队列。如果在某部分之外设置此选项，则未指定 MASTER_COMMAND 的任何 [CHANNEL] 部分都会将其用作默认选项。在 [POOL] 部分中将忽略此选项。
MAX_LIFE_AGE=*integer*	指定通道主作业的最大生命周期 （以秒为单位）。如果没有为通道指定此参数，则使用全局默认值。如果没有指定默认值，则使用 1800 （30 分钟）。
MAX_LIFE_CONNS=*integer*	除了最大生命周期参数以外，通道主作业的生命期限还受其可以询问作业控制器是否有任何邮件的次数的限制。如果没有为通道指定此参数，则使用全局默认值。如果没有指定默认值，则使用 300。
SLAVE_COMMAND=*file_spec*	指定指向作业控制器创建的 UNIX 系统进程要执行的命令的完整路径，以便运行通道并轮询通过该通道的外来邮件。大多数 MTA 通道没有 SLAVE_COMMAND。如果是这种情况，则应指定保留值 NULL。如果在某部分之外设置此选项，则未指定 SLAVE_COMMAND 的任何 [CHANNEL] 部分都会将其用作默认选项。在 [POOL] 部分中将忽略此选项。

别名

MTA 提供了一个工具，用以支持与本地系统 （不一定对应于实际用户）关联的邮箱名称：**别名**。别名对于构造邮件列表、转发邮件并提供用户名的同义词十分有用。有关如何处理别名解析的说明，请参见第 186 页的 “$V 元字符”。

在 aliases 文件或别名数据库中定义的旧样式邮递列表现在接受非位置 [capture] 参数。如果使用， [capture] 参数将指定具有相同语义的捕获地址作为在 LDAP 中应用到用户或组的 LDAP_CAPTURE 属性指定的捕获地址。

别名数据库

使用别名数据库时，您会觉得很失望。请使用 aliases 文件，因为使用 imsimta reload 命令可以动态地重新装入别名文件。

MTA 将使用该目录中的信息并创建别名数据库。每次参考常规别名文件时都会参考一次别名数据库。但是，使用常规别名文件之前，将先检查别名数据库。实际上，数据库充当一种在使用别名文件之前调用的地址重写程序。

注 数据库本身的格式是专用的。请勿尝试直接编辑数据库。请在目录中进行全部必需更改。

别名文件

`aliases` 文件用于设置未在目录中设置的别名。特别地，邮寄主管别名是一个很好的示例。如果目录中存在同一别名，则将忽略在此文件中设置的别名。可以通过发出 `imsimta reload` 命令激活更改 （或重新启动 MTA）。以感叹号开始的任何行都被看作注释，并将被忽略。空行也将被忽略。

注 Messaging Server 提供了其他用于地址处理的工具，例如，地址反向数据库和专用映射表。但为了获得最佳性能，在可以执行地址操作时应使用重写规则。请参见第 11 章 “配置重写规则”。

此文件中的物理行限制为 1024 个字符。您可以使用反斜杠 (\) 继续符将一个逻辑行分成多个物理行。

文件的格式如下：

user@domain：<*address*> （**用于托管域中的用户**）

user@domain：<*address*> （**用于非托管域中的用户。示例：默认域**）

例如：

```
! A /var/mail/ user
inetmail@siroe.com: inetmail@native-daemon

! A message store user
ms_testuser@siroe.com: mstestuser@ims-ms-daemon
```

在别名文件中包含其他文件

可以将其他文件包含到主 aliases 文件中。以下格式行对 MTA 进行定向，以读取 file-spec 文件：

```
<file-spec
```

文件规范必须是一个完整的文件路径规范，且文件的保护级别与主 aliases 文件的保护级别必须相同，例如，该文件必须可由所有用户读取。

被包含文件的内容将插入到 aliases 文件中其引用点处。将被包含文件的引用替换为文件的实际内容也可以达到相同的效果。被包含文件的格式与主 aliases 文件本身的格式相同。实际上，被包含文件本身也可以包含其他文件。被包含文件最多允许嵌套三层。

命令行实用程序

Messaging Server 提供了多个命令行实用程序，使您可以执行 MTA 的各种维护、测试和管理任务。例如，您可以使用 imsimta cnbuild 命令编译 MTA 配置、别名、映射、安全性、系统级过滤器及选项文件。有关 MTA 命令行实用程序的完整信息，请参见 Messaging Server Reference Manual。

SMTP 安全性和访问控制

有关 SMTP 安全性和访问控制的信息，请参见第 17 章 “邮件过滤和访问控制”和第 19 章 “配置安全和访问控制”。

日志文件

所有 MTA 特定日志文件都保存在日志目录 (*msg_svr_base*/log) 中。此目录中包含说明通过 MTA 的邮件通信的日志文件，以及说明有关特定主程序或从程序的信息的日志文件。

有关 MTA 日志文件的更多信息，请参见第 21 章 “管理日志记录”。

将地址由内部格式转换为公用格式

使用地址反向数据库 （也称为**反向数据库**）和 REVERSE 映射表，可以将地址由内部格式转换为公用的公布格式。例如，尽管 uid@mailhost.siroe.com 在 siroe.com 域中可能是一个有效的地址，它可能不是一个向外公开的合适的地址。您可能希望使用类似于 firstname.lastname@siroe.com 的公用地址。

注 Messaging Server 提供了其他地址处理工具，例如 aliases 文件和专门的映射表。但为了获得最佳性能，在可以执行地址操作时应使用重写规则。请参见第 11 章 “配置重写规则”。

在反向数据库中，每个用户的公用地址是由目录中用户条目的 mail 属性来指定的。专用或内部地址是由 mailAlternativeAddress 属性指定的。分发列表也是一样。

反向数据库包含任何有效的地址与此公用地址之间的映射。反向数据库通常位于 MTA 数据库目录中。该数据库是一个名称由 *msg_svr_base*/config/imta_tailor 文件中的 IMTA_REVERSE_DATABASE 选项指定的文件，默认情况下为文件 *msg_svr_base*/data/db/reversedb.*。

如果在数据库中找到了地址，则数据库右侧对应的内容将替换为该地址。如果未找到地址，则会尝试在 mappings 文件中查找名为 REVERSE 的映射表。如果该表不存在或表中没有匹配的条目，则不进行替换且重写操作正常终止。

如果在 mappings 文件中找到了 REVERSE 映射表，并且地址与映射条目匹配，则结果字符串将替换该地址 （如果该条目指定了 $Y）。如果指定了 $N，将放弃映射结果。如果映射条目除指定了 $Y 以外，还指定了 $D，则结果字符串将再次在反向数据库中运行，并且如果出现匹配，则数据库中的模板将替换映射结果 （从而替换地址）。常规的 REVERSE 映射表条目 （即，应用于所有通道的条目）的格式如下所示。注意，标志可以在新地址之前，也可以在新地址的结尾。

```
REVERSE

  OldAddress        $Y[Flags]NewAddress
```

特定于通道的条目 （即，仅在邮件通过特定通道时才发生的映射）的格式如下所示。注意，您必须在 option.dat 中将 use_reverse_database 设置为 13，才能使特定于通道的条目正常工作。

```
REVERSE

  source-channel|destination-channel|OldAddress  $Y[Flags]NewAddresS
```

表 10-7 中显示了 REVERSE 映射表标志。

表 10-7 REVERSE 映射表标志

标志	说明
$Y	将输出作为新的地址。
$N	地址保留不变。
$D	在反向数据库中运行输出。
$A	将模式添加为反向数据库条目。
$F	将模式添加为正向数据库条目。
标志比较	**说明**
$:B	仅匹配标题 （正文）地址。
$:E	仅匹配信封地址。
$:F	仅匹配指向前的地址。
$:R	仅匹配指向后的地址。
$:I	仅匹配邮件 ID。

设置地址反向控制

reverse 和 noreverse 通道关键字以及 MTA 选项 USE_REVERSE_DATABASE 和 REVERSE_ENVELOPE 都用于控制何时以及如何应用地址反向的详细设置。默认情况下，地址反向操作应用于所有地址，不仅仅是指向后的地址。

通过设置 REVERSE_ENVELOPE 系统选项的值 （默认值：1 — 打开， 0 — 关闭）可以启用或禁用地址反向。

目标通道上的 noreverse 指定不对邮件中的地址应用地址反向， reverse 指定应用地址反向。有关详细信息，请参见 *Sun Java System Messaging Server Administration Reference*。

USE_REVERSE_DATABASE 控制 MTA 是否使用地址反向数据库并且是否将 REVERSE 映射用作替换地址的源。 0 表示不在任何通道中使用地址反向。 5 （默认值）指定在 MTA 地址重写进程执行重写后对所有的地址都应用地址反向 （而不仅是应用于指向后的地址）。13 指定在 MTA 地址重写进程执行重写后对包含 reverse 通道关键字的地址应用地址反向 （而不仅是应用于指向后的地址）。通过设置 USE_REVERSE_DATABASE 选项的位值，可以进一步精确地指定地址反向操作。有关详细信息，请参见 *Sun Java System Messaging Server Administration Reference*。

REVERSE_ENVELOPE 选项可以控制是否将地址反向应用到信封的 From 地址以及邮件标题地址。

有这些选项和关键字的影响的其他信息，请参见 Sun Java System Messaging Server Administration Reference 中的详细说明。

常规反向映射示例

以下是常规 REVERSE 映射的示例：假设 siroe.com 中内部地址的格式为 user@mailhost.siroe.com。但是，由于用户名称空间属于这类格式，因此 user@host1.siroe.com 和 user@host2.siroe.com 为 siroe.com 中的所有主机指定了同一个人。以下 REVERSE 映射可以与地址反向数据库一起使用：

```
REVERSE

  *@*.siroe.com         $0@siroe.com$Y$D
```

在此示例中，格式为 *name*@*anyhost*.siroe.com 的地址将被更改为 *name*@siroe.com。$D 元字符使得地址反向数据库可被查询。地址反向数据库应包含以下格式的条目：

```
user@mailhost.siroe.com      first.last@siroe.com
```

特定于通道的反向映射示例

默认情况下，如果将路由能力范围设置为邮件服务器域，则将使用地址反向数据库。特定于通道的 REVERSE 映射表条目的示例如下：

```
REVERSE

  tcp_*|tcp_local|binky@macho.siroe.com    $D$YRebecca.Woods@siroe.com
```

此条目告知 MTA，对于源通道为 tcp_*、外发目标通道为 tcp_local 的任何邮件，会将格式为 binky@macho.siroe.com 的地址更改为 Rebecca.Woods@siroe.com。

注 要启用特定于通道的反向映射，您必须将 option.dat 中的 USE_REVERSE_DATABASE 选项设置为 13。（默认值为 5。）

正向查找表和 FORWARD 地址映射

地址反向不会应用于信封的 To: 地址。省略此操作的原因相当明显 — 信封的 To: 地址随着邮件在邮件系统中的传送，不断地被重写和修改。路由的整体目标是将信封的 To: 地址转换为不断增加的系统和特定于邮箱的格式。地址反向的规范化功能完全不适合于信封的 To: 地址。

在任何情况下，均可以在 MTA 中使用大量的工具替换信封的 To: 地址。别名文件、别名数据库及常规查找表恰好具备此功能。

MTA 还提供正向查找表和 FORWARD 映射，可用于特殊种类的转发目的，例如，基于模式的转发、特定于源的转发或地址的自动注册。请注意，正向查找表和 FORWARD 映射主要用于某些特殊种类的地址转发；但是，使用 MTA 的某一其他转发机制，可更好地执行大多数种类的地址转发。

信封的 To: 地址的各种替换机制与反向查找表的功能等效，但是上面讨论的机制中还没有哪一种与反向映射功能等效。而且确实会发生需要对信封的 To: 地址使用映射功能的情况。

FORWARD 映射表

FORWARD 映射表提供了基于模式的转发功能和特定于源的转发机制。如果映射文件中存在 FORWARD 映射表，它将应用于每一个信封的 To: 地址。如果该映射表不存在或没有映射匹配条目，则不会进行任何更改。

如果地址匹配某个映射条目，则将测试映射结果。如果该条目指定 $Y，结果字符串将替换信封的 To: 地址；指定 $N 将放弃映射结果。有关其他标志的列表，请参见表 10-8。

表 10-8 FORWARD 映射表标志说明

标志	说明
$D	在重写进程中再次运行输出
$G	在正向查找表中运行输出 （如果已启用正向查找表）
$H	禁用进一步的正向查找表或 FORWARD 映射查找
$I	将邮件保存为 .HELD 文件
$N	地址保留不变
$Y	将输出用作新地址

在执行任何正向查找表查找之前，都会查询 FORWARD 映射 （如果存在）。如果 FORWARD 映射匹配并具有标志 $G，则会将 FORWARD 映射的结果与正向查找表进行核对 （如果已通过适当地设置 USE_FORWARD_DATABASE 启用了正向查找表）。（注意，如果已指定通道特定的正向查找表，则在正向查找表中进行查找之前，会将源地址和源通道置于 FORWARD 映射的结果之前。）如果匹配的 FORWARD 映射条目指定了 $D，则 FORWARD 映射 （和可选的正向表查找）的结果将在 MTA 地址重写进程中再次运行。如果匹配的 FORWARD 映射条目指定了 $H，则在后续地址重写 （源自 $D 的使用）期间将不会执行进一步的 FORWARD 映射或数据库查找。

以下示例说明了复杂的 REVERSE 和 FORWARD 映射的使用。假设系统或与 mr_local 通道关联的名为 am.sigurd.innosoft.com 的伪域生成常规格式的 RFC 822 地址：

```
"lastname, firstname"@am.sigurd.example.com
```

或

```
"lastname,firstname"@am.sigurd.example.com
```

尽管这些地址完全合法，但它们经常会使不完全符合 RFC 822 语法规则的其他邮件程序 （例如，那些没有正确处理引用地址的邮件程序）产生混淆。因此，不要求引用的地址格式可用于更多的邮件程序。此类格式之一为

```
firstname.lastname@am.sigurd.example.com
```

复杂的 FORWARD 和 REVERSE 映射的示例：

```
REVERSE

 *|mr_local|"*,$ *"@am.sigurd.innosoft.com $Y"$1,$ $2"@am.sigurd.innosoft.com
 *|mr_local|"*,*"@am.sigurd.innosoft.com   $Y"$1,$ $2"@am.sigurd.innosoft.com
 *|*|"*,$ *"@am.sigurd.innosoft.com        $Y$3.$2@am.sigurd.innosoft.com
 *|*|"*,*"@am.sigurd.innosoft.com          $Y$3.$2@am.sigurd.innosoft.com
 *|mr_local|*.*@am.sigurd.innosoft.com     $Y"$2,$ $1"@am.sigurd.innosoft.com
 *|*|*.*@am.sigurd.innosoft.com            $Y$2.$3@am.sigurd.innosoft.com


FORWARD

 "*,$ *"@am.sigurd.innosoft.com            $Y"$0,$ $1"@am.sigurd.innosoft.com
 "*,*"@am.sigurd.innosoft.com              $Y"$0,$ $1"@am.sigurd.innosoft.com
 *.*@am.sigurd.innosoft.com                $Y"$1,$ $0"@am.sigurd.innosoft.com
```

因此，以上示例中的样例映射表的目的有三个方面。(1) 允许使用以上三种地址格式中的任何一种。(2) 仅对 mr_local 通道显示原始格式的地址，必要时进行格式转换。(3) 仅对所有其他通道显示最新未引用格式的地址，必要时进行格式转换。（以上的 REVERSE 映射中假设 MTA 选项 USE_REVERSE_DATABASE 中的第 3 位已设置。）

正向查找表

当地址转发需要进行自动注册或特定于源时，可以使用正向查找表。注意，使用正向查找表进行邮件的简单转发通常并不适合； aliases 文件或别名查找表是执行此类转发的更有效方法。默认情况下不会使用正向查找表，必须通过 USE_FORWARD_DATABASE 选项明确启用正向查找表，才能使用该表。正向表查找是在执行了地址重写和别名扩展，且检查了所有 FORWARD 映射之后执行的。如果正向表查找成功，则结果替换地址将在整个 MTA 地址重写进程中再次运行。

有两种正向查找表机制，即内存内散列表或常规数据库。除非表的大小过分大，否则建议使用散列表。（1,000 不会受到限制，但是 100,000 就会受到限制）。通过设置 use_text_database 和 use_forward_database 选项中的第 3 位 （值为 34）可以启用散列表。散列表位于 *msg_svr_base*/configure/forward.txt 中，它经过编译成为配置的可重新装入的部分，并可通过 imsimta reload 命令强制重新装入活动 MTA 进程。

正向数据库是一个 MTA crdb 数据库，是使用 crdb 实用程序从源文本文件创建的。源文本文件的默认格式为：

```
user1@domain1    changedmailbox1@changeddomain1
user2@domain2    changedmailbox@changeddomain2
```

但是，如果已通过设置 USE_FORWARD_DATABASE 选项中的第 3 位来启用特定源的正向数据库，则源文本文件的格式为：

```
source-channel|source-address|original-address  changed-address
```

例如，以下条目

```
tcp_limited|bob@blue.com|helen@red.com  "helen of  troy"@siroe.com
```

如果且仅在邮件来自于 bob@blue.com 且排队通道为 tcp_limited 时，将 To: 地址 address helen@red.com 映射为 "helen of troy"@siroe.com。

控制传送状态通知邮件

传送状态通知或**状态通知**是由 MTA 发送给发件人和邮寄主管 （可选）的电子邮件状态消息。 Messaging Server 使您可以按照内容和语言自定义通知邮件。您也可以为每类传送状态 （例如 FAILED、 BOUNCED、 TIMEDOUT 等等）创建不同的消息。另外，您还可以为源于特定通道的邮件创建通知邮件。

默认情况下，状态通知存储于 *msg_svr_base*/config/locale/C 目录 （由 *msg_svr_base*/config/imta_tailor 文件中的 IMTA_LANG 设置指定）中。文件名如下所示：

```
return_bounced.txt, return_delivered.txt  return_header.opt, return_timedout.txt,
return_deferred.txt, return_failed.txt, return_prefix.txt, return_delayed.txt,
return_forwarded.txt, return_suffix.txt.
```

*.txt 文件的邮件文本应限制为每行 78 个字符。注意，因为 Messaging Server 升级时会覆盖这些文件，所以您不应直接更改这些文件。如果要修改这些文件并将它们用作唯一一组通知邮件模板文件 (return_*.txt)，请将这些文件复制到一个新目录中并在其中对它们进行编辑。然后，将 imta_tailor 文件中的 IMTA_LANG 选项设置为指向包含这些模板的新目录。如果希望有多组通知文件 （例如，每种语言一组），则需要设置 NOTIFICATION_LANGUAGE 映射表。

构造和修改状态通知

单个的通知邮件是由三个文件构造的：return_prefix.txt + return_*ActionStatus*.txt + return_suffix.txt

要自定义或本地化通知，应该为每种语言环境和 / 或自定义创建完整的一组 return_*.txt 文件并将其存储在单独的目录中。例如，您可以将法语通知文件存储在一个目录中，将西班牙语通知文件存储在另一个目录中，并将特殊的未经许可的批量电子邮件通道的通知存储在第三个目录中。

注 本发行版中包含法语、德语和西班牙语的样例文件。您可以修改这些文件，使它们适合于特定的需要。

对于双字节语言，例如日语，请确保使用日语构造文本，然后就像查看 ASCII 一样查看该文本，以检查 % 字符。如果有意外的 % 字符，则使用 %% 替换它们。

下面介绍了状态通知邮件集的格式和结构。

1. return_prefix.txt 提供了适当的标题文本以及正文的介绍材料。以下是美国英语语言环境的默认设置：

   ```
   Content-type: text/plain; charset=us-asci
   Content-language: EN-US

   This report relates to a message you sent with the following
   header fields: %H
   ```

   非美国 ASCII 状态通知邮件应相应更改 charset 参数和 Content-Language 标题值（例如，对于法语的本地化文件，值为 ISO-8859-1 和 fr）。 %H 是表 10-9 中定义的标题替换序列。

2. return_<*ActionStatus*>.txt 包含特定于状态的文本。 *ActionStatus* 是指邮件的 MTA 状态类型。例如， return_failed.txt 的默认文本如下：

   ```
   您的邮件无法传送给以下收件人：
   %R
   ```

   return_bounced.txt 的默认文本为：

   ```
   您的邮件已被返回。该邮件已被邮寄主管
   强制返回。

   此邮件的收件人列表为：
   %R
   ```

3. return_suffix.txt 包含结束文本。默认情况下，此文件为空。

表 10-9 通知邮件替换序列

替换	定义
%H	扩展为邮件的标题。
%C	扩展为已排队的邮件的单位[1] 的数量。
%L	扩展为返回邮件之前，邮件在队列中剩余的单位[1] 的数量。
%F	扩展为邮件可在队列中停留的单位[1] 的数量。
%S [%s]	扩展为字母 S 或 s （如果先前扩展的数值不等于一）。示例：根据邮件已排队的天数， "%C day%s" 可以扩展为 “1 天”或 “2 天”。
%U [%u]	扩展为正在使用的时间单位[1] 小时或天。示例：根据邮件已排队的天数或小时数以及 MTA 选项 RETURN_UNITS 的值， "%C %U%s" 可以扩展为 “2 天”或 “1 小时”。如果您已设置 RETURN_UNITS=1 （小时），并且您的站点正在使用本地化的状态通知邮件，则需要为除英语以外的所有语言编辑 return_delayed.txt 和 return_timedout.txt 并将单词 “天”替换为单词 “小时”。对于法语，将 jour(s) 替换为 heure(s)。对于德语，将 Tag(e) 替换为 Stunde(n)。对于西班牙语，将 día(s) 替换为 hora(s)
%R	扩展为邮件收件人的列表。
%%	% （注意，无论为何种字符集，都将针对替换序列逐个字节地扫描文本。如果您正在使用双字节字符集，请检查非预期的 % 符号。）

[1] 单位由 MTA 选项文件中的 RETURN_UNITS 选项定义，可以为小时或天 （默认值）。

自定义和本地化传送状态通知邮件

可以本地化传送状态通知邮件，以便将邮件以不同的语言返回给不同用户。例如，可以将法语通知返回给首选使用法语的用户。

本地化或自定义状态通知邮件包括两个步骤：

1. 创建一组本地化 / 自定义的 return_*.txt 邮件文件，并将每组文件存储在单独的目录中。第 241 页的 “构造和修改状态通知”中说明了此步骤。
2. 设置一个 NOTIFICATION_LANGUAGE 映射表。

NOTIFICATION_LANGUAGE 映射表 （位于 *msg_svr_base*/config/mappings 目录中）指定了要使用的一组本地化或自定义的通知邮件文件 （取决于**起始邮件** [发出通知的邮件] 的属性 [语言、国家 / 地区、域或地址]）。

原始发件人的邮件将被解析，以确定状态通知类型、源通道、首选语言、返回地址及第一收件人。根据该表的构造方式，将根据以上的一个或多个属性来选择一组通知文件。

NOTIFICATION_LANGUAGE 映射表的格式为：

```
NOTIFICATION_LANGUAGE

 dsn-type-list|source-channel|preferred-language|return-address|first-recipient $Idirectory-spec
```

dsn-type-list 是以逗号分隔的传送状态通知类型的列表。如果指定了多种类型，则这些类型必须由逗号分隔，中间不能包含空格 （空格将终止映射表条目的模式）。这些类型如下：

failed — 常规的永久性错误消息 （例如，无此用户）。使用 return_failed.txt 文件。

bounced — 与手动 “退回”结合使用的通知邮件。由邮寄主管完成。使用 return_bounced.txt 文件。

timedout — MTA 无法在允许的传送时间内传送邮件。邮件将被返回。使用 return_timedout.txt 文件。

delayed — MTA 无法传送邮件，但将继续尝试传送。使用 return_delayed.txt 文件。

deferred — 与 “延迟”类似的非传送通知，但并不表明 MTA 将继续尝试传送多长时间。使用 return_deferred.txt 文件。

forwarded — 为此邮件请求了发送收据，但是该邮件已被转发给不支持此类收据的系统。使用 return_forwarded.txt 文件。

source-channel 是生成通知邮件的通道，即，邮件当前排队的通道。例如， ims-ms 对应于邮件存储的传送队列， tcp_local 对应于外发 SMTP 队列，等等。

preferred-language 是正在处理的邮件 （为其生成通知的邮件）中所表示的语言。此信息的源最初是 accept_language 字段。如果该字段不存在，则使用 Preferred-language: 标题字段和 X-Accept-Language: 标题字段。有关标准语言代码值的列表，请参阅文件 *msg_svr_base*/config/languages.txt。

如果此字段不为空，则它将成为为 Preferred-language: 或 X-Accept-language: 标题行指定的邮件的创始者。因此，您可以在此字段中找到无意义的字符。

return-address 是原始邮件的信封的 From: **地址**。它是要向其发送通知邮件的信封地址，因此也是要使用的语言的指示符。

first-recipient 是要向其发送原始邮件的信封的 To: 地址 （第一个地址，如果邮件无法到达多个收件人处）。例如，在通知 “无法将您的邮件传送至 dan@siroe.com” 中 — 在这种情况下， dan@siroe.com 是报告的信封 To: 地址。

directory-spec 是包含要使用的 return_*.txt 文件的目录 （如果映射表探测匹配）。注意， $I 必须在目录规范之前。

例如，在 /lc_messages/table/notify_french/ 目录中存储法语通知文件 (return_*.txt) 和在 /lc_messages/table/notify_spanish/ 目录中的 return_*.txt 文件中存储西班牙语通知文件的站点可能使用如下所示的表。注意，每个条目的开始处都必须有一个或多个空格，并且条目之间可以不含空行。

代码示例 10-2 通知语言映射表示例

```
NOTIFICATION_LANGUAGE

! Preferred-language: header value specified
!
   *|*|fr|*|*     $I/lc_messages/table/notify_french/
   *|*|es|*|*     $IIMTA_TABLE/notify_spanish/
   *|*|en|*|*     $I/imta/lang/
!
! If no Preferred-language value, then select notification based on the
! country code in the domain name. EX: PF=French Polynesia; BO=Bolivia
!
   *|*|*|*.fr|*   $I/imta/table/notify_french/
   *|*|*|*.fx|*   $I/imta/table/notify_french/
   *|*|*|*.pf|*   $I/imta/table/notify_french/
   *|*|*|*.tf|*   $I/imta/table/notify_french/
   *|*|*|*.ar|*   $I/imta/table/notify_spanish/
   *|*|*|*.bo|*   $I/imta/table/notify_spanish/
   *|*|*|*.cl|*   $I/imta/table/notify_spanish/
   *|*|*|*.co|*   $I/imta/table/notify_spanish/
   *|*|*|*.cr|*   $I/imta/table/notify_spanish/
   *|*|*|*.cu|*   $I/imta/table/notify_spanish/
   *|*|*|*.ec|*   $I/imta/table/notify_spanish/
   *|*|*|*.es|*   $I/imta/table/notify_spanish/
   *|*|*|*.gp|*   $I/imta/table/notify_spanish/
   *|*|*|*.gt|*   $I/imta/table/notify_spanish/
   *|*|*|*.gy|*   $I/imta/table/notify_spanish/
   *|*|*|*.mx|*   $I/imta/table/notify_spanish/
   *|*|*|*.ni|*   $I/imta/table/notify_spanish/
   *|*|*|*.pa|*   $I/imta/table/notify_spanish/
   *|*|*|*.ve|*   $I/imta/table/notify_spanish/
```

注 安装时将提供一个默认的 mappings.locale 文件，并将其包含在启用通知语言映射的 mappings 文件中。要禁用通知语言映射，请注释以下包含行：

```
! <IMTA_TABLE:mappings.locale
```

（请阅读该文件中的注释并根据您的需要进行修改。）

将生成的通知国际化

有两个选项文件既可用于传送状态也可用于邮件处理通知。这些文件旨在使生成的通知的国际化过程更加灵活。这些文件如下所示：

IMTA_LANG:return_option.dat (DSN)
IMTA_LANG:disposition_option.dat (MDN)

表 10-10 介绍了这些文件可用的选项

表 10-10 传送状态和邮件处理通知选项

选项	说明
DAY (DSN)	当设置 RETURN_UNITS=0 （默认值）时，用来替换 %U 或 %u 的插入文本。请注意， %U 和 %u 没有区别 （这与分别替换英文 "Day" 或 "day" 的默认情况不同）。
DIAGNOSTIC_CODE (DSN)	替换 DSN 第一部分各收件人部分的构建中使用的 "Diagnostic code:" 文本。指定此字段所用的字符集应与 DSN 第一部分使用的字符集相同。
HOUR (DSN)	当设置了 RETURN_UNITS=1 时，用来替换 %U 或 %u 的插入文本。请注意，%U 和 %u 没有区别 （这与分别替换英文 "Hour" 或 "hour" 的默认情况不同）。
n.n.n (DSN)	当构建 DSN 的各收件人部分时，将检查是否存在一个选项，该选项的名称与各收件人的数值状态相匹配。如果匹配，将在 DSN 中插入相应的文本。此外，如果上面指定的 REASON 选项生成零长度结果，则不会插入 REASON 字段。
ORIGINAL_ADDRESS (DSN)	替换 DSN 第一部分各收件人部分的构建中使用的 "Original address:" 文本。指定此字段所用的字符集应与 DSN 第一部分使用的字符集相同。
REASON (DSN)	替换 DSN 第一部分各收件人部分的构建中使用的 "Reason:" 文本。指定此字段所用的字符集应与 DSN 第一部分使用的字符集相同。
RECIPIENT_ADDRESS (DSN)	替换 DSN 第一部分各收件人部分的构建中使用的 "Recipient address:" 文本。指定此字段所用的字符集应与 DSN 第一部分使用的字符集相同。
RETURN_PERSONAL (DSN 和 MDN)	替换个人姓名字段，以与 From: 字段结合使用字段。此字段应采用 RFC 2047 编码。如果未指定此选项，则使用由 RETURN_PERSONAL MTA 选项设置的值。
SUBJECT (DSN 和 MDN)	替换 Subject: 字段。该值仅在通知未提供其自身的主题字段时使用。此字段应采用 RFC 2047 编码。如果未使用此选项并且通知未提供，将构建一个相应的主题。

表 10-10 传送状态和邮件处理通知选项

选项	说明
TEXT_CHARSET (MDN)	MDN 第一部分和主题应转换为的字符集文本。默认情况下，不执行任何转换。

附加的状态通知邮件功能

前几个小节中介绍了设置状态通知邮件的基本过程。以下小节将介绍附加功能。

阻塞较大邮件的内容返回

通常情况下，当邮件被退回或阻塞时，邮件的内容会返回发件人和通知邮件中的本地域邮寄主管。如果完整地返回大量较大的邮件，则可能使资源负载过重。要阻塞超过一定大小的邮件返回内容，请设置 MTA 选项文件中的 CONTENT_RETURN_BLOCK_LIMIT 选项。

从状态通知邮件包含的标题中删除非美国 ASCII 字符

Internet 邮件标题的原始格式不允许包含非美国 ASCII 字符。如果在邮件标题中使用非美国 ASCII 字符，则会使用 RFC 2047 中说明的 “MIME 标题编码”对这些字符进行编码。因此，电子邮件消息中的中文 “主题”行将实际显示为：

```
Subject: =?big5?Q?=A4j=AB=AC=A8=B1=AD=B1=B0=D3=F5=A5X=AF=B2?=
```

电子邮件客户机负责在显示这些标题时删除编码。

因为 %H 模板将标题复制到通知邮件的正文中，所以已编码的标题文本会正常显示。但是，如果主题中的字符集 （这种情况下为 "big5"）匹配 return_prefix.txt 中的 Content-Type 标题字符集参数，则 Messaging Server 将删除编码。如果不匹配，则 Messaging Server 将保留编码，不作更改。

设置通知邮件传送间隔

关键字：notices、 nonurgentnotices、 normalnotices、 urgentnotices。

无法传送的邮件将在给定的通道队列中保存一段指定的时间，然后再返回发件人。此外， Messaging Server 尝试传送的同时，会将一系列状态 / 警告消息返回发件人。可以使用关键字 notices、nonurgentnotices、normalnotices 或 urgentnotices 指定邮件之间的时间和间隔。示例：

```
notices 1 2 3
```

对于所有邮件，将在 1 到 2 天之后发送瞬态失败状态通知邮件。如果 3 天之后邮件仍然没有传送，则会将邮件返回其创始者。

```
urgentnotices 2,4,6,8
```

对于优先级为紧急的邮件，将在 2、4 和 6 天之后发送瞬态失败通知。如果 8 天之后邮件仍然没有传送，则会将邮件返回其创始者。

注意，MTA 选项文件中的 RETURN_UNITS 选项使您可以以小时 (1) 或天 (0) 指定单位。默认设置为天 (0)。如果设置了 RETURN_UNITS=1，则需要安排返回作业每小时运行一次，并且每小时获取一次通知。当返回作业每小时运行一次时，它同时将每小时翻滚 mail.log* 文件一次。要防止每小时都翻滚 mail.log 文件，可以将 imta.tailor 文件中的 IMTA_RETURN_SPLIT_PERIOD 调整文件选项设置为 24。返回作业时间安排由 local.schedule.return_job configutil 参数控制。

如果没有指定 notices 关键字，则默认使用本地通道 1 的 notices 设置。如果未对本地通道进行设置，则将默认使用 notices 3, 6, 9, 12。

在状态通知邮件中包含已变更的地址

关键字：includefinal、 suppressfinal、 useintermediate。

MTA 生成通知邮件 （退回邮件、发送收据邮件等）时，可能同时存在可用于 MTA 的 “原始”格式的收件人地址和已变更的 “最终”格式的该收件人的地址。 MTA 始终会将原始格式 （假如存在）包含在通知邮件中，因为这是通知邮件的收件人（通知邮件所关心的原始邮件的发件人）最可能识别的一种格式。

includefinal 和 suppressfinal 通道关键字控制 MTA 是否还包含最终格式的地址。抑制包含最终格式的地址可能会符合要向外界 “隐藏”其内部的邮箱名称的站点的利益。此类站点可能只愿意在状态通知邮件中包含原始的 “外部”格式的地址。includefinal 是默认设置，包含最终格式的收件人地址。如果通知邮件中包含原始地址格式，则 suppressfinal 会使 MTA 抑制最终的地址格式。

useintermediate 关键字使用在列表扩展之后，但在用户邮箱名称生成之前生成的地址的中间格式。如果此信息不可用，则使用最终的格式。

对邮寄主管发送、阻塞和指定状态通知邮件

默认情况下，除非返回了错误，并使用空的 Errors-to: 标题行或空的信封 From: 地址完全抑制了警告，否则将向邮寄主管发送失败和警告状态通知邮件的副本。进一步精确地向邮寄主管传送通知邮件可以通过以下小节和表 10-11 中说明的大量通道关键字来控制。

返回的失败邮件

关键字：sendpost、 nosendpost、 copysendpost、 errsendpost。

由于长时间的服务故障或无效的地址，通道程序可能无法传送邮件。发生这种情况时， MTA 通道程序会将邮件返回给发件人，并附带有邮件未传送的原因的说明。可选地，所有失败的邮件的副本可以发送给本地邮寄主管。这对监视邮件故障十分有用，但是可能会导致邮寄主管必须处理过多的通信量。（请参见表 10-11。）

警告消息

关键字：warnpost、 nowarnpost、 copywarnpost、 errwarnpost。

除了返回邮件， MTA 还可以发送未传送邮件的详细警告。这种现象通常是由于 notices 通道关键字的设置而引起的超时所致，但是在某些情况下，通道程序可能在传送尝试失败后生成警告消息。警告消息包含故障和传送尝试持续时间的说明。大多数情况下，警告消息还包含有问题的邮件的标题和前几行。

可选地，所有警告邮件的副本可以发送给本地邮寄主管。在某种程度上，这对监视各个队列的状态十分有用，尽管它确实会产生大量要由邮寄主管处理的通信量。关键字 warnpost、 copywarnpost、 errwarnpost 和 nowarnpost 用于控制向邮寄主管发送警告消息。（请参见表 10-11。）

空的信封返回地址

关键字： returnenvelope

returnenvelope 关键字使用翻译为一组位标志的单个整数值。位 0 （值 = 1）控制由 MTA 生成的返回通知书写的是空的信封地址还是本地邮寄主管的地址。设置该位将强制使用本地邮寄主管地址，清除该位将强制使用空的地址。

注	RFC 1123 强制使用空的地址。但是，某些系统不能正确处理信封 From: 地址，但可能又需要使用此选项。

位 1 （值 = 2）控制 MTA 是否将所有空的信封地址都替换为本地邮寄主管的地址。此选项用于适应不符合 RFC 821、 RFC 822 或 RFC 1123 的非兼容系统。

位 2 （值 = 4）禁止句法上无效的返回地址。

位 3 （值 = 8）与 mailfromdnsverify 关键字相同。

邮寄主管返回的邮件内容

关键字：postheadonly、 postheadbody。

通道程序或定期邮件返回作业将邮件返回给邮寄主管和原始发件人时，邮寄主管副本可以是整个邮件，也可以只是标题。将邮寄主管副本限制为标题，可以进一步增加用户邮件的保密级别。但是，此操作本身并不保证邮件的安全性。邮寄主管和系统管理员通常可以使用超级用户系统权限 （如果他们这样选择）读取邮件内容。（请参见表 10-11。）

设置每个通道邮寄主管的地址

关键字：aliaspostmaster、 returnaddress、 noreturnaddress、 returnpersonal、 noreturnpersonal。

默认情况下，MTA 构造退回邮件或状态通知邮件时所使用的邮寄主管的返回地址为 postmaster@*local-host*，其中 *local-host* 为正式的本地主机名 （本地通道上的名称），邮寄主管的个人名称为 "MTA e-Mail Interconnect"。选择邮寄主管地址时应小心 — 非法的选择可能会导致快速的邮件循环并产生大量错误消息。

可以使用 RETURN_ADDRESS 和 RETURN_PERSONAL 选项设置 MTA 系统的默认邮寄主管地址和个人名称。或者，如果需要控制每个通道，可以使用 returnaddress 和 returnpersonal 通道关键字。 returnaddress 和 returnpersonal 都使用必需变量分别指定邮寄主管地址和个人名称。 noreturnaddress 和 noreturnpersonal 是默认设置，表示应使用默认值。这两个默认值是通过 RETURN_ADDRESS 和 RETURN_PERSONAL 选项或正常的默认值建立的 （如果未设置此选项）。

如果将 aliaspostmaster 关键字置于通道上，则按正式通道名寄往用户名 postmaster （小写、大写或大小写混合）的任何邮件都将重定向到 postmaster@*local-host*，其中 *local-host* 是正式的本地主机名 （本地通道上的名称）。注意， Internet 标准要求 DNS 中接收邮件的任何域均需具有用来接收邮件的有效邮寄主管帐户。因此，在需要集中邮寄主管的责任，而不是为单独的域设置单独的邮寄主管帐户时，该关键字是十分有用的。即，尽管 returnaddress 可以控制 MTA 从邮寄主管生成通知邮件时所使用的返回邮寄主管地址， aliaspostmaster 将影响 MTA 对寄往邮寄主管的邮件的处理。

表 10-11 用于将通知邮件发送给邮寄主管和发件人的关键字

关键字	**说明**
返回的邮件内容	**指定通知的地址**
notices	指定发送通知和返回邮件之前可能经历的时间。
nonurgentnotices	指定为非紧急优先级的邮件发送通知和返回邮件之前可能经历的时间。
normalnotices	指定为正常优先级的邮件发送通知和返回邮件之前可能经历的时间。
urgentnotices	指定为紧急优先级的邮件发送通知和返回邮件之前可能经历的时间。
返回的邮件	**如何处理返回邮件的错误通知。**
sendpost	启用向邮寄主管发送所有失败邮件的副本。
copysendpost	向邮寄主管发送错误通知的副本 （除非失败的邮件上的创始者地址为空），在这种情况下，邮寄主管将收到所有失败邮件的副本 （除本身实际上为退回邮件或通知邮件的那些邮件）。

表 10-11 用于将通知邮件发送给邮寄主管和发件人的关键字

关键字	说明
errsendpost	仅在无法将通知返回创始者时向邮寄主管发送错误通知的副本。如果指定了 nosendpost，则永远不会向邮寄主管发送失败的邮件。
nosendpost	禁用向邮寄主管发送所有失败邮件的副本。
警告消息	**如何处理警告消息。**
warnpost	启用向邮寄主管发送警告消息的副本。默认设置是向邮寄主管发送警告的副本 （除非使用空的 Warnings-to: 标题或空的信封 From: 地址。
copywarnpost	向邮寄主管发送警告消息的副本 （除非未传送邮件上的创始者地址为空）。
errwarnpost	在无法将通知返回创始者时向邮寄主管发送警告消息的副本。
nowarnpost	禁用向邮寄主管发送警告消息的副本。
返回的邮件内容	**指定向邮寄主管发送整个邮件，还是只发送标题。**
postheadonly	仅向邮寄主管返回标题。将邮寄主管副本限制为标题，可以进一步增加用户邮件的保密级别。但是，此操作并不保证邮件的安全性，因为邮寄主管和系统管理员可以使用超级用户系统权限 （如果他们这样选择）来读取邮件的内容。
postheadbody	同时返回邮件的标题和内容。
返回的邮件内容	**指定通知的地址**
includefinal	在传送通知中包含地址的最终格式 （收件人地址）。
returnenvelope	控制空的信封返回地址的使用。 returnenvelope 关键字使用翻译为一组位标志的单个整数值。 位 0 （值 = 1）控制由 MTA 生成的返回通知书写的是空的信封地址还是本地邮寄主管的地址。设置该位将强制使用本地邮寄主管地址，清除该位将强制使用空的地址。 位 1 （值 = 2）控制 MTA 是否将所有空的信封地址都替换为本地邮寄主管的地址。此选项用于适应不符合 RFC 821、 RFC 822 或 RFC 1123 的非兼容系统。 位 2 （值 = 4）禁止句法上无效的返回地址。 位 3 （值 = 8）与 mailfromdnsverify 关键字相同。
suppressfinal	抑制通知邮件中的最终地址格式 （如果通知邮件中存在原始地址格式）。
useintermediate	使用在列表扩展之后，但在用户邮箱名称生成之前生成的地址的中间格式。如果此信息不可用，则使用最终的格式。
返回的邮件内容	**指定通知的地址**
aliaspostmaster	将按正式的通道名称寄往 postmaster 用户名的邮件重定向至 postmaster@local-host，其中 local-host 是本地主机名 （本地通道上的名称）。
returnaddress	指定本地邮寄主管的返回地址。

表 10-11 用于将通知邮件发送给邮寄主管和发件人的关键字

关键字	说明
noreturnaddress	将 RETURN_ADDRESS 选项值用作邮寄主管地址名称。
returnpersonal	设置本地邮寄主管的个人名称。
noreturnpersonal	将 RETURN_PERSONAL 选项值用作邮寄主管个人名称。

控制邮件处理通知

邮件处理通知 (MDN) 是由 MTA 发送给发件人和 / 或邮寄主管的电子邮件报告，内容是邮件的传送处理。例如，如果邮件被 Sieve 过滤器拒绝，将给发件人发送 MDN。 MDN 也称为已读回执、确认、回执通知或发送收据。 Sieve 脚本撰写语言通常用于邮件传送过滤和休假邮件。

自定义和本地化邮件处理通知邮件

修改和本地化 MDN 的说明与自定义和本地化传送状态通知邮件的说明类似，两者只有一些细微的差别 （如下所述）。（请参见第 242 页的 “自定义和本地化传送状态通知邮件”和第 245 页的 “将生成的通知国际化”。）

此映射 （称为 DISPOSITION_LANGUAGE 映射）与用于国际化状态通知的 notification_language 映射表 （代码示例 10-2 第 244 页）类似。

但是，采用如下的格式探测 MDN：

```
type|modifiers|source-channel|header-language|return|recipient
```

其中：

type 是处理类型，可为下列类型之一：displayed、 dispatched、 processed、 deleted、 denied 或 failed。

modifiers 是以逗号分隔的处理修饰符列表。当前列表为：error、 warning、 superseded 和 expired。

source-channel 是生成 MDN 的源频道。

header-language 是下列之一指定的语言：accept-language、 preferred-language 或 x-accept-language。（MTA 使用这些选项中存在的第一个选项。）

return 是通知的返回地址。

recipient 是处理针对的地址。

处理映射的结果由两条或三条信息组成，各条信息之间用垂直条 (|) 分隔。第一条信息是该处理通知的模板文件的存放目录。第二条信息是独立的处理文本应该强制转换成的字符集。（此信息是必需的，因为一些处理，特别是由自动回复生成的处理或在休假 Sieve 操作中使用 :mime 参数生成的处理，不使用模板文件，从而不能从模板文件中继承字符集。）最后，第三条信息是通知的替换主题行。此信息只有当映射还设置了 $T 标志时才使用。

下面附加的模板文件用于构建 MDN：

```
disposition_deleted.txt disposition_failed.txt
disposition_denied.txt disposition_prefix.txt
disposition_dispatched.txt disposition_processed.txt
disposition_displayed.txt disposition_suffix.txt
disposition_option.opt
```

这些模板文件的使用与状态通知邮件的各种 return_*.txt 文件的使用类似。*.txt 文件的邮件文本应限制为每行 78 个字符。

第 11 章

配置重写规则

本章说明如何在 imta.cnf 文件中配置重写规则。如果您还未阅读过第 10 章 “关于 MTA 服务和配置”，则应该在阅读本章前阅读这一章。

本章包含以下各节：

- 第 256 页的 “重写规则结构”
- 第 257 页的 “重写规则模式和标记”
- 第 260 页的 “重写规则模板”
- 第 262 页的 “MTA 如何将重写规则应用到地址”
- 第 267 页的 “模板替换和重写规则控制序列”
- 第 278 页的 “处理大量的重写规则”
- 第 278 页的 “测试重写规则”
- 第 279 页的 “重写规则示例”

Messaging Server 的地址重写工具是处理和更改地址的主机部分或域部分的主要工具。 Messaging Server 提供了用于地址操作的其他工具，如别名、地址逆向数据库及专用的映射表。但为了获得最佳性能，在可以执行地址操作时应使用重写规则。

注 在对 imta.cnf 文件中的重写规则进行更改时，您必须在装入配置数据的所有程序或频道启动时仅重新启动它们一次 — 例如通过使用 imsimta restart 命令重新启动 SMTP 服务器。如果使用的是编译的配置，则必须重新编译然后再重新启动。

有关编译配置信息和启动程序的详细信息，请参见 Messaging Server Reference Manual。

重写规则结构

重写规则显示在 MTA 配置文件 imta.cnf 的上半部分中。配置文件中的每个规则都以单行显示。各个规则之间允许有注释但不允许有空白行。重写规则以空白行结束，其后跟通道定义。以下示例显示了部分配置文件的重写规则部分。

```
! test.cnf - An example configuration file.
!
! This is only an example of a configuration file.It serves
! no useful purpose and should not be used in a real system.
!
a.com   $U@a-host
b.org   $U@b-host
c.edu   $U%c@b-daemon
d.com   $U%d@a-daemon

!Begin channel definitions
```

重写规则由两部分组成：模式，然后是等值字符串或**模板**。尽管每个部分内部不允许有空格但这两部分必须用空格分隔。重写规则的结构如下所示：

```
pattern  template
```

pattern

表示要在域名中搜索的字符串。在表 11-3 中，模式为 a.com、b.org、 c.edu 和 d.com。

如果模式与地址的域部分匹配，则重写规则适用于该地址。模式和模板必须用空白区域分隔。有关模式语法的详细信息，请参见第 257 页的 “重写规则模式和标记”。

template

为以下模板之一：

UserTemplate%*DomainTemplate*@*ChannelTag* [*controls*]

UserTemplate@*ChannelTag* [*controls*]

UserTemplate%*DomainTemplate* [*controls*]

UserTemplate@*DomainTemplate*@*ChannelTag* [*controls*]

UserTemplate@*DomainTemplate*@*SourceRoute*@*ChannelTag* [*controls*]

其中

UserTemplate 指定重写地址的用户部分的方法。替换序列可用于表示原始地址的部分或数据库查找的结果。替换序列将被替换为其表示的内容以构造重写地址。在表 11-4 中，使用的是 $U 替换序列。有关更多信息，请参见第 267 页的 “模板替换和重写规则控制序列”。

DomainTemplate 指定重写地址的域部分的方法。类似 *UserTemplate*，*DomainTemplate* 也可以包含替换序列。

ChannelTag 表示此邮件要发送到的通道。（所有通道定义必须包含通道标记和通道名称。通道标记通常显示在重写规则及其通道定义中。）

controls 使用控件可以限制规则的适用性。某些控件序列必须在规则的开始部分显示；其他控件必须在规则的结尾部分显示。有关控件的详细信息，请参见第 267 页的 “模板替换和重写规则控制序列”。

有关模板语法的详细信息，请参见第 260 页的 “重写规则模板”。

重写规则模式和标记

本节包含以下几个部分：

- 第 259 页的 “与百分比黑客匹配的规则”
- 第 259 页的 “与 Bang 式样 (UUCP) 地址匹配的规则”
- 第 260 页的 “与任何地址匹配的规则”
- 第 260 页的 “标记的重写规则集”

大多数重写规则模式包含将只与某主机匹配的特定主机名或将与整个子域中的任何主机 / 域匹配的子域模式。

例如，以下重写规则模式包含将只与特定主机匹配的特定主机名：

```
host.siroe.com
```

下一个重写规则模式包含将与整个子域中的任何主机或域匹配的子域模式：

```
.siroe.com
```

但该模式将不会与确切的主机名 `siroe.com` 匹配；要与确切的主机名 `siroe.com` 匹配，需要一个单独的 `siroe.com` 模式。

MTA 将尝试从特定主机名开始重写主机 / 域名，然后逐渐地将该名称一般化以使其不太特别。这意味着将优先使用较特定的重写规则模式，而不是较一般的重写规则模式。例如，假设在配置文件中存在以下重写规则模式：

```
hosta.subnet.siroe.com
.subnet.siroe.com
.siroe.com
```

基于不同的重写规则模式，地址 jdoe@hosta.subnet.siroe.com 将与 hosta.subnet.siroe.com 重写规则模式匹配；地址 jdoe@hostb.subnet.siroe.com 将与 .subnet.siroe.com 重写规则模式匹配；地址 jdoe@hostc.siroe.com 将与 .siroe.com 重写规则模式匹配。

特别是，包含子域重写规则模式的重写规则的使用对于 Internet 上的站点是常用的。这样的站点通常具有许多用于其内部主机和子网的重写规则，并且还将顶层 Internet 域的重写规则包括在其文件 internet.rules (*msg_svr_base*/config/internet.rules) 的配置中。

要确保正确重写 Internet 目的地 （不是通过较特定的重写规则处理的内部主机目的地）的邮件并将其路由到外发 TCP/IP 通道，请确保 imta.cnf 文件包含：

- 其模式与顶层 Internet 域匹配的重写规则
- 用于重写地址使该类模式与外发 TCP/IP 通道匹配的模板

```
!    Ascension Island
.AC                       $U%$H$D@TCP-DAEMON
. [text
.     removed for
.             brevity]
!      Zimbabwe
.ZW                           $U%$H$D@TCP-DAEMON
```

IP 域文字遵循类似的分层匹配模式，但是从右向左 （而不是从左向右）匹配。例如，以下模式仅与并完全与 IP 文字 [1.2.3.4] 匹配：

```
[1.2.3.4]
```

下一个模式与 1.2.3.0 子网中的任何文字匹配：

```
[1.2.3.]
```

除了已经介绍的比较常用的几种主机或子域重写规则模式以外，重写规则也可以使用几种特殊模式，在表 11-1 中概括了这些模式并将在以下小节中对其进行介绍。

表 11-1 重写规则的特殊模式摘要

模式	说明 / 用法
$*	匹配任何地址。如果指定此规则，则将首先尝试该规则而不考虑其在文件中的位置。
$%	百分比黑客规则。与 A%B 形式的任何主机 / 域说明匹配。
$!	Bang 式样规则。与 B!A 形式的任何主机 / 域说明匹配。
[ ]	IP 文字全匹配规则。与任何 IP 域文字匹配。
.	与任何主机 / 域说明匹配。例如， joe@[129.165.12.11]

除了这些特殊模式以外， Messaging Server 还具有**标记**的概念，标记可能会显示在重写规则模式中。当某个地址可能被重写多次，并且根据以前的重写，必须通过控制与该地址匹配的重写规则在后续重写中进行区分的情况下，将使用这些标记。有关更多信息，请参见第 260 页的 “标记的重写规则集”。

与百分比黑客匹配的规则

如果 MTA 尝试重写 A%B 形式的地址时失败，则其将在失败以及将该地址形式视为 A%B@localhost 之前尝试一个附加规则。（有关这些地址形式的详细信息，请参见第 260 页的 “重写规则模板”。）此附加规则是**百分比黑客规则**。其模式为 $%。该模式从不会更改。只有在包含百分比符号的本地部分以任何其他方法 （包括以下介绍的全匹配规则）重写均失败时，该规则才有效。

百分比黑客规则可用于将某个特殊的内部含义指定到百分比黑客地址。

与 Bang 式样 (UUCP) 地址匹配的规则

如果 MTA 尝试重写 B!A 形式的地址时失败，则此 MTA 将在失败并将该地址形式视为 B!A@localhost 之前尝试一个附加规则。此附加规则是 *bang* **式样规则**。其模式为 $!。该模式从不会更改。只有在包含感叹号的本地部分以任何其他方法 （包括以下介绍的默认规则）重写均失败时，该规则才有效。

bang 式样规则可用于将 UUCP 式样的地址强制路由到具有 UUCP 系统和路由选择的全面知识的系统。

与任何地址匹配的规则

如果没有其他规则与主机 / 域说明匹配并且无法在通道表中找到主机 / 域说明，则特殊模式 "." （单个句点）将与任何主机 / 域说明匹配。也就是说，当其他方法的地址重写失败时， ”.” 规则将作为最后的方法。

注 关于替换序列，当全匹配规则匹配并且其模板扩展时， $H 将扩展为全主机名，$D 将扩展为单个点 "."。因此 $D 在全匹配规则模板中的使用将受到限制！

标记的重写规则集

随着重写进程的继续，可能适合使用不同的规则集。这是通过使用重写规则标记来实现的。在配置文件或域数据库中查找当前标记之前，该标记已前置于每个模式。通过使用重写规则模板 （下面将介绍）中的 $T 替换字符串可以用匹配的任何重写规则更改该标记。

标记有些麻烦；设置标记之后，它们将不断应用到从单个地址提取的所有主机。这意味着在使用所有标记后，必须谨慎提供以正确的标记值开头的备用规则。实际上这几乎不是什么问题，因为标记通常只用于非常专用的应用程序中。重写完地址后，标记将被重置为默认标记 — 空的字符串。

依照约定，所有标记值都以垂直条 | 结束。该字符在标准地址中不使用，因此可以在模式的其余部分随意勾画标记。

重写规则模板

以下各节将详细介绍重写规则的模板格式。表 11-2 汇总了模板的格式。

表 11-2 重写规则的模板格式摘要

模板	页	用法
A%B	261	A 将变为新的用户 / 邮箱名称，B 将变为新的主机 / 域说明，再次重写。
A@B	261	将被视为 A%B@B。
A%B@C	261	A 将变为新的用户 / 邮箱名称，B 将变为新的主机 / 域说明，路由到与主机 C 相关联的通道。
A@B@C	261	将被视为 A@B@C@C。
A@B@C@D	261	A 将变为新的用户 / 邮箱名称，B 将变为新的主机 / 域说明，插入 C 作为源路由，路由到与主机 D 相关联的通道。

普通重写模板：A%B@C 或 A@B

以下模板是最常用的模板形式。规则适用于地址的用户部分和地址的域部分。然后使用新地址将邮件路由到一个特定通道 （由 *ChannelTag* 表示）。

UserTemplate%*DomainTemplate*@*ChannelTag* [*controls*]

下一个模板形式在应用方面与最常用的模板形式相同。但此模板形式只有在 *DomainTemplate* 和 *ChannelTag* 相同时才可用。

UserTemplate@*ChannelTag* [*controls*]

重复的重写模板 A%B

以下模板格式用于元规则，这些规则在规则应用后需要附加的重写。规则应用后，将在产生的新地址上重复整个重写进程。（所有其他重写规则格式会导致重写进程在规则应用后终止。）

UserTemplate%*DomainTemplate* [*controls*]

例如，以下规则可以将 `.removable` 域的所有事件从地址的结尾删除：

```
.removable      $U%$H
```

使用这些重复规则时必须非常谨慎；使用疏忽可能会创建一个 “规则循环”。因此，只有在绝对必要时才应使用元规则。确保使用 `imsimta test -rewrite` 命令来测试元规则。有关 `test -rewrite` 命令的详细信息，请参见 Messaging Server Reference Manual。

指定的路由重写模板 A@B@C@D 或 A@B@C

以下模板格式与较常用的模板 *UserTemplate*%*DomainTemplate*@*ChannelTag* 的使用方法相同 （注意第一个分隔符的区别），除了 *ChannelTag* 作为源路由被插入地址中。然后邮件被路由到 *ChannelTag*：

UserTemplate@*DomainTemplate*@*Source-Route*
@*ChannelTag* [*controls*]

重写的地址变为 @*route*:*user*@*domain*。以下模板也有效：

UserTemplate@*DomainTemplate*@*ChannelTag* [*controls*]

例如，以下规则将把地址 `jdoe@com1` 重写到源路由的地址 `@siroe.com:jdoe@com1`。通道标记将变为 `siroe.com`：

```
com1 $U@com1@siroe.com
```

重写规则模板中的大小写区分

与重写规则中的模式不同，模板中的字符大小写将被保留。当使用重写规则为区分字符大小写的邮件系统提供接口时，这是必要的。请注意类似 $U 和 $D 的替换序列（替换从地址提取的材料）也将保留字符的原始大小写。

在需要强制被替换的材料使用特定的大小写时 （如在 UNIX 系统中强制邮箱为小写），在模板中可以使用特殊的替换序列以强制被替换的材料为所需的大小写。具体来说， $\ 强制后续被替换的材料为小写， $^ 强制后续被替换的材料为大写，而 $_ 则要求使用原始的大小写。

例如，您可以使用以下规则来强制 unix.siroe.com 地址的邮箱为小写：

```
unix.siroe.com    $\$U$_%unix.siroe.com
```

MTA 如何将重写规则应用到地址

以下步骤介绍 MTA 如何将重写规则应用到给定地址：

1. MTA 从地址中提取第一个主机说明或域说明。

   一个地址可以指定多个主机或域名，如下例所示：

   jdoe%hostname@siroe.com。

2. 识别了第一个主机或域名后， MTA 将进行搜索，扫描其模式与主机或域名匹配的重写规则。

3. 找到匹配的重写规则后， MTA 将根据该规则的模板部分重写地址。

4. 最后， MTA 会将通道标记和与每个通道相关联的主机名进行比较。

   如果找到匹配， MTA 会将邮件排入相关联的通道中；否则该重写进程将失败。如果匹配的通道为本地通道，则会通过查找别名数据库和别名文件来进行地址的某个附加的重写。

在下个小节中将更加详细地介绍这些步骤。

注 使用不属于任何现有通道的通道标记将导致其地址与此规则匹配的邮件被退回。也就是使匹配的邮件无法路由。

步骤 1. 提取第一个主机或域说明

重写地址的进程通过从地址中提取第一个主机或域说明开始。（建议不熟悉 RFC 822 地址约定的读者阅读该标准以便理解以下讨论内容。）扫描地址中的主机 / 域说明的顺序如下所示：

1. 源路由中的主机 （从左向右读取）
2. 主机显示在 "at" 符号 (@) 的右侧
3. 主机显示在最后单个百分比符号 (%) 的右侧
4. 主机显示在第一个感叹号 (!) 的左侧

如果 bangoverpercent 关键字在正进行地址重写的通道上有效 （即如果尝试排队信息的通道自身被标上 bangoverpercent 通道关键字），则最后两个项目的顺序将被切换。

表 11-3 中显示了可以首先提取的一些地址和主机名的示例。

表 11-3 提取的地址和主机名

地址	第一个主机域说明	注释
user@a	a	“简短形式”域名。
user@a.b.c	a.b.c	“全限定”域名 (FQDN)。
user@[0.1.2.3]	[0.1.2.3]	“域文字”。
@a:user@b.c.d	a	带有简短形式域名 "route" 的源路由的地址。
@a.b.c:user@d.e.f	a.b.c	源路由的地址；路由部分被完全限定。
@[0.1.2.3]:user@d.e.f	[0.1.2.3]	源路由的地址；路由部分是域文字。
@a,@b,@c:user@d.e.f	a	带有 a 到 b 到 c 路由的源路由的地址。
@a,@[0.1.2.3]:user@b	a	在路由部分中带有域文字的源路由的地址。
user%A@B	B	这个不标准的路由形式称为 “百分比黑客”。
user%A	A	
user%A%B	B	
user%%A%B	B	
A!user	A	“Bang 式样”寻址；通常用于 UUCP。
A!user@B	B	

表 11-3 提取的地址和主机名 （续）

地址	第一个主机域说明	注释
A!user%B@C	C	
A!user%B	B	nobangoverpercent 关键字为活动的；默认值。
A!user%B	A	bangoverpercent 关键字为活动的。

RFC 822 不在地址中对感叹号 (！) 和百分比符号 (%) 进行解释。如果 at 符号不存在，百分比符号通常与 at 符号 (@) 的解释方法相同，因此 Messaging Server MTA 采用了该约定。

重复的百分比符号的特殊解释用于允许将百分比符号作为本地用户名的部分；在处理某些外部邮件系统地址时这可能会有用。感叹号的解释符合 RFC 976 的 “bang 式样”地址约定，因此可以在 Messaging Server MTA 中使用 UUCP 地址。

RFC 822 或 RFC 976 都没有指定这些解释的顺序，因此可以使用 bangoverpercent 和 nobangoverpercent 关键字来控制执行重写的通道应用这些解释的顺序。尽管在某些情况下其他设置可能会有用，但默认设置更 “标准”一些。

注 不建议在地址中使用感叹号 (!) 或百分比符号 (%)。

步骤 2. 扫描重写规则

从地址中提取出第一个主机或域说明后， MTA 将咨询重写规则以找出要执行的操作。将主机 / 域说明与每个规则的模式部分 （即每个规则的左侧）进行比较。该比较不区分大小写。RFC 822 规定不区分大小写。MTA 不区分大小写，但在可能的情况下将保留大小写。

如果主机或域说明与任何模式均不匹配，即所谓的 “与任何规则均不匹配”的情况，则主机或域说明的第一个部分 （第一个句点前的部分，通常是主机名）将被删除并用星号 (*) 替换，然后将再次尝试以查找产生的主机或域说明，但只在配置文件重写规则中查找 （不咨询域数据库）。

如果此操作失败，则会删除第一个部分并重复该过程。如果此操作也失败了，则会删除下一个部分 （通常为子域），重写程序会再次尝试，首先带星号然后不带星号。包含星号的所有探测只在配置文件重写规则表中进行；不检查域数据库。此过程将继续，直到找到匹配或用尽整个主机或域说明。此过程的作用是尝试首先与最为特别的域匹配，然后逐渐与不太特别和比较一般的域匹配。

从倾向于算法的角度看，此匹配过程为：

- 主机 / 域说明被用作比较字符串 spec_1 和 spec_2 的初始值。（例如， spec_1 = spec_2 = a.b.c）。
- 比较字符串 spec_1 与配置文件中每个重写规则的模式部分进行比较，然后与域数据库比较直到找到匹配。如果找到了匹配则将退出匹配过程。
- 如果未找到匹配，则 spec_2 最左侧的非星号部分将被转换成星号。例如，如果 spec_2 为 a.b.c，则将被更改为 *.b.c ；如果 spec_2 为 *.b.c，则将被更改为 *.*.c。如果找到了匹配则会退出匹配过程。
- 如果未找到匹配，则比较字符串 spec_1 的第一部分 （包括任何前导句点）将被删除。如果 spec_1 只有一个部分 （如 .c 或 c），则该字符串将被单个句点 "." 替换。如果产生的字符串 spec_1 的长度为非零值，则您将返回步骤 1。如果产生的字符串的长度为零 （例如为先前的 "."），则查找进程已失败并且您将退出匹配过程。

例如，假设地址 dan@sc.cs.siroe.edu 将被重写。这将导致 MTA 按照给定的顺序查找以下模式：

```
sc.cs.siroe.edu
*.cs.siroe.edu
.cs.siroe.edu
*.*.siroe.edu
.siroe.edu
*.*.*.edu
.edu
*.*.*.*
.
```

步骤 3. 根据模板重写地址

主机 / 域说明与某个重写规则匹配后，将使用该规则的模板部分进行重写。模板指定了三个内容：

1. 地址的新用户名。
2. 地址的新的主机 / 域说明。
3. 用于识别现有 MTA 通道 （该地址的邮件应该发送到此通道）的通道标记。

步骤 4. 完成重写进程

主机 / 域说明重写后可能会出现下面两种情况之一。

- 如果通道标记既不与本地通道关联也不与标记了 routelocal 通道关键字的通道关联，或者地址中没有附加的主机 / 域说明，则重写的说明将被替换为替换原始说明 （为进行重写而提取的）的地址，并且重写进程将终止。
- 如果通道标记与本地通道或标记了 routelocal 的通道关联，并且在地址中显示了附加的主机 / 域说明，则重写的地址将被放弃，将从地址中删除原始 （初始）主机 / 域说明，并从地址中提取新的主机 / 域说明，然后重复整个过程。重写将继续直到用尽所有主机 / 域说明或找到一个通过非本地、非 routelocal 通道的路由。此重复机制就是 MTA 为源路由提供支持的方式。实际上，通过本地系统和 routelocal 系统的多余的路由都通过此进程从地址中删除了。

重写规则失败

如果主机 / 域说明无法与任何重写规则匹配并且不存在默认规则时， MTA 将使用“原样”说明；例如原始说明将变成新的说明和路由系统。如果地址中包含无意义的主机 / 域说明，则当路由系统不匹配与任何通道相关联的任何系统名时，将检测出该说明并将邮件退回。

重写后的语法检查

重写规则应用到地址后不进行附加的语法检查。这是有意的 — 这样可以使用重写规则将地址转换成不符合 RFC 822 的格式。但是，这也意味着配置文件中的错误可能会导致邮件为 MTA 留下不正确或非法的地址。

处理域文字

在重写进程中将对域文字进行特殊的处理。如果地址的域部分中显示的域文字与某个重写规则模式不匹配，则该文字将被解释为由句点分隔并由方括号括起来的一组字符串。最右侧的字符串将被删除并会重复进行搜索。如果此操作不起作用则将删除下一个字符串，以此类推直到只剩下空括号。如果搜索空括号失败，则会删除整个域的文字并会对域地址的下一个部分 （如果该部分存在）继续进行重写。域文字的内部处理中不使用星号；由星号替换整个域文字时，星号的数量与域文字中的元素的数量相对应。

类似标准的域或主机说明，也是按最特定到最不特定的顺序尝试对域文字进行处理。其模式与域文字相匹配的第一个规则将是用来重写主机或域说明的规则。如果规则列表中有两个相同的模式，则会使用首先显示的模式。

例如，假设地址 dan@[128.6.3.40] 将被重写。重写程序将查找 [128.6.3.40]，然后查找 [128.6.3.]，接着查找 [128.6.]，然后再查找 [128.]，接下来将查找 []，之后会查找 [*.*.*.*]，最后查找全匹配规则 "."。

模板替换和重写规则控制序列

替换用于通过将字符串插入到重写的地址中来重写用户名或地址，替换的值由所用的特定替换序列确定。本节包含以下几个部分：

- 第 270 页的 “用户名和子地址替换， $U、 $0U、 $1U”
- 第 270 页的 “主机 / 域和 IP 文字替换， $D、 $H、 $nD、 $nH、 $L”
- 第 271 页的 “文字字符替换， $$、 $%、 $@”
- 第 271 页的 “LDAP 查询 URL 替换， $]...[”
- 第 272 页的 “常规数据库替换， $(...)”
- 第 273 页的 “应用指定的映射， ${...}”
- 第 273 页的 “用户提供的例程替换， $[...]”
- 第 274 页的 “单个字段替换， $&、 $!、 $*、 $#”
- 第 274 页的 “唯一字符串替换”
- 第 275 页的 “特定于源通道的重写规则 （$M、 $N）”
- 第 275 页的 “特定于目标通道的重写规则 ($C, $Q)”
- 第 276 页的 “特定于主机位置的重写 （$A、 $P、 $S、 $X）”
- 第 277 页的 “更改当前标记值， $T”
- 第 277 页的 “控制与重写 ($?) 相关联的错误消息”

例如，在以下模板中， $U 是一个替换序列。该替换序列将导致被重写的地址的 *username* 部分被替换成模板的输出。因此，如果 jdoe@mailhost.siroe.com 被此模板重写，产生的输出将会是 jdoe@siroe.com， $U 将在 *username* 部分替换原始地址的 jdoe：

```
$U@siroe.com
```

控制序列为给定重写规则的适用性强加了附加条件。不仅重写规则的模式部分必须与要检查的主机或域说明匹配，而且要重写的地址的其他方面也必须满足由控制序列设置的条件。例如， $E 控制序列要求被重写的地址为信封地址，而 $F 控制序列要求其为正向指示地址。以下重写规则仅适用于 （重写） user@siroe.com 形式的信封 To: 地址：

```
siroe.com $U@mail.siroe.com$E$F
```

如果域或主机说明与某个重写规则的模式部分匹配，但不满足该规则的模板中由控制序列强加的所有条件，则该重写规则将失败，重写程序将继续查找其他适用的规则。

表 11-4 汇总了模板替换和控制序列。

表 11-4 重写规则模板替换和控制序列的摘要

替换序列	替换
$D	匹配的域说明的部分。
$H	不匹配的主机 / 域说明的部分；模式中的点的左侧。
$L	不匹配的域文字的部分；模式文字中的点的右侧。
$U	原始地址中的用户名。
$nA	插入从位置 0 开始的当前地址左侧第 n 个字符，如果忽略 n，则将插入整个地址。
$nX	插入从 0 开始的邮件主机左侧第 n 个组件，如果忽略 n，则将插入整个邮件主机。
$0U	原始地址中的本地部分 （用户名），减去任何子地址。
$1U	原始地址的本地部分 （用户名）中的子地址 （如果存在）。
$$	插入文字美元符号 ($)。
$%	插入文字百分比符号 (%)。
$@	插入文字 at 符号 (@)。
$\	强制材料为小写。
$^	强制材料为大写。
$_	使用原始大小写。
$=	强制后续替换字符经适当引用插入到 LDAP 搜索过滤器中。材料为大写。
$W	在随机、唯一的字符串中替换。
$]...[	LDAP 搜索 URL 查找。
$ （文本）	常规数据库替换；如果查找失败则规则失败。
${...}	将指定的映射应用于提供的字符串。

表 11-4 重写规则模板替换和控制序列的摘要 （续）

替换序列	替换
$[...]	调用用户提供的例程；在结果中替换。
$&*n*	不匹配的 （或通配的）主机的第 *n* 个部分，由 0 开始从左向右数。
$!*n*	不匹配的 （或通配的）主机的第 *n* 个部分，由 0 开始从右向左数。
$**n*	匹配模式的第 *n* 个部分，由 0 开始从左向右数。
$#*n*	匹配模式的第 *n* 个部分，由 0 开始从右向左数。
$*n*D	匹配的域说明的部分，保留从 0 开始的第 n 个最左侧部分
$*n*H	不匹配的主机 / 域说明的部分，保留从 0 开始的第 n 个最左侧部分
控制序列	**对重写规则的作用**
$1M	只有当通道为内部重新处理通道时才适用。
$1N	只有当通道不是内部重新处理通道时才适用。
$1~	执行所有待定通道匹配检查。如果检查失败将会成功地终止当前重写规则模板的处理。
$A	如果主机在 at 符号的右侧则适用
$B	只适用于标题 / 主体地址
$C *channel*	如果发送到 *channel* 将失败
$E	只适用于信封地址
$F	只适用于正向指引的 （如 To:）地址
$M *channel*	只在 *channel* 重写地址时适用
$N *channel*	如果 *channel* 正在重写地址则将失败
$P	如果主机在百分比符号的右侧则适用
$Q *channel*	如果发送到 *channel* 则适用
$R	只适用于逆向指引的 （如 From:）地址
$S	如果是源路由的主机则适用
$T*newtag*	将重写规则标记设置为 newtag
$V*host*	如果未在 LDAP 目录（在 DC 树中或作为虚拟域）中定义主机名则会失败。如果 LDAP 搜索超时，主机名后面的字符之后紧跟的重写模式的剩余部分将会被 MTA 选项字符串 DOMAIN_FAILURE 替换。
$X	如果主机在感叹号的左侧则适用
$Z*host*	如果在 LDAP 目录（在 DC 树中或作为虚拟域）中定义了主机名则会失败。如果 LDAP 搜索超时，主机名后面的字符之后紧跟的重写模式的剩余部分将会被 MTA 选项字符串 DOMAIN_FAILURE 替换。
$?*errmsg*	如果重写失败，将返回 *errmsg* 而不是默认的错误消息。错误消息必须为 US ASCII。

表 11-4 重写规则模板替换和控制序列的摘要 （续）

替换序列	替换
$*number*?*errmsg*	如果重写失败将返回 *errmsg* 而不是默认错误消息，并将 SMTP 扩展的错误代码设置为 *a.b.c*： • *a* 是 *number*/1000000 的第一个数字 • *b* 是 *number*/1000 的余数的第 2 个到第 4 个数字的值 • *c* 是 *number* 除以 1000 的余数的最后三个数字的值。 以下示例将错误代码设置为 3.45.89： `$3045089?the snark is a boojum`

用户名和子地址替换， $U、 $0U、 $1U

模板中出现的所有 $U 都将被原始地址的用户名 （RFC 822 “本地部分”）替换。注意， a.“b”形式的用户名将被 “a.b”形式的用户名替换，因为 RFC2822 不支持 RFC 822 的前一种语法，并期望后一种用法将来能成为强制性的语法。

模板中出现的所有 $0U 都将被原始地址的用户名替换，减去任何子地址和子地址指示字符 (+)。模板中出现的所有 $1U 都将被原始地址的子地址和子地址指示字符（如果存在）替换。因此请注意， $0U 和 $1U 是用户名的补充部分， $0U$1U 与简单 $U 等效。

主机 / 域和 IP 文字替换，$D、$H、$nD、$nH、$L

出现的所有 $H 都将被与规则不匹配的主机 / 域说明部分替换。出现的所有 $D 都将被与重写规则匹配的主机 / 域说明部分替换。$nH 和 $nD 字符是保留从 0 开始数的第 n 个最左侧部分的标准 $H 或 $D 部分的变体。即 $nH 和 $nD 分别省略了通常为 $H 或 $D 替换的最左侧的 n 部分 （从 1 开始数）。特别是， $0H 与 $H 等效， $0D 与 $D 等效。

例如，假设地址 `jdoe@host.siroe.com` 与以下重写规则匹配：

```
host.siroe.com     $U%$1D@TCP-DAEMON
```

产生的地址是 `jdoe@siroe.com`，该地址将 `TCP-DAEMON` 作为外发通道。其中 $D 将在匹配的整个域 `host.siroe.com` 中进行替换，而 $1D 将在从第一部分 （第一部分为 `siroe`）开始的匹配的部分中进行替换，即，在 `siroe.com` 中进行替换。

$L 将替换与重写规则不匹配的域文字部分。

文字字符替换， $$、 $%、 $@

$、 % 和 @ 字符通常是重写规则模板中的元字符。要执行此类字符的文字插入，请为其引上美元字符 $。即， $$ 扩展成单个美元符号 $ ； $% 扩展成单个百分比 %（这种情况下不将百分比解释为模板字段分隔符）； $@ 扩展成单个 at 符号 @（也不解释为字段分隔符）。

LDAP 查询 URL 替换， $]...[

$]ldap-url[形式的替换被解释为 LDAP 查询 URL，并且 LDAP 查询的结果将被替换。使用标准 LDAP URL 时省略了主机和端口。而主机和端口在 msg.conf 文件（local.ldaphost 和 local.ldapport 属性）中指定。

即，应该按如下所示指定 LDAP URL，其中方括号字符 [ ] 表示 URL 的可选部分：

```
ldap:///dn[?attributes[?scope?filter]]
```

dn 是必需的独特名称，用于指定搜索基准。 URL 的可选属性、范围和过滤器部分进一步完善了要返回的信息内容。对于重写规则，指定返回所需的属性可能是 mailRoutingSystem 属性 （或某个类似的属性）。范围可能是任意基准 （默认设置）、某个基准或子基准。所需的过滤器可能会请求返回其 mailDomain 值与要被重写的域匹配的对象。

如果 LDAP 目录模式包括属性 mailRoutingSystem 和 mailDomain，则确定要将给定种类的地址路由到哪个系统的可能的重写规则可能会显示如下，其中 LDAP URL 替换序列 $D 用于将当前域名替换到构造的 LDAP 查询中：

```
.siroe.com \
  $U%$H$D@$]ldap:///o=siroe.com?mailRoutingSystem?sub?\
  (mailDomain=$D)
```

为了便于读取，使用了反斜杠字符将单个逻辑重写规则行继续到第二个物理行。表 11-5 列出了 LDAP URL 替换序列。

表 11-5 LDAP URL 替换序列

替换序列	说明
$$	文字 $ 字符
$~ 帐户	用户帐户的主目录
$A	地址

表 11-5 LDAP URL 替换序列

替换序列	说明
$D	域名
$H	主机名 （全限定域名的第一部分）
$L	用户名减去任何特殊的前导字符，如 ~ 或 _
$S	子地址
$U	用户名

MTA 现在高速缓存在重写规则和映射中查找到的 URL 结果。这个新的 URL 结果高速缓存由两个新的 MTA 选项控制， URL_RESULT_CACHE_SIZE （默认为 10000 个条目）和 URL_RESULT_CACHE_TIMEOUT （默认为 600 秒）。

常规数据库替换， $(...)

$ （文本）形式的替换要特殊处理。文本部分被用作访问特殊的常规数据库的密钥。该数据库包括在 /imta/config/imta_tailor 文件中通过 IMTA_GENERAL_DATABASE 选项指定的文件，这个文件通常是 /imta/db/generaldb.db。

该数据库由 imsimta crdb 实用程序生成。如果在数据库中找到了 “文本字符串”，则数据库中相应的模板将被替换。如果 “文本字符串”与数据库中的任何项都不匹配，则重写进程失败；这就相当于重写规则根本从未匹配过。如果替换成功，则从数据库中提取的模板将被重新扫描以进行附加替换。但是，提取的模板中的附加 $ （文本）替换会被禁止以防止没完没了的递归引用。

例如，假设地址 jdoe@siroe.siroenet 与以下重写规则匹配：

```
.SIROENET $($H)
```

则将在常规数据库中查找文本字符串 siroe，并且查找的结果 （如果存在）将用于重写规则的模板。假设查找 siroe 的结果为 $u%eng.siroe.com@siroenet。则模板的输出将会是 jdoe@eng.siroe.com （即，用户名 = jdoe、主机 / 域说明 = eng.siroe.com），路由系统将是 siroenet。

如果常规数据库存在，则其应该是全局可读的以确保正常运行。

应用指定的映射， ${...}

form.SIROENET $($H) ${mapping,argument} 的替换是用于从 MTA 映射文件中查找并应用映射。mapping 字段指定要使用的映射表的名称，而 argument 指定要传送到映射的字符串。若想重写成功，映射必须存在并在其输出中设置 $Y 标志；如果映射不存在或未设置 $Y 则重写将失败。如果重写成功，则映射的结果将合并到当前位置的模板中并重新扩展。

此机制允许 MTA 重写进程以各种复杂的方式进行扩展。例如，可以选择性地分析和修改地址的用户名部分，通常这并不是 MTA 重写进程具有的功能。

用户提供的例程替换， $[...]

$[*image*、 *routine*、 *argument*] 形式的替换用于查找并调用用户提供的例程。在 UNIX 上运行时， MTA 使用 dlopen 和 dlsym 动态地装入并调用从共享库映像指定的例程。则该例程被称为函数，带有以下变量列表：

```
status := routine (argument, arglength, result, reslength)
```

argument 和 *result* 是 252 字节长的字符串缓冲区。在 UNIX 上， *argument* 和 *result* 作为指针被传送到字符串 （例如，在 C 中作为 char*）。 *arglength* 和 *reslength* 是由引用传送的带符号的长整数。输入时， *argument* 包含重写规则模板中的变量字符串， *arglength* 是该字符串的长度。返回时，结果字符串应放在 *result* 中，其长度应放在 *reslength* 中。然后该结果字符串将替换重写规则模板中的“$[*image,routine,argument*]”。如果重写规则失败则例程将返回 0，如果重写规则成功则例程将返回 -1。

此机制允许重写进程以各种复杂的方式进行扩展。例如，可以执行对某种类型的名称服务的调用并使用调用的结果来按某种方式改变地址。对主机 siroe.com 的正向指示地址 （例如 To: 地址）的目录服务查找可能是如下所示使用以下重写规则执行的。在第 276 页的 “特定于方向和位置的重写规则 ($B, $E, $F, $R)”中介绍的 $F 导致此规则仅用于正向指示地址：

```
siroe.com $F$[LOOKUP_IMAGE,LOOKUP,$U]
```

正向指示地址 jdoe@siroe.com 与该重写规则匹配时会导致 LOOKUP_IMAGE （UNIX 上的共享库）被装入内存，然后导致例程 LOOKUP 被调用，同时 jdoe 作为变量参数。然后例程 LOOKUP 可能会在结果参数中返回一个不同的地址 （如 John.Doe%eng.siroe.com）和值 -1 来表示重写规则成功。结果字符串中的百分比符号（请参见第 261 页的 “重复的重写模板 A%B”）将导致重写进程再次启动并使用 John.Doe@eng.siroe.com 作为要重写的地址。

在 UNIX 系统上，站点提供的共享库映像应该是全局可读的。

单个字段替换， $&、 $!、 $*、 $#

单个字段替换从正被重写的主机 / 域说明中提取单个子域部分。表 11-6 中显示了可用的单个字段替换。

表 11-6 单个字段替换

控制序列	用法
$&n	替换主机说明（不匹配或与某种通配符匹配的部分）中的第 n 个元素，n = 0、1、2、…、9。元素由点分隔；左侧的第一个元素为元素零。如果请求的元素不存在则重写失败。
$!n	替换主机说明（不匹配或与某种通配符匹配的部分）中的第 n 个元素，n = 0、1、2、…、9。元素由点分隔；右侧的第一个元素为元素零。如果请求的元素不存在则重写失败。
$*n	替换域说明（与模式中的显式文本匹配的部分）中的第 n 个元素， n = 0、1、2、…、9。元素由点分隔；左侧的第一个元素为元素零。如果请求的元素不存在则重写失败。
$#n	替换域说明（与模式中的显式文本匹配的部分）中的第 n 个元素， n = 0、1、2、…、9。元素由点分隔；右侧的第一个元素为元素零。如果请求的元素不存在则重写失败。

假设地址 `jdoe@eng.siroe.com` 与以下重写规则匹配：

```
*.SIROE.COM      $U%$&0.siroe.com@mailhub.siroe.com
```

则从模板得到的结果将会是 `jdoe@eng.siroe.com`，并将 `mailhub.siroe.com` 用作路由系统。

唯一字符串替换

$W 控制序列每次使用时都会插入一个由大写字母和数字组成的文本字符串，这些大写字母和数字都是唯一并且不可重复的。在必须构造非重复的地址信息时， $W 很有用。

特定于源通道的重写规则 （$M、 $N）

重写规则可以只与特定的源通道一起使用。这在简短形式的名称具有两种含义时很有用：

1. 当其在到达某个通道的邮件中显示时。
2. 当其在到达另一个通道的邮件中显示时。

特定于源通道的重写与使用中的通道程序以及通道关键字 rules 和 norules 相关联。如果在与正进行重写的 MTA 组件相关联的通道上指定了 norules，则将不会进行特定于通道的重写检查。如果在通道上指定了 rules，则会强制进行特定于通道的规则检查。关键字 rules 是默认设置。

特定于源通道的重写和与给定地址匹配的通道不相关联。该重写仅取决于进行重写的 MTA 组件以及该组件的通道表条目。

特定于通道的重写检查由规则的模板部分中的 $N 或 $M 控制序列触发。 $N 或 $M 后边的字符，一直到 at 符号 (@)、百分比符号 (%) 或后面的 $N、$M、$Q、$C、$T 或 $? 都被解释为通道名称。

例如，如果 *channel* 当前没有进行重写，则 $M*channel* 将导致规则失败。如果 *channel* 正进行重写，则 $N*channel* 将导致规则失败。可以指定多个 $M 和 $N 子句。如果多个 $M 子句中的任何一个子句匹配，则规则成功。如果多个 $N 子句中的任何一个子句匹配，则规则将失败。

特定于目标通道的重写规则 ($C, $Q)

可以具有这样的重写规则，其应用程序取决于邮件要排入的通道。当某个主机有两个名称，一个由一组主机所知晓，一个由另一组主机所知晓时，该重写规则很有用。通过使用不同的通道将邮件发送给每个组，可以对地址进行重写以指代每个组所知晓的名称的主机。

特定于目标通道的重写与邮件将在其中被排出队列并进行处理的通道以及该通道的通道关键字 rules 和 norules 相关联。如果在目标通道上指定了 norules，则不会进行特定于通道的重写检查。如果在目标通道上指定了 rules，则会强制进行特定于通道的规则检查。关键字 rules 是默认设置。

特定于目标通道的重写和与给定地址匹配的通道不相关联。该重写仅取决于邮件的信封 To: 地址。排入邮件时，其信封 To: 地址将首先被重写以确定该邮件要排入的通道。在重写 envelope To: 地址时，将忽略所有 $C 和 $Q 控制序列。重写了 envelope To: 地址以及确定了目标通道之后，将使用 $C 和 $Q 控制序列，因为与该邮件相关联的其他地址已被重写。

特定于目标通道的重写检查由规则的模板部分中的 $C 或 $Q 控制序列触发。$C 或 $Q 后边的字符，一直到 at 符号 (@)、百分比符号 (%) 或后面的 $N、$M、$C、$Q、$T 或 $? 都被解释为通道名称。

例如，如果 *channel* 不是目标通道，则 $Q*channel* 会导致规则失败。再如，如果 *channel* 是目标通道，则 $C*channel* 会导致规则失败。可以指定多个 $Q 和 $C 子句。如果多个 $Q 子句中的任何一个子句匹配，则规则成功。如果多个 $C 子句中的任何一个子句匹配，则规则失败。

特定于方向和位置的重写规则 ($B, $E, $F, $R)

有时需要指定仅应用于信封地址或仅应用于标题地址的重写规则。如果被重写的地址不是信封地址，控制序列 $E 将强制使重写失败。如果被重写的地址不是来自邮件标题或主体的地址，控制序列 $B 将强制使重写失败。这些序列对重写没有其他作用并且可能会显示在重写规则模板中的任何位置。

地址也可以按方向分类。正向指示地址源自 To:、 Cc:、 Resent-to: 或其他标题，或源自引用了目标的信封行。逆向指示地址如 From:、 Sender: 或 Resent-From:，指的是源。如果地址是正向指示的，则控制序列 $F 将导致应用重写。如果地址是反向指示的，则控制序列 $R 将导致应用重写。

特定于主机位置的重写 （$A、 $P、 $S、 $X）

有时需要对地址中主机名显示的位置敏感的重写。主机名可以显示在地址中几个不同的上下文中：

- 在源路由中
- 在 at 符号 (@) 的右侧
- 在本地部分中的百分比符号 (%) 的右侧
- 在本地部分中的感叹号的左侧

正常情况下，应该以相同的方式处理主机名，而不考虑其显示的位置。有些情况可能需要特殊处理。

四个控制序列用于控制基于地址中主机的位置的匹配。

- $S 指定规则可以与从源路由提取的主机匹配。
- $A 指定规则可以与 @ 符号右侧的主机匹配。
- $P 指定规则可以与 % 符号右侧的主机匹配。

- $X 指定规则可以与感叹号 (!) 左侧的主机匹配。

如果主机的位置不是指定的位置，则规则将失败。这些序列可以组合成一个重写规则。例如，如果指定了 $S 和 $A，规则将与源路由中或 at 符号右侧指定的主机匹配。不指定这些序列相当于指定了所有序列；规则可以匹配而不考虑位置。

更改当前标记值， $T

$T 控制序列用于更改当前重写规则标记。在配置文件和域数据库中查找重写规则模式之前，所有重写规则模式都前置了重写规则标记。 $T 后边的文本，一直到 at 符号、百分比符号、 $N、 $M、 $Q、 $C、 $T 或 $? 都是新标记。

在处理特殊寻址形式 （遇到某个组件时更改了地址的整个特征）时，标记很有用。例如，假设在源路由中找到特殊主机名 internet 时，应将其从地址中删除，产生的地址被迫与 TCP-DAEMON 通道匹配。

这可以通过类似以下的规则 （假设本地主机的正式名称为 localhost）来实现：

```
internet                $S$U@localhost$Tmtcp-force|

mtcp-force|.$U%$H@TCP-DAEMON
```

如果第一个规则在源路由中显示，则其将与特殊的主机名 internet 匹配。该规则强制 internet 与本地通道匹配，这将确保将 internet 从地址中删除。然后设置重写标记。重写将继续，但由于该标记的原因将不会有常规规则匹配。最后，将通过标记尝试使用默认规则，并且该组的第二个规则将激活，强制地址与 TCP-DAEMON 通道匹配而不考虑任何其他条件。

控制与重写 ($?) 相关联的错误消息

重写及通道匹配失败时， MTA 将提供默认错误消息。在某些情况下，更改这些邮件的能力将很有用。例如，如果某人尝试将邮件发送到以太网路由器箱，则显示类似“我们的路由器无法接受邮件”的信息可能要比通常的 “指定了非法的主机 / 域”更加明确。

如果规则失败，可以使用特殊控制序列来更改显示的错误消息。序列 $? 用于指定错误消息。如果此重写的结果无法与任何通道匹配，则 $? 后面的文本，一直到 at 符号 (@)、百分比符号 (%)、$N、$M、$Q、$C、$T 或 $? 都将是要显示的错误消息的文本。错误消息的设置比较 “麻烦”并将贯穿重写进程。

包含 $? 的规则的操作类似于任何其他规则。规则中只包含一个 $? （而没有任何其他符号）的特殊情况应该引起特别注意 --- 重写进程被终止 （而不更改地址的邮箱或主机部分），并按原样在通道表中查找主机。此查找将要失败，结果将返回错误消息。

例如，假设 MTA 配置文件中的最后一个重写规则如下所示：

```
. $?Unrecognized address; contact postmaster@siroe.com
```

在此示例中，可能失败的所有不可识别的主机或域说明在失败的过程中都会生成错误消息：不可识别的地址；请与 postmaster@siroe.com 联系。

处理大量的重写规则

MTA 总是从 imta.cnf 文件中读取所有的重写规则并将它们存储在内存的散列表中。使用编译的配置可以在每次需要信息时避开与读取配置文件相关联的系统开销；散列表仍用于存储内存中的所有重写规则。此方案适合于少量到中等数量的重写规则。但是，某些站点可能需要 10,000 个或更多的重写规则，这可能会消耗过分高的内存。

MTA 通过提供一个用于在辅助索引数据文件中存储大量重写规则的可选功能来解决此问题。无论何时读取常规配置文件，MTA 都将检查域数据库的存在情况。如果此数据库存在，则当尝试与配置文件中找到的规则匹配失败时，将打开该数据库并进行咨询。只有在配置文件中未找到给定的规则时才检查域数据库，因此始终可以将规则添加到配置文件中以覆盖数据库中的规则。默认情况下，域数据库用于存储与托管域相关联的重写规则。 IMTA_DOMAIN_DATABASE 属性存储在 imta_tailor 文件中。数据库的默认位置为 *msg_svr_base*/data/db/domaindb.db。

注 请勿手动编辑此文件。

测试重写规则

可以用 imsimta test -rewrite 命令测试重写规则。 -noimage 限定符将允许您在重新编译新配置前测试对配置文件所作的更改。

您会发现通过 -debug 限定符使用此实用程序来重写几个地址是很有帮助的。此实用程序将向您显示如何逐步地重写地址。例如，发出以下命令：

```
% imsimta test -rewrite -debug joe@siroe.com
```

有关 imsimta test -rewrite 实用程序的详细说明，请参见 Messaging Server Reference Manual。

重写规则示例

以下示例提供了重写规则样例以及规则如何重写样例地址。

假设系统 SC.CS.SIROE.EDU 的配置文件中包含如下示例中所示的重写规则：

```
sc                      $U@sc.cs.siroe.edu
sc1                     $U@sc1.cs.siroe.edu
sc2                     $U@sc2.cs.siroe.edu
*                       $U%$&0.cs.siroe.edu
*.cs                    $U%$&0.cs.siroe.edu
*.cs.siroe              $U%$&0.cs.siroe.edu
*.cs.siroe.edu          $U%$&0.cs.siroe.edu@ds.adm.siroe.edu
sc.cs.siroe.edu         $U@$D
sc1.cs.siroe.edu        $U@$D
sc2.cs.siroe.edu        $U@$D
sd.cs.siroe.edu         $U@sd.cs.siroe.edu
.siroe.edu              $U%$H.siroe.edu@cds.adm.siroe.edu
.edu                    $U@$H$D@gate.adm.siroe.edu
[]                      $U@[$L]@gate.adm.siroe.edu
```

表 11-7 显示了一些地址样例以及如何根据重写规则重写并路由这些地址。

表 11-7 地址范例和重写

初始地址	重写为	路由到
user@sc	user@sc.cs.siroe.edu	sc.cs.siroe.edu
user@sc1	user@sc1.cs.siroe.edu	sc1.cs.siroe.edu
user@sc2	user@sc2.cs.siroe.edu	sc2.cs.siroe.edu
user@sc.cs	user@sc.cs.siroe.edu	sc.cs.siroe.edu
user@sc1.cs	user@sc1.cs.siroe.edu	sc1.cs.siroe.edu
user@sc2.cs	user@sc2.cs.siroe.edu	sc2.cs.siroe.edu
user@sc.cs.siroe	user@sc.cs.siroe.edu	sc.cs.siroe.edu
user@sc1.cs.siroe	user@sc1.cs.siroe.edu	sc1.cs.siroe.edu
user@sc2.cs.siroe	user@sc2.cs.siroe.edu	sc2.cs.siroe.edu
user@sc.cs.siroe.edu	user@sc.cs.siroe.edu	sc.cs.siroe.edu
user@sc1.cs.siroe.edu	user@sc1.cs.siroe.edu	sc1.cs.siroe.edu
user@sc2.cs.siroe.edu	user@sc2.cs.siroe.edu	sc2.cs.siroe.edu
user@sd.cs.siroe.edu	user@sd.cs.siroe.edu	sd.cs.siroe.edu

表 11-7 地址范例和重写

初始地址	重写为	路由到
user@aa.cs.siroe.edu	user@aa.cs.siroe.edu	ds.adm.siroe.edu
user@a.eng.siroe.edu	user@a.eng.siroe.edu	cds.adm.siroe.edu
user@a.cs.sesta.edu	user@a.cs.sesta.edu	gate.adm.siroe.edu — 插入的路由
user@b.cs.sesta.edu	user@b.cs.sesta.edu	gate.adm.siroe.edu — 插入的路由
user@[1.2.3.4]	user@[1.2.3.4]	gate.adm.siroe.edu — 插入的路由

基本上，这些重写规则的意思是：如果主机名是我们的简短形式的名称之一 （sc、sc1 或 sc2）或我们的全名 （sc.cs.siroe.edu 等）之一，则将其扩展为我们的全名并路由给我们。将 cs.cmu.edu 附加到一部分简短形式的名称并重试。将 .cs 后边的一部分转换成 .cs.siroe.edu 后边的一部分并重试。同时将 .cs.siroe 转换成 .cs.siroe.edu 并重试。

如果名称为 sd.cs.siroe.edu （可能是我们直接连接的某个系统），则进行重写并将其路由到那里。如果主机名为 .cs.siroe.edu 子域中的任何其他名称，则将其路由到 ds.cs.siroe.edu （.cs.siroe.edu 子域的网关）。如果主机名为 .siroe.edu 子域中的任何其他名称，则将其路由到 cds.adm.siroe.edu （.siroe.edu 子域的网关）。如果主机名为 .edu 顶层域中的任何其他名称，则将其路由到 gate.adm.siroe.edu （假定其可以将邮件路由到正确的目标）。如果使用了域文字，则也将其发送到 gate.adm.siroe.edu。

重写规则的大多数应用程序 （如先前的示例）将不会以任何方式更改地址的用户名（或邮箱）部分。当 MTA 用于与不符合 RFC 822 的邮件程序 （需要将主机 / 域说明部分加入到地址的用户名部分的邮件程序）配合共作时，将使用更改地址用户名部分的功能。确实要使用此功能时应格外谨慎。

第 12 章

配置通道定义

本章说明了如何在 MTA 配置文件 `imta.cnf` 中使用通道关键字定义。阅读本章之前，请先阅读第 10 章 “关于 MTA 服务和配置”、第 177 页的 “通道定义”和第 206 页的 “MTA 配置文件”。本章包含以下各节：

- 按字母顺序列出的通道关键字
- 按功能分类的通道关键字
- 配置通道默认值
- 配置 SMTP 通道
- 配置邮件处理和传送
- 配置地址处理
- 配置标题处理
- 附件和 MIME 处理
- 对邮件、配额、收件人和验证尝试次数的限制
- MTA 队列中的文件创建
- 指定邮箱过滤器文件位置
- 配置记录和调试
- 其他关键字

注 如果在 imta.cnf 中更改了通道定义，则当装入了配置数据的任何程序或通道 （例如， SMTP 服务器）启动时，必须使用 imsimta restart 命令对其进行重新启动 （仅一次）。如果使用的是编译的配置，则必须重新编译然后再重新启动。有关编译配置信息和启动程序的更多信息，请参见 Messaging Server Reference Manual。

按字母顺序列出的通道关键字

下表是按字母顺序排列的关键字列表。

表 12-1 按字母顺序排列的通道关键字

关键字	页	关键字	页	关键字	页	关键字	页
733	327	822	327	addreturnpath	333	addrsperfile	348
Aliasdetourhost	355	aliaslocal	336	aliaspostmaster	248	allowetrn	303
allowswitchchannel	313	alternatechannel	347	alternateblocklimit	347	alternatelinelimit	347
alternaterecipientlimit	347	authrewrite	316	backoff	321	bangoverpercent	329
bangstyle	327	bidirectional	320	blocketrn	303	blocklimit	346
cacheeverything	310	cachefailures	310	cachesuccesses	310	channelfilter	354
charset7	306	charset8	306	charsetesc	306	checkehlo	303
commentinc	334	commentmap	334	commentomit	334	commentstrip	334
commenttotal	334	connectalias	330	connectcanonical	330	copysendpost	247
copywarnpost	248	daemon	314	datefour	340	datetwo	340
dayofweek	340	defaulthost	331	defaultmx	312	defaultnameservers	313
deferralrejectlimit	359	deferred	320	defragment	343	dequeue_removeroute	337
destinationfilter	354	destinationnosolicit	358	destinationspamfilterXoptin	355	disableetrn	303
dispositionchannel	353	disconnectbadauthlimit	346	disconnectbadcommandlimit	351	domainetrn	303
domainvrfy	304	dropblank	332	ehlo	303	eightbit	306
eightnegotiate	306	eightstrict	306	errsendpost	247	errwarnpost	248

表 12-1 按字母顺序排列的通道关键字

关键字	页	关键字	页	关键字	页	关键字	页
expandchannel	326	expandlimit	326	expnallow	305	expndisable	305
expndefault	305	exproute	329	fileinto	354	filesperjob	322
filter	354	forwardcheckdelete	311	forwardchecknone	311	forwardchecktag	311
header_733	327	header_822	327	header_uucp	327	headerlabelalign	341
headerlimit	350	headerlinelength	341	headerread	339	headertrim	339
holdexquota	348	holdlimit	326	identnone	311	identnonelimited	311
identnonenumeric	311	identnonesymbolic	311	identtcp	311	identtcplimited	311
identtcpsymbolic	311	ignoreencoding	343	immnonurgent	320	improute	329
includefinal	247	indenttcpnumeric	311	inner	338	innertrim	339
interfaceaddress	310	interpretencoding	343	language	342	lastresort	313
linelength	345	linelimit	346	localvrfy	304	logging	352
logheader	352	loopcheck	353	mailfromdnsverify	305	master	320
master_debug	352	maxblocks	344	maxheaderaddrs	341	maxheaderchars	341
maxjobs	322	maxlines	344	maxprocchars	341	maysaslserver	315
maytls	317	maytlsclient	317	maytlsserver	317	missingrecipientpolicy	331
msexchange	317	multiple	348	mustsaslserver	315	musttls	317
musttlsclient	317	musttlsserver	317	mx	312	namelengthlimit	349
nameservers	313	noaddreturnpath	333	nobangoverpercent	329	noblocklimit	346
nocache	310	nochannelfilter	354	nodayofweek	340	nodefaulthost	331
nodeferred	320	nodefragment	343	nodestinationfilter	354	nodropblank	332
noehlo	303	noexproute	329	noexquota	348	nofileinto	354
nofilter	354	noheaderread	339	noheadertrim	339	noimproute	329
noinner	338	noinnertrim	339	nolinelimit	346	nologging	352
noloopcheck	353	nomailfromdnsverify	305	nomaster_debug	352	nomsexchange	316
nomx	312	nonrandomemx	312	nonurgentbackoff	321	nonurgentblocklimit	324
nonurgentnotices	246	noreceivedfor	334	noreceivedfrom	334	noremotehost	331
norestricted	333	noreturnaddress	248	noreturnpersonal	248	noreverse	332
normalbackoff	321	normalblocklimit	324	normalnotices	246	norules	337
nosasl	315	nosaslserver	315	nosaslswitchchannel	315	nosendetrn	303

表 12-1 按字母顺序排列的通道关键字

关键字	页	关键字	页	关键字	页	关键字	页
nosendpost	247	noservice	326	noslave_debug	352	nosmtp	302
nosourcefilter	354	noswitchchannel	313	notices	246	notificationchannel	353
notls	317	notlsclient	317	notlsserver	317	novrfy	304
nowarnpost	248	nox_env_to	340	parameterlengthlimit	349	percentonly	329
percents	327	personalinc	335	personalmap	335	personalomit	335
personalstrip	335	pool	322	port	310	postheadbody	248
postheadonly	248	randommx	312	receivedfor	334	receivedfrom	334
recipientcutoff	349	recipientlimit	349	rejectsmtplonglines	349	remotehost	331
restricted	333	returnaddress	248	returnenvelope	248	returnpersonal	248
reverse	332	routelocal	330	rules	337	rules	337
saslswitchchannel	315	sendetrn	303	sendpost	247	sensitivitycompanyconfidential	342
sensitivitynormal	342	sensitivitypersonal	342	sensitivityprivate	342	service	326
sevenbit	306	silentetrn	303	single	348	single_sys	314
slave	320	slave_debug	352	smtp	302	smtp_cr	302
smtp_crlf	302	smtp_crorlf	302	smtp_lf	302	sourceblocklimit	346
sourcecommentinc	334	sourcecommentmap	334	sourcecommentomit	334	sourcecommentstrip	334
sourcecommenttotal	334	sourcefilter	354	sourcenosolicit	358	sourcepersonalinc	335
sourcepersonalmap	335	sourcepersonalomit	335	sourcepersonalstrip	335	sourceroute	327
sourcespamfilterXoptin	355	streaming	307	subaddressexact	336	subaddressrelaxed	336
subaddresswild	336	subdirs	351	submit	354	suppressfinal	247
switchchannel	313	threaddepth	325	tlsswitchchannel	317	transactionlimit	324
truncatesmtplonglines	349	unrestricted	333	urgentbackoff	321	urgentblocklimit	324
urgentnotices	246	useintermediate	247	user	354	uucp	327
viaaliasoptional	337	viaaliasrequired	337	vrfyallow	304	vrfydefault	304
vrfyhide	304	warnpost	248	wrapsmtplonglines	349	x_env_to	340

按功能分类的通道关键字

下表是分类后的关键字列表。类别如下所示：

- 第 285 页的 “地址处理”
- 第 287 页的 “附件和 MIME 处理”
- 第 287 页的 “字符集和八位数据”
- 第 287 页的 “MTA 队列区域中的文件创建”
- 第 287 页的 “标题”
- 第 290 页的 “外来通道匹配和切换”
- 第 290 页的 “记录和调试”
- 第 290 页的 “长地址列表或标题”
- 第 290 页的 “邮箱过滤器”
- 第 291 页的 “NO-SOLICIT SMTP 扩展支持”
- 第 291 页的 “通知和邮寄主管邮件”
- 第 292 页的 “处理控制和作业提交”
- 第 293 页的 “敏感度限制”
- 第 293 页的 “对邮件的限制、用户配额、权限和验证尝试”
- 第 294 页的 “SMTP 验证、 SASL 和 TLS”
- 第 295 页的 “SMTP 命令和协议”
- 第 296 页的 “TCP/IP 连接和 DNS 查找支持”
- 第 297 页的 “其他”

表 12-2 按功能分类的通道关键字

关键字	页	定义
地址处理		
733	327	在信封中使用 % 路由；与 `percents` 同义。
822	327	在信封中使用源路由；与 `sourceroute` 相同。
addreturnpath	333	向加入此通道队列的邮件添加 `Return-path:` 标题。
aliaslocal	336	在别名文件和别名数据库中查找重写的地址。

表 12-2 按功能分类的通道关键字

关键字	页	定义
authrewrite	316	用于源通道中，它使 MTA 将已验证的创始者信息 （如果可用）传播到标题中。
bangoverpercent	329	将 A!B%C 归入组 A!(B%C)
bangstyle	327	在信封中使用 UUCP ! 路由；与 uucp 同义。
defaulthost	331	指定用于完成地址的域名
dequeue_removeroute	337	从信封 To: 地址中删除源。
exproute	329	将地址传递到远程系统时，要求显式路由。
holdlimit	326	当信封收件人地址的数量超过此限制时，将保留邮件。
improute	329	此通道地址的隐式路由
missingrecipientpolicy	331	为缺少收件人标题的邮件设置如何使其合法化 （添加何种标题）的策略。
noaddreturnpath	333	邮件进行排队时不添加 Return-path: 标题。
nobangoverpercent	329	将 A!B%C 归入组 (A!B)%C
nodefaulthost	331	不指定用于完成地址的域名
noexproute	329	无用于此通道地址的显式路由
noimproute	329	无用于此通道地址的隐式路由
noreceivedfrom	334	构建 Received: 标题行，但不包含原来的信封 From: 地址。
noremotehost	331	使用本地主机的域名作为完成地址的默认域名
norestricted	333	与 unsrestricted 相同。
noreverse	332	使邮件地址免受地址反向处理
norules	337	不对此通道强制执行特定于通道的重写规则检查。
percentonly	329	忽略 bang 路径。在信封中使用 % 路由。
percents	327	在信封中使用 % 路由；与 733 同义。
remotehost	331	使用远程主机的名称作为完成地址的默认域名
restricted	333	通道连接到需要编码的邮件系统。
reverse	332	已根据地址反向数据库或 REVERSE 映射检查地址
routelocal	330	向通道重写地址时，使 MTA 尝试让地址中所有显式路由 “短路”。
rules	337	对此通道强制执行针对通道的重写规则检查。
sourceroute	327	与 822 同义。
subaddressexact	336	在条目匹配期间不执行特殊的子地址处理；整个邮箱 （包含子地址）都与条目匹配时才认为该别名匹配。
subaddressrelaxed	336	对完全匹配以及名称 +* 格式的匹配进行查找后， MTA 应另外检查仅名称部分相同的匹配。

表 12-2 按功能分类的通道关键字

关键字	页	定义
subaddresswild	336	对完全匹配 （包含整个子地址）进行查找后，接下来 MTA 应查找名称 +* 格式的条目。
unrestricted	333	通知 MTA 不执行 RFC 1137 编码和解码。
uucp	327	在信封中使用 UUCP! 路由；与 bangstyle 同义。
viaaliasoptional	337	不要求别名生成与通道相匹配的最终收件人地址。
viaaliasrequired	337	与通道匹配的最终收件人地址必须由别名生成。
附件和 MIME 处理		
defragment	343	将在通道排队的部分邮件放置到片段整理通道队列中。
ignoreencoding	343	忽略外来邮件中的 Encoding: 标题。
interpretencoding	343	对外来邮件中的 Encoding: 标题进行解释 （如果需要）。
nodefragment	343	禁用片段整理。
字符集和八位数据		
charset7	306	与 7 位文本邮件关联的默认字符集
charset8	306	与 8 位文本邮件关联的默认字符集
charsetesc	306	与包含换码符的 7 位文本关联的默认字符集
eightbit	306	通道支持八位字符。
eightnegotiate	306	如果可能，通道应对使用八位传输进行协商。
eightstrict	306	拒绝包含未经协商的八位数据标题的邮件。
sevenbit	306	不支持 8 位字符；必须对 8 位字符进行编码。
MTA 队列区域中的文件创建		
addrsperfile	348	可与通道队列中单个邮件文件相关联的收件人最大数量的限制
expandchannel	326	指定由于应用 expandlimit 而在其中执行延迟扩展的通道。
expandlimit	326	地址数目超过此限制时，“脱机”处理外来邮件。
multiple	348	对邮件文件中收件人的数量未作限制，但将 SMTP 通道默认为 99。
single	348	为通道中每个目标地址分别创建一个邮件副本。
single_sys	348	为所用的每个目标系统创建一个邮件副本。
subdirs	351	指定将在其中分布通道队列的邮件的子目录的数量。
标题		
authrewrite	316	用于源通道中，它使 MTA 将已验证的创始者信息 （如果可用）传播到标题中。
commentinc	334	完好保留邮件标题行中的注释。
commentmap	334	通过 COMMENT_STRINGS 映射表运行邮件标题行中的注释字符串。

表 12-2 按功能分类的通道关键字

关键字	页	定义
commentomit	334	从邮件标题行中删除注释。
commentstrip	334	从邮件标题行的注释字段中删除有问题的字符。
commenttotal	334	删除除 Received: 标题行以外的所有标题行中的注释 （括号中的内容）标题行。不建议使用。
datefour	340	将所有年份字段扩展为四位数。
datetwo	340	删除四位数日期中的前两位数。提供与要求两位数日期的邮件系统的兼容性；不得用于其他用途。
dayofweek	340	保留星期几信息，并将其添加到缺少此信息的日期和时间标题中。
defaulthost	331	指定用于完成地址的域名
dropblank	332	删除外来邮件中的非法空标题。
header_733	327	在邮件标题中使用 % 路由。
header_822	327	在邮件标题中使用源路由。
headerlabelalign	341	控制加入此通道队列的邮件标题的对齐点；它使用整数参数。
headerlinelength	341	控制加入此通道队列的标题行的长度。
headerread	339	在处理原来的邮件标题之前，邮件加入队列后对邮件标题应用选项文件中的标题剪裁规则 （请小心使用）。
headertrim	339	在处理原来的邮件标题之后，对邮件标题应用选项文件中的标题剪裁规则。
header_uucp	327	在标题中使用 ! 路由
inner	338	分析邮件并重写内部标题。
innertrim	339	对内部邮件标题应用选项文件中的标题剪裁规则 （请小心使用）。
language	342	指定标题的默认语言。
maxheaderaddrs	341	控制一行中可以显示的地址数量。
maxheaderchars	341	控制一行中可以显示的字符数量。
missingrecipientpolicy	331	为缺少收件人标题的邮件设置如何使其合法化 （添加何种标题）的策略。
nodayofweek	340	从日期和时间标题中删除星期几。提供与不能处理此信息的邮件系统的兼容性；不得用于其他用途。
nodefaulthost	331	不指定用于完成地址的域名
nodropblank	332	不删除外来邮件中的非法空标题。
noheaderread	339	不应用选项文件中的标题剪裁规则。
noheadertrim	339	不应用选项文件中的标题剪裁规则。
noinner	338	不重写内部邮件标题行。

表 12-2 按功能分类的通道关键字

关键字	页	定义
noinnertrim	339	不对内部邮件标题应用标题剪裁。
noreceivedfor	334	构建 Received: 标题行，而不包含任何信封收件人信息。
noreceivedfrom	334	构建 Received: 标题行，但不包含原来的信封 From: 地址。
noremotehost	331	使用本地主机的域名作为完成地址的默认域名
noreverse	332	使在此通道排队的邮件地址免受地址反向处理
norules	337	不对此通道强制执行特定于通道的重写规则检查。
nox_env_to	340	删除 X-Envelope-to 标题行。
personalinc	335	完好保留邮件标题行中的个人名称字段。
personalmap	335	通过 PERSONAL_NAMES 映射表运行个人名称。
personalomit	335	从邮件标题行中删除个人名称字段。
personalstrip	335	从标题行的个人名称字段中删除有问题的字符。
receivedfor	334	如果邮件只发送给一个信封收件人，将该信封 To: 地址包含在它构建的 Received: 标题行中。
receivedfrom	334	如果 MTA 更改了信封 From: 地址，则在构建外来邮件的 Received: 标题行时，将包含原始信封 From: 地址。
remotehost	331	使用远程主机的名称作为完成地址的默认域名
restricted	333	通道连接到需要此编码的邮件系统。
reverse	332	根据地址反向数据库或 REVERSE 映射检查地址
rules	337	对此通道强制执行针对通道的重写规则检查。
sensitivitycompanyconfidential	342	Companyconfidential 是所接受的邮件的敏感度上限。
sensitivitynormal	342	Normal 是所接受的邮件的敏感度上限。
sensitivitypersonal	342	Personal 是所接受的邮件的敏感度上限。
sensitivityprivate	342	Private 是所接受的邮件的敏感度上限。
sourcecommentinc	334	保留外来邮件标题行中的注释。
sourcecommentmap	334	通过源通道运行标题行中的注释字符串。
sourcecommentomit	334	删除来从外来邮件标题行 （例如， To:、 From: 和 Cc: 标题）的所有注释。
sourcecommentstrip	334	从外来标题行的注释字段中删除有问题的字符。
sourcecommenttotal	334	删除外来邮件中的注释 （扩号中的内容）。
sourcepersonalinc	335	完好保留外来邮件标题行中的个人名称。
sourcepersonalmap	335	通过源通道中运行个人名称。

表 12-2 按功能分类的通道关键字

关键字	页	定义
sourcepersonalomit	335	从外来邮件标题行中删除个人名称字段。
sourcepersonalstrip	335	从外来邮件标题行的个人名称字段中删除有问题的字符。
unrestricted	333	通知 MTA 不执行 RFC 1137 编码和解码。
x_env_to	340	启用生成 X-Envelope-to 标题行。
外来通道匹配和切换		
allowswitchchannel	313	允许从 switchchannel 通道切换到此通道
nosaslswitchchannel	315	SASL 验证成功完成后，不切换到此通道
noswitchchannel	313	不应该切换到此通道或从此通道切换到其他通道。
switchchannel	313	从服务器通道切换到与发件主机关联的通道。
saslswitchchannel	315	使外来连接在客户机成功使用 SASL 后切换到指定的通道。
tlsswitchchannel	317	TLS 协商成功后，切换到其他通道。
记录和调试		
logging	352	将邮件入队和出队信息记录到日志文件中，并为特定通道激活记录。
loopcheck	353	在 SMTP EHLO 响应标题中放入字符串，以便 MTA 检查它是否在与自身通信。
master_debug	352	在通道的主程序输出中创建调试输出。
nologging	352	不将邮件入队和出队信息记录到日志文件中。
noloopcheck	353	不在 SMTP EHLO 响应标题中放入字符串。
nomaster_debug	352	通道的主程序输出中无调试输出。
noslave_debug	352	不生成从属调试输出。
slave_debug	352	生成从属调试输出。
长地址列表或标题		
expandchannel	326	指定由于应用 expandlimit 而在其中执行延迟扩展的通道。
expandlimit	326	地址数目超过此限制时，“脱机”处理外来邮件。
holdlimit	326	地址数量超过此限制时保留邮件。
maxprocchars	341	可以处理和重写的最大长度的标题。
邮箱过滤器		
channelfilter	354	通道过滤器文件的位置；与 destinationfilter 相同。
destinationfilter	354	应用到外发邮件的通道过滤器文件的位置。
destinationspamfilter Xoptin	355	通过垃圾邮件过滤软件 X 运行发送到此通道的邮件。

表 12-2 按功能分类的通道关键字

关键字	页	定义
fileinto	354	指定应用邮箱过滤器 fileinto 操作时对地址的影响。
filter	354	指定用户过滤器文件的位置。
nochannelfilter	354	不对外发邮件进行通道过滤。也称为 nodestinationfilter。
nodestinationfilter	354	不对外发邮件执行通道过滤。
nofileinto	354	邮箱过滤器 fileinto 操作无影响。
nofilter	354	不执行用户邮箱过滤。
nosourcefilter	354	不对外来邮件执行通道过滤。
sourcefilter	354	为外来邮件指定通道过滤器文件的位置。
sourcespamfilterXoption	355	通过垃圾邮件过滤软件 X 运行源自此通道的邮件。
NO-SOLICIT SMTP 扩展支持		
sourcenosolicit	358	指定一个以逗号分隔的列表，此列表包括将在此通道提交的邮件中被阻塞的请求字段值。
destinationnosolicit	358	指定一个以逗号分隔的列表，此列表包括不会被此通道中排队的邮件接受的请求字段值。
通知和邮寄主管邮件 （有关完整的通知过程，请参见第 240 页）		
aliaspostmaster	248	将发送给正式通道名称中用户名称邮寄主管的邮件重定向到 postmaster@local-host，其中 local-host 是本地主机名 （本地通道中的名称）。
copysendpost	247	将失败通知的副本发送给邮寄主管，除非失败邮件中的创始者地址为空。
copywarnpost	248	向邮寄主管发送警告消息的副本 （除非未传送邮件上的创始者地址为空）。
errsendpost	247	仅在无法将通知返回创始者时向邮寄主管发送错误通知的副本。
errwarnpost	248	在无法将通知返回创始者时向邮寄主管发送警告消息的副本。
includefinal	247	传送通知时包含收件人地址的最终格式。
nonurgentnotices	246	指定在发送通知和返回非紧急优先级邮件前可能经过的时间。
noreturnaddress	248	将 RETURN_ADDRESS 选项值用作邮寄主管地址名称。
noreturnpersonal	248	将 RETURN_PERSONAL 选项值用作邮寄主管个人名称。
normalnotices	246	指定在发送通知和返回普通优先级邮件前可能经过的时间。
nosendpost	247	禁用向邮寄主管发送所有失败邮件的副本。
notices	246	指定在发送通知和返回邮件之前可能经过的时间。
nowarnpost	248	禁用向邮寄主管发送警告消息的副本。
postheadbody	248	同时返回邮件的标题和内容。

表 12-2 按功能分类的通道关键字

关键字	页	定义
postheadonly	248	仅向邮寄主管返回标题。
returnaddress	248	指定本地邮寄主管的返回地址。
returnenvelope	248	控制空的信封返回地址的使用。
returnpersonal	248	设置本地邮寄主管的个人名称。
sendpost	247	启用向邮寄主管发送所有失败邮件的副本。
suppressfinal	247	抑制通知邮件中的最终地址格式 （如果通知邮件中存在原始地址格式）。
urgentnotices	246	指定在发送通知和返回紧急优先级邮件之前可能经过的时间。
useintermediate	247	使用在列表扩展之后，但在用户邮箱名称生成之前生成的地址的中间格式。
warnpost	248	启用向邮寄主管发送警告消息的副本。
处理控制和作业提交 **（有关更详细的功能说明，请参见表 12-7 第 318 页）**		
backoff	321	尝试重新传送未成功传送的邮件的频率。可以被关键字 normalbackoff、nonurgentbackoff、 urgentbackoff 覆盖。
bidirectional	320	主程序和从程序为其服务的通道。
deferred	320	识别和生效 Deferred-delivery:。
expandchannel	326	指定由于应用 expandlimit 而在其中执行延迟扩展的通道。
expandlimit	326	地址数目超过此限制时，“脱机”处理外来邮件。
filesperjob	322	将由单个作业处理的队列条目的数量。
immnonurgent	320	紧急、正常和不紧急邮件提交后，立即开始传送。
master	320	主程序 (master) 为其服务的通道。
maxjobs	322	可以同时为通道运行的作业的最大数量。
nodeferred	320	指定不使 Deferred-delivery: 标题行生效。
nonurgentbackoff	321	尝试重新传送非紧急邮件的频率。
nonurgentblocklimit	324	将超过此大小的邮件强制降到非紧急优先级 （二类优先级）以下，意味着邮件将始终等待下一个周期的作业以进一步处理。
normalbackoff	321	尝试重新传送普通邮件的频率。
normalblocklimit	324	将超过此大小的邮件强制降到非紧急优先级。
noservice	326	必须通过 CHARSET-CONVERSION 启用进入此通道的邮件的服务转换。
pool	322	为通道指定池。后面必须跟池名称，当前通道的传送作业将被置于该池名称中。
service	326	无条件启用服务转换，不考虑 CHARSET-CONVERSION 条目。
slave	320	由从程序 （从）提供服务的通道。

表 12-2 按功能分类的通道关键字

关键字	页	定义
threaddepth	325	使用多线程 SMTP 客户机触发新线程的邮件的数目。
transactionlimit		限制每个连接允许的邮件数目。
urgentbackoff	321	尝试重新传送紧急邮件的频率。
urgentblocklimit	324	将超过此大小的邮件强制降至普通优先级。
user	354	用于 pipe 通道中，指明通道将在其下运行的用户名称。
敏感度限制		
sensitivitycompanyconfidential	342	所接受的邮件的敏感度上限。
sensitivitynormal	342	`Normal` 是所接受的邮件的敏感度上限。
sensitivitypersonal	342	`Personal` 是所接受的邮件的敏感度上限。
sensitivityprivate	342	`Private` 是所接受的邮件的敏感度上限。
对邮件的限制、用户配额、权限和验证尝试		
alternatechannel	347	alternateblocklimit、 alternatelinelimit 及 alternaterecipientlimit 的备用目标通道。
alternateblocklimit	347	指定将邮件发送到 alternativechannel 之前邮件中的块数限制。
alternatelinelimit	347	指定将邮件发送到 alternativechannel 之前邮件中的行数限制。
alternaterecipientlimit	347	指定将邮件发送到 alternativechannel 之前邮件中收件人数量的限制。
blocklimit	346	每个邮件中允许的 MTA 块的最大数量。
disconnectbadauthlimit	346	断开会话连接之前，对允许在会话中进行的不成功验证尝试的次数的限制。
disconnectbadcommandlimit	351	限制错误命令的数量。
disconnectrecipientlimit	351	限制会话收件人的数量。
disconnectrejectlimit	351	限制被拒绝的收件人的数量。
disconnecttransactionlimit	351	限制事务的数量。
headerlimit	350	限制主 （最外层）邮件标题的最大大小
holdexquota	348	为超过配额的用户保留邮件。
holdlimit	326	地址数目超过此限制时，保留外来邮件。
linelength	345	基于各个通道限制允许的最大邮件行长度。
linelimit	346	每个邮件中允许的最大行数。
maxblocks	344	指定邮件中允许的最大块数。

表 12-2 按功能分类的通道关键字

关键字	页	定义
maxlines	344	指定邮件中允许的最大行数。
nameparameterlengthlimit	349	控制 name content-type 和 filename content-disposition 参数的截断点。
noblocklimit	346	不限制每个邮件中允许的 MTA 块的数量。
noexquota	348	将发给超过配额的用户的所有邮件返回创始者。
nolinelimit	346	不对每个邮件中允许的行数指定限制。
nonurgentblocklimit	324	将超过此大小的邮件强制降到非紧急优先级 （二类优先级）以下，意味着邮件将始终等待下一个周期的作业以进一步处理。
normalblocklimit	324	将超过此大小的邮件强制降到非紧急优先级。
parameterlengthlimit	349	控制通用内容类型和内容处理参数的截断点。
recipientcutoff.	349	如果收件人超过此值，则拒绝邮件。
recipientlimit	349	限制接受的邮件收件人地址的数量。
rejectsmtplonglines	349	拒绝包含超过 1000 个字符 （包括 CRLF）的行的邮件。
sourceblocklimit	346	每个外来邮件中允许的 MTA 块的最大数量。
truncatesmtplonglines	349	当行超过 1000 个字符时，将其截断。
wrapsmtplonglines	349	当行超过 1000 个字符时换行。
urgentblocklimit	324	将超过此大小的邮件强制降至普通优先级。
SMTP 验证、 SASL 和 TLS （有关更详细的功能说明，请参见 315）		
authrewrite	316	用于源通道中，它使 MTA 将已验证的创始者信息 （如果可用）传播到标题中。
maysaslserver	315	允许客户机尝试使用 SASL 验证。
maytls	317	使 MTA 向外来连接提供 TLS，并对外发连接尝试 TLS。
maytlsclient	317	发送外发邮件时，如果是发送到支持 TLS 的 SMTP 服务器， MTA SMTP 客户机将尝试使用 TLS。
maytlsserver	317	MTA SMTP 服务器将公布支持 STARTTLS 扩展，并允许在接收邮件时使用 TLS。
msexchange	317	用于 TCP/IP 通道，通知 MTA 此通道是与 Microsoft Exchange 网关及客户机通信的通道。
mustsaslserver	315	除非远程客户机验证成功，否则 SMTP 服务器不接收邮件。
musttls	317	坚持在外发和外来连接中使用 TLS。
musttlsclient	317	MTA SMTP 客户机将坚持在发送外发邮件时使用 TLS （MTA 将发出 STARTTLS 命令，并且该命令必须成功）。
musttlsserver	317	MTA SMTP 服务器将公布支持 STARTTLS 扩展，并坚持在接收外来邮件时使用 TLS。

表 12-2 按功能分类的通道关键字

关键字	页	定义
nomsexchange	316	默认设置。
nosasl	315	不允许或不尝试 SASL 验证。
nosaslserver	315	不允许 SASL 验证。
notls	317	不允许或不尝试 TLS。
notlsclient	317	MTA SMTP 客户机不对外发连接尝试使用 TLS （外发连接期间不发出 STARTTLS 命令）。
notlsserver	317	MTA SMTP 服务器不允许对外来连接使用 TLS （SMTP 服务器不公布 STARTTLS 扩展，也不接受命令本身）。
saslswitchchannel	315	使外来连接在客户机成功使用 SASL 后切换到指定的通道。
tlsswitchchannel	317	使外来连接在客户机的 TLS 协商成功后切换到指定的通道。它使用一个必需的值，以指定将切换到的通道。
SMTP 命令和协议 **（有关更详细的功能说明，请参见表 12-4 第 301 页）**		
allowetrn	303	执行 ETRN 命令。
blocketrn	303	阻止 ETRN 命令。
checkehlo	303	检查 SMTP 响应标题，以确定使用 EHLO 还是 HELO。
disableetrn	303	禁用对 ETRN SMTP 命令的支持。
domainetrn	303	仅执行指定域的那些 ETRN 命令。
domainvrfy	304	使用完整地址发出 VRFY 命令。
ehlo	303	在初始连接中使用 SMTP EHLO 命令。
eightbit	306	通道支持八位字符。
eightnegotiate	306	如果可能，通道应对使用八位传输进行协商。
eightstrict	306	拒绝包含未经协商的八位数据标题的邮件。
expnallow	305	允许 EXPN，即使已使用 DISABLE_EXPAND SMTP 通道选项在 SMTP 服务器级别禁用 EXPN。
expndisable	305	无条件禁用 EXPN。
expndefault	305	如果已将 SMTP 服务器设置为允许 EXPN，则允许 EXPN。
localvrfy	304	使用本地地址发出 VRFY 命令。
mailfromdnsverify	305	验证 MAIL FROM: 命令中使用的域存在于 DNS 中。
noehlo	303	不使用 EHLO 命令。
nomailfromdnsverify	305	不验证 MAIL FROM: 命令中使用的域存在于 DNS 中。
nosendetrn	303	不发送 ETRN 命令。

表 12-2 按功能分类的通道关键字

关键字	页	定义
nosmtp	302	不支持 SMTP 协议。该值为默认值。
novrfy	304	不发出 VRFY 命令。
sendetrn	303	发送 ETRN 命令。
sevenbit	306	不支持 8 位字符；必须对 8 位字符进行编码。
silentetrn	303	执行 ETRN 命令，不回显通道信息。
smtp	302	支持 SMTP 协议。关键字 `smtp` 对所有 SMTP 通道都具有强制性。（此关键字等效于 `smtp_crorlf`。）
smtp_cr	302	接受以回车 (CR) （不跟换行符 [LF]）终止的行。
smtp_crlf	302	必须以回车 (CR) 加换行符 (LF) 序列终止行。
smtp_crorlf	302	可以使用回车 (CR)、换行符 (LF) 序列或完整的 CRLF 终止行。
smtp_lf	302	接受以换行符 (LF) （前面没有 CR）终止的行。
streaming	**307**	控制与通道关联的协议中使用的协议流的程度。
vrfyallow	304	向 VRFY 命令提供信息响应。
vrfydefault	304	根据通道的 HIDE_VERIFY 选项设置，向 VRFY 命令提供默认响应。
vrfyhide	304	向 SMTP VRFY 命令提供模糊的响应。
TCP/IP 连接和 DNS 查找支持 **（有关更详细的功能说明，请参见表 12-5 第 308 页）**		
cacheeverything	310	缓存所有连接信息。
cachefailures	310	仅缓存连接失败信息。
cachesuccesses	310	仅缓存连接成功信息。
connectalias	330	传送到收件人地址中列出的任意主机。
connectcanonical	330	连接到 MTA 原本应该连接的系统的主机别名。
daemon	314	连接到特定主机系统而不考虑信封地址。
defaultmx	312	通道确定是否从网络中查找 MX。
defaultnameservers	313	查看 TCP/IP 栈选择的名称服务器。
forwardcheckdelete	311	如果已执行反向 DNS 查找，则接下来对返回的名称执行向前查找，以检查返回的 IP 号是否与原号相匹配；如果不匹配，则删除名称并使用 IP 地址。
forwardchecknone	311	DNS 反向查找后不执行向前查找。
forwardchecktag	311	如果已执行反向 DNS 查找，则接下来对返回的名称执行向前查找，以检查返回的 IP 号是否与原号相匹配；如果不匹配，则用 * 标记名称。
identnone	311	不执行 IDENT 查找；执行 IP 到主机名的转换；在 `Received:` 标题中包含主机名和 IP 地址。

表 12-2 按功能分类的通道关键字

关键字	页	定义
identnonelimited	311	不执行 IDENT 查找；执行 IP 到主机名的转换，但在通道切换期间不使用主机名；在 Received: 标题中包含主机名和 IP 地址。
identnonenumeric	311	不执行 IDENT 查找或 IP 到主机名的转换。
identnonesymbolic	311	不执行 IDENT 查找；执行从 IP 到主机名的转换；在 Received: 标题中仅包含主机名。
identtcp	311	对外来 SMTP 连接执行 IDENT 查找以及 IP 到主机名的转换；在 Received: 标题中包含标题
identtcplimited	311	对外来 SMTP 连接执行 IDENT 查找以及 IP 到主机名的转换，但在通道切换期间不使用主机名。在 Received: 标题中包含主机名和 IP 地址。
indenttcpnumeric	311	对外来 SMTP 连接执行 IDENT 查找，但不执行 IP 到主机名的转换。
identtcpsymbolic	311	对外来 SMTP 连接执行 IDENT 查找以及 IP 到主机名的转换；在 Received: 标题中仅包含主机名。
interfaceaddress	310	绑定到指定的 TCP/IP 接口地址。
lastresort	313	指定最后可用的主机。
mailfromdnsverify	305	验证 MAIL FROM: 命令中使用的域存在于 DNS 中。
mx	312	TCP/IP 网络和软件支持 MX 记录查找。
nameservers	313	指定要查看的名称服务器列表，而不查看 TCP/IP 栈自身选择的名称服务器；nameservers 要求用于名称服务器的以空格分隔的 IP 地址列表。
nocache	310	不缓存任何连接信息。
nomailfromdnsverify	305	不验证 MAIL FROM: 命令中使用的域存在于 DNS 中。
nomx	312	TCP/IP 网络不支持 MX 查找。
nonrandomemx	312	执行 MX 查找；对返回的具有同等优先级的条目不进行随机化处理。
port	310	指定用于 SMTP 连接的默认端口号。标准端口为 25。
randommx	312	执行 MX 查找；对返回的具有同等优先级的条目进行随机化处理。
single	314	指定应该为通道中每个目标地址分别创建一个邮件副本。
single_sys	314	为所用的每个目标系统创建一个邮件副本。
threaddepth	**325**	使用多线程 SMTP 客户机触发新线程的邮件的数目。
其他		
deferralrejectlimit	359	设置错误 RCPT TO 的数量限制：地址
dispositionchannel	353	将进程通道替换为用于初始队列传送状态通知 (DSN) 的位置。
destinationfilter	354	用于在一般 MTA 通道中指定应用于外发邮件的通道级别的过滤器。
filter	354	使用一个必需的 URL 参数，该参数说明过滤器文件的位置

表 12-2 按功能分类的通道关键字

关键字	页	定义
nodestinationfilter	354	通道的两个方向都没有启用通道邮箱过滤器。
nosourcefilter	354	没有为源通道启用通道邮箱过滤器。
nofilter	354	没有为通道启用用户邮箱过滤的默认值和方法。
notificationchannel	353	将进程通道替换为用于初始队列邮件处理通知 (MDN) 的位置。
sourcefilter	354	用于在一般 MTA 通道中指定应用于外来邮件的通道级别的过滤器。
submit	354	用于将通道标记为仅用来提交的通道。
user	354	用于 pipe 通道中，指明通道将在其下运行的用户名称。

配置通道默认值

许多配置使各种通道关键字在所有或几乎所有通道上重复。维护这样的配置不但麻烦而且容易出错。要简化某些配置，可以为各种通道指定默认的关键字。

例如，某个配置文件中的以下行表示该行后面所有通道块都将继承行中指定的关键字：

`defaults` *`keyword1 keyword2 keyword3 ...`*

我们可以认为， `defaults` 行是一个更改了关键字默认值但实际上并未指定通道的特殊通道块。 `defaults` 行也不需要任何附加的通道块信息行 （指定的信息行将被忽略）。

对于可以指定的 `defaults` 行数没有限制 — 多个默认行是累积的效果，其中最近遇到的行 （从顶部到底部读取）具有优先级。

从配置文件的某个点 （例如，外部文件中关于通道块的独立部分的开始处）开始无条件消除 `defaults` 行的影响是很有用的。为此我们提供了 `nodefaults` 行。例如，在配置文件中插入以下行将取消前面所有的默认通道创建的所有设置，并使配置返回到未指定默认值时所应用的状态：

```
nodefaults
```

与常规通道块一样，必须使用空行将每个 `defaults` 或 `nodefaults` 通道块与其他通道块分隔开来。在配置文件中， `defaults` 和 `nodefaults` 通道块是可以出现在本地通道之前的仅有的通道块。但是，与所有其他通道块一样，它们必须出现在最后的重写规则之后。

配置 SMTP 通道

根据安装的类型， Messaging Server 在安装时提供了多个 SMTP 通道 （请参见下表）。这些通道将实现基于 TCP/IP 的 SMTP。多线程的 TCP SMTP 通道包含一个多线程的 SMTP 服务器，该服务器在分发程序的控制下运行。外发 SMTP 邮件由通道程序 `tcp_smtp_client` 处理，并根据需要在作业控制器的控制下运行。

表 12-3 SMTP 通道

通道	定义
`tcp_local`	接收来自远程 SMTP 主机的外来邮件。根据是否使用智能主机 / 防火墙配置，将外发邮件直接发送到远程 SMTP 主机，或者将外发邮件发送到智能主机 / 防火墙系统。
`tcp_intranet`	在内部网中接收和发送邮件。
`tcp_auth`	用作 tcp_local 的切换通道；经过验证的用户将切换到 tcp_auth 通道，以避免中继阻止限制。
`tcp_submit`	在保留的提交端口 587 上接受邮件提交 （请参见 RFC 2476），这些提交通常来自用户代理。
`tcp_tas`	IA 特殊通道，站点使用该通道进行统一的邮件传送。

您可以修改上述通道的定义，或通过添加或删除本节中说明的关键字来创建新通道。此外，可以使用选项文件来控制 TCP/IP 通道的各种特性。此类选项文件必须存储于 MTA 配置目录 (*msg_svr_base*/config) 中，并命名为 *x_option*，其中 *x* 为通道名称。有关详细信息，请参见 Sun Java System Messaging Server Administration Reference。

本节分为以下小节：

- 第 300 页的 “配置 SMTP 通道选项”
- 第 300 页的 “SMTP 命令和协议支持”
- 第 308 页的 “TCP/IP 连接和 DNS 查找支持”
- 第 315 页的 “SMTP 验证、 SASL 和 TLS”
- 第 316 页的 “在标题中使用来自 SMTP AUTH 的已验证的地址”
- 第 316 页的 “在标题中使用来自 SMTP AUTH 的已验证的地址”
- 第 317 页的 “指定 Microsoft Exchange 网关通道”
- 第 317 页的 “传输层安全性”

配置 SMTP 通道选项

TCP/IP 通道选项文件可以控制 TCP/IP 通道的各种特征。通道选项文件必须存储在 MTA 配置目录中，并命名为 *x*_option，其中 *x* 是通道的名称。例如，*/msg_svr_base*/config/tcp_local_option

选项文件由一个或多个关键字及其关联的值组成。例如，通过在选项文件中包含 DISABLE_EXPAND 关键字并将值设置为 1，可以在服务器上禁用邮递列表扩展。

使用其他选项文件关键字可以进行以下设置：

- 对每个邮件中允许的收件人数量设置限制 (ALLOW_RECIPIENTS_PER_TRANSACTION)
- 对每个连接中允许的邮件数量设置限制 (ALLOW_TRANSACTIONS_PER_SESSION)
- 对记录到 MTA 日志文件中的信息类型进行微调 (LOG_CONNECTION，LOG_TRANPORTINFO)
- 指定客户机通道程序允许的同时外发连接的最大数量 (MAX_CLIENT_THREADS)

有关所有通道选项关键字和语法的信息，请参见 Messaging Server Reference Manual。

SMTP 命令和协议支持

您可以指定 SMTP 通道是否支持特定的 SMTP 命令，例如 EHLO、 ETRN、 EXPN 和 VRFY。您也可以指定通道是否支持 DNS 域验证，通道接受为行终止符的字符等。本节说明了以下内容：

- 第 302 页的 “通道协议选定和行终止符”
- 第 303 页的 “EHLO 命令支持”
- 第 303 页的 “ETRN 命令支持”
- 第 304 页的 “VRFY 命令支持”
- 第 305 页的 “DNS 域验证”
- 第 306 页的 “字符集标记和 8 位数据”
- 第 307 页的 “协议流”

表 12-4 汇总了本节中说明的关键字。

表 12-4 SMTP 命令和协议关键字

通道关键字	说明
协议选定和行终止符	**指定通道是否支持 SMTP 协议，并指定接受为行终止符的字符序列。**
smtp	支持 SMTP 协议。关键字 smtp 对所有 SMTP 通道都具有强制性。（此关键字等效于 smtp_crorlf。）
nosmtp	不支持 SMTP 协议。该值为默认值。
smtp_cr	接受以回车 (CR) （不跟换行符 [LF]）终止的行。
smtp_crlf	必须以回车 (CR) 加换行符 (LF) 序列终止行。
smtp_lf	接受以换行符 (LF) （前面没有 CR）终止的行。
smtp_crorlf	可以使用回车 (CR)、换行符 (LF) 序列或完整的 CRLF 终止行。
EHLO 关键字	**指定通道处理 EHLO 命令的方式**
ehlo	在初始连接中使用 SMTP EHLO 命令。
checkehlo	检查 SMTP 响应标题，以确定使用 EHLO 还是 HELO。
noehlo	不使用 EHLO 命令。
ETRN 关键字	**指定通道处理 ETRN 命令 （请求队列处理）的方式**
allowetrn	执行 ETRN 命令。
blocketrn	阻止 ETRN 命令。
domainetrn	仅执行指定域的那些 ETRN 命令。
silentetrn	执行 ETRN 命令，不回显通道信息。
sendetrn	发送 ETRN 命令。
nosendetrn	不发送 ETRN 命令。
VRFY 关键字	**指定通道处理 VRFY 命令的方式**
domainvrfy	使用完整地址发出 VRFY 命令。
localvrfy	使用本地地址发出 VRFY 命令。
novrfy	不发出 VRFY 命令。
vrfyallow	向 VRFY 命令提供信息响应。
vrfydefault	根据通道的 HIDE_VERIFY 选项设置，向 VRFY 命令提供默认响应。
vrfyhide	向 SMTP VRFY 命令提供模糊的响应。
EXPN 关键字	**指定通道处理 EXPN 关键字的方式**

表 12-4 SMTP 命令和协议关键字

通道关键字	说明
expnallow	允许 EXPN，即使已使用 DISABLE_EXPAND SMTP 通道选项在 SMTP 服务器级别禁用 EXPN。
expndisable	无条件禁用 EXPN。
expndefault	如果已将 SMTP 服务器设置为允许 EXPN，则允许 EXPN。（默认值）
DNS 域验证	**指定通道是否执行 DNS 域验证**
mailfromdnsverify	验证 MAIL FROM: 命令中使用的域存在于 DNS 中。
nomailfromdnsverify	不验证 MAIL FROM: 命令中使用的域存在于 DNS 中。
字符集和八位数据	**指定通道处理八位数据的方式 （注意：尽管这些关键字通常用于 SMTP 通道中，但是它们与所有类型的通道都具有潜在的相关性。）**
charset7	与 7 位文本邮件关联的默认字符集
charset8	与 8 位文本邮件关联的默认字符集
charsetesc	与包含换码符的 7 位文本关联的默认字符集
eightbit	通道支持八位字符。
eightnegotiate	如果可能，通道应对使用八位传输进行协商。
eightstrict	通道应拒绝包含非法的八位数据的邮件。
sevenbit	通道不支持八位字符；必须对八位字符进行编码。
协议流	**指定通道要使用的协议流的程度**
streaming	控制与通道关联的协议中使用的协议流的程度。

通道协议选定和行终止符

关键字：smtp、 nosmtp、 smtp_crlf、 smtp_cr、 smtp_crorlf 和 smtp_lf

关键字 smtp 和 nosmtp 指定通道是否支持 SMTP 协议。 smtp 关键字或它的其中一个变量对所有 STMP 通道都具有强制性。

关键字 smtp_crlf、 smtp_cr、 smtp_crorlf 和 smtp_lf 可用于在 SMTP 通道上指定 MTA 将接受作为行终止符的字符序列。关键字 smtp_crlf 的意思是必须以回车 (CR) 加换行符 (LF) 序列终止行。关键字 smtp_lf 或 smtp 的意思是接受前面不带 CR 的 LF。最后， smtp_cr 的意思是接受后面不跟 LF 的 CR。上述选项只对外来内容的处理有影响。

由于 SMTP 标准要求将 CRLF 作为行终止符，因此 MTA 始终生成标准的 CRLF 序列。各种 smtp 关键字只控制 MTA 是否接受其他非标准行终止符。例如，如果希望 MTA 只接受完全合法的 SMTP 邮件，拒绝所有带有非标准行终止符的邮件，则可以指定 stmp_crlf。

EHLO 命令支持

关键字：ehlo、 noehlo 和 checkehlo

SMTP 协议已经被扩展 (RFC 1869) 为允许附加命令的协商。这是通过使用新的 EHLO 命令 （替代 RFC 821 的 HELO 命令）来进行的。扩展的 SMTP 服务器通过提供服务器支持的扩展列表来响应 EHLO。未扩展的服务器返回未知命令错误，然后客户机发送旧的 HELO 命令。

这种应变策略通常与扩展的服务器和未扩展的服务器都能协同工作。但是不按照 RFC 821 实现 SMTP 的服务器却会出现问题。尤其是，某些不兼容的服务器在收到未知命令后会断开连接。

当任何服务器收到 EHLO 后断开连接时，SMTP 客户机实现尝试重新连接并使用 HELO 的策略。但是，如果远程服务器收到 EHLO 后不仅断开连接而且进入问题状态，则该策略可能无法工作。

为了处理上述情况，我们提供了通道关键字 ehlo、noehlo 和 checkehlo。关键字 ehlo 通知 MTA 在所有初始连接尝试中使用 EHLO 命令。关键字 noehlo 禁用所有对 EHLO 命令的使用。关键字 checkehlo 测试远程 SMTP 服务器返回的响应标题中是否含有字符串 "ESMTP"。如果查找到该字符串，则使用 EHLO ；如果未查找到，则使用 HELO。默认行为是在所有初始连接尝试中使用 EHLO，除非标题行含有字符串 "fire away"，在这种情况下将使用 HELO ；请注意，没有与此默认行为相对应的关键字，它介于 ehlo 和 checkehlo 关键字产生的行为之间。

ETRN 命令支持

关键字：allowetrn、 blocketrn、 disableetrn、 domainetrn、 silentetrn、 sendetrn、 nosendetrn、 novrfy

ETRN 命令 （在 RFC 1985 中定义）对 SMTP 服务进行了扩展，使 SMTP 客户机和服务器可以交互操作，从而使服务器有机会启动对于将进入给定主机的邮件队列的处理。

使用 ETRN， SMTP 客户机可以请求远程 SMTP 服务器启动对于将被发送到 SMTP 客户机的邮件队列的处理。这样， ETRN 提供了对进入自身系统的邮件实现远程 SMTP 系统 “轮询”的方法。这对于彼此之间只有瞬态连接的系统 （例如，设置为其他站点 [只能拨号连接到 Internet] 的辅助邮件交换 [MX] 主机的站点）可能会很有用。通过启用该命令，远程 （可能是拨号）服务器可以请求对其邮件的传送。

SMTP 客户机在 SMTP ETRN 命令行中指定要向其发送邮件的系统名 （通常为 SMTP 客户机系统自身的名称）。如果远程 SMTP 服务器支持 ETRN 命令，它将触发执行一个单独的进程，以重新连接到指定的系统，并为该系统发送所有正在等待传送的邮件。

对 *ETRN* 命令的响应

当发送邮件的 SMTP 客户机发出 ETRN 命令，请求 MTA 尝试传送 MTA 队列中的邮件时， allowetrn、 blocketrn、 domainetrn 和 silentetrn 关键字将控制 MTA 的响应。

默认情况下， MTA 将尝试执行所有 ETRN 命令；也就是说，将启用 allowetrn 关键字。通过在通道定义中包含 blocketrn 关键字可以指定 MTA 不执行 ETRN 命令。

通过包含 silentetrn 关键字，可以指定 MTA 执行所有 ETRN 命令，但不回显域所匹配的、MTA 将尝试运行的通道名。domainetrn 关键字指定 MTA 仅执行指定了域的 ETRN 命令；另外它还使 MTA 不回显域所匹配的、 MTA 将尝试运行的通道名。

disableetrn 完全禁用对 ETRN 命令的支持； SMTP 服务器不将 ETRN 公布为支持的命令。

发送 *ETRN* 命令

sendetrn 和 nosendetrn 通道关键字控制 SMTP 连接开始时 MTA 是否发送 ETRN 命令。默认设置为 nosendetrn，表示 MTA 将不发送 ETRN 命令。如果远程 SMTP 服务器声称支持 ETRN， sendetrn 关键字将通知 MTA 发送 ETRN 命令。 sendetrn 关键字后面应跟请求尝试传送其邮件的系统的名称。

VRFY 命令支持

关键字：domainvrfy、 localvrfy、 vrfyallow、 vrfydefault 和 vrfyhide

VRFY 命令使 SMTP 客户机能够向 SMTP 服务器发送请求，请求验证特定用户名称的邮件是否位于服务器中。 VRFY 命令是在 RFC 821 中定义的。

服务器将发送响应，表明用户是否本地用户、是否要转发邮件等。编号为 250 的响应表示用户名是本地的；编号为 251 的响应表示用户名不是本地的，但服务器可以转发邮件。服务器响应包含邮箱名称。

发送 *VRFY* 命令

正常情况下，没有理由将 VRFY 命令作为 SMTP 对话的一部分发出。 SMTP RCPT TO 命令应该执行与 VRFY 相同的功能，并返回相应的错误。但是，存在这样一些服务器，它们可以接受 RCPT TO 中的所有地址 （以后退回），但是在 VRFY 命令中同样的服务器却执行更全面的检查。

默认情况下， MTA 不发送 VRFY 命令 （启用 novrfy 关键字）。

如果需要，可以通过在通道定义中包含 domainvrfy 或 localvrfy 关键字将 MTA 配置为发出 SMTP VRFY 命令。使用关键字 domainvrfy 可以发出 VRFY 命令，并将完整地址 (user@host) 作为其变量。 localvrfy 关键字使 MTA 发出仅带有地址的本地部分 (user) 的 VRFY 命令。

响应 *VRFY* 命令

当发送邮件的 SMTP 客户机发出 SMTP VRFY 命令时，关键字 vrfyallow、vrfydefault 和 vrfyhide 控制 SMTP 服务器的响应。

vrfyallow 关键字通知 MTA 发出提供详细信息的响应。 vrfydefault 通知 MTA 提供具有详细信息的响应，除非已经指定通道选项 HIDE_VERIFY=1。 vrfyhide 关键字通知 MTA 只发出模糊的响应。与 HIDE_VERIFY 选项相反，上述关键字允许控制每个通道的 VRFY 响应，而 HIDE_VERIFY 通常适用于通过同一 SMTP 服务器处理的所有外来 TCP/IP 通道。

EXPN 支持

关键字：expnallow、 expndisable、 expndefault

expnallow 允许 EXPN，即使已使用 DISABLE_EXPAND SMTP 通道选项在 SMTP 服务器级别禁用 EXPN。expndisable 无条件禁用 EXPN。如果已将 SMTP 服务器设置为允许 EXPN （默认），则 expndefault 允许 EXPN。可以基于列表禁用扩展，但如果在服务器级别禁用扩展，基于列表的设置将是不相关的设置。

DNS 域验证

关键字：mailfromdnsverify 和 nomailfromdnsverify

在外来 TCP/IP 通道中设置 mailfromdnsverify 后， MTA 将验证 DNS 中是否存在 SMTP MAIL FROM 命令中使用的域条目，如果不存在该条目，则拒绝邮件。默认设置 nomailfromdnsverify 的意思是不执行上述检查。请注意，对返回的地址域执行 DNS 检查将导致某些需要的有效邮件 （例如，来自仅仅是未注册域名的合法站点的邮

件，或 DNS 中有错误信息时）被拒绝；这违背了 “RFC 1123：Internet 主机要求” 中表达的大量接收信息以及尽量让 e-mail 通过的精神。但是某些站点可能需要执行上述检查，以防使用伪造的电子邮件地址从不存在的域发送主动提供的批量电子邮件 (UBE)。

由于在 COM 和 ORG 顶层域中引入 DNS 通配符条目导致 mailfromdnsverify 作用减小，因此已对 mailfromdnsverify 代码进行了修改。 DNS 返回一个或多个 A 记录时，系统会将这些值与新 MTA 选项 BLOCKED_MAIL_FROM_IPS 指定的域文字进行比较。如果找到匹配项，则该域被视为无效。为了恢复正常操作，当前的正确设置为：

```
BLOCKED_MAIL_FROM_IPS=[64.94.110.11]
```

此选项的默认值为空字符串。

字符集标记和 8 位数据

关键字：charset7、 charset8、 charsetesc、 sevenbit、 eightbit、 eightnegotiate 和 eightstrict

字符集标记

MIME 规范提供了一种机制，用以标记纯文本邮件中使用的字符集。特别是，可以将参数 charset= 指定为 Content-type: 标题行。 MIME 中定义了各种字符集名称，包括 US-ASCII （默认）、 ISO-8859-1、 ISO-8859-2 以及随后定义的许多其他字符集。

某些现有系统和用户代理不提供生成上述字符集标记的机制；因此某些纯文本邮件可能未被正确标记。 charset7、 charset8 和 charsetesc 通道关键字提供了针对每个通道的机制，用以指定字符集名称，该名称将被插入到缺少字符集标记的邮件标题中。每个关键字都需要一个参数来指定字符集名称。系统不检查名称的有效性。但是请注意，只能对 MTA 表格目录的字符集定义文件 charsets.txt 中指定的字符集进行字符集转换。如果可能，请使用该文件中定义的名称。

如果邮件仅包含七位字符，则使用 charset7 字符集名称；如果在邮件中发现八位数据，则使用 charset8 字符集名称；如果邮件仅包含七位数据并同时包含换码符，则使用 charsetesc。如果未指定正确的关键字，字符集名称将不被插入到 Content-type: 标题行。

请注意， charset8 关键字还控制邮件标题中 8 位字符的 MIME 编码 （标题中 8 位字符是绝对非法的）。如果未指定 charset8， MTA 通常对邮件标题中遇到的所有 （非法） 8 位数据进行 MIME 编码，将其标记为未知字符集。

这些字符集规范不会覆盖现有的标记，也就是说，如果邮件已经具有字符集标记或者不属于文本类型的邮件，则字符集规范没有任何影响。通常应当对 MTA 本地通道进行如下标记：

```
l ... charset7 US-ASCII charset8 ISO-8859-1 ...
hostname
```

如果邮件中没有 Content-type 标题，将添加该标题。如果缺少 MIME-version: 标题行，此关键字也添加该标题行。

如果通道接收的未标记邮件使用了日语或韩语字符集并包含换码符， charsetesc 关键字将尤其有用。

八位数据

某些传输限制使用带有大于 127 （十进制）的序数值的字符。尤其需要注意的是，某些 SMTP 服务器会删除高位值，因而使用上述八位范围中的字符的邮件将出现乱码。

Messaging Server 提供了对这类邮件进行自动编码的功能，以便有问题的八位字符不直接出现在邮件中。通过指定 sevenbit 关键字，可以将该编码功能应用到所有加入给定通道队列的邮件。如果不存在这类限制，应将通道标记为 eightbit。

SMTP 协议不允许 eightbit 数据，“除非远程 SMTP 服务器明确声称支持允许 eightbit 数据的 SMTP 扩展”。某些传输 （例如扩展的 SMTP）可能会实际支持某种形式的协商，以确定是否可以传输八位字符。因此，我们强烈建议使用 eightnegotiate 关键字，以便在协商失败时指示通道对邮件进行编码。这是所有通道的默认设置；不支持协商的通道将假定传输可以处理八位数据。

eightstrict 关键字通知 Messaging Server 拒绝所有标题包含非法八位数据的外来邮件。

协议流

关键字：streaming

某些邮件协议支持流操作。这意味着 MTA 可以同时发出多个操作，并等待每个操作的回复分批到达。 streaming 关键字控制与通道关联的协议中使用的协议流的程度。此关键字要求一个整数参数；参数的解释方式取决于所使用的特定协议。

正常情况下，系统使用 SMTP 流水线作业扩展来协商可用的流支持的程度。因此，正常情况下不应该使用此关键字。

流操作可用值的范围是 0 到 3。0 不指定流操作，1 使 RCPT TO 命令组进行流操作，2 使 MAIL FROM/RCPT TO 进行流操作，3 使 HELO/MAIL FROM/RCPT TO 或 RSET/MAIL FROM/RCPT TO 进行流操作。默认值是 0。

TCP/IP 连接和 DNS 查找支持

您可以指定有关服务器如何处理 TCP/IP 连接和地址查找的信息。本节说明了以下内容：

- 第 310 页的 “TCP/IP 端口号和接口地址”
- 第 310 页的 “缓存通道连接信息”
- 第 311 页的 “反向 DNS 查找”
- 第 311 页的 “IDENT 查找”
- 第 312 页的 “TCP/IP MX 记录支持”
- 第 313 页的 “名称服务器查找”
- 第 313 页的 “最后可用的主机”
- 第 313 页的 “外来邮件的备用通道 （切换通道）”
- 第 314 页的 “目标主机选择”

表 12-5 列出了本节中说明的 TCP/IP 连接和 DNS 查找关键字。

表 12-5 TCP/IP 连接和 DNS 查找关键字

通道关键字	说明
端口选定和接口地址	**指定用于 SMTP 连接的默认端口号和接口地址**
port	指定用于 SMTP 连接的默认端口号。标准端口为 25。
interfaceaddress	绑定到指定的 TCP/IP 接口地址。
缓存关键字	**指定对连接信息进行缓存的方式**
cacheeverything	缓存所有连接信息。
cachefailures	仅缓存连接失败信息。
cachesuccesses	仅缓存连接成功信息。
nocache	不缓存任何连接信息。
反向 DNS 查找	**指定对外来 SMTP 连接进行反向 DNS 查找的方式**

表 12-5 TCP/IP 连接和 DNS 查找关键字

通道关键字	说明
forwardcheckdelete	如果已执行反向 DNS 查找，则接下来对返回的名称执行向前查找，以检查返回的 IP 号是否与原号相匹配；如果不匹配，则删除名称并使用 IP 地址。
forwardchecknone	DNS 反向查找后不执行向前查找。
forwardchecktag	如果已执行反向 DNS 查找，则接下来对返回的名称执行向前查找，以检查返回的 IP 号是否与原号相匹配；如果不匹配，则用 * 标记名称。
IDENT 查找 /DNS 反向查找	**指定对外来 SMTP 连接进行 IDENT 查找和 DNS 反向查找的方式**
identnone	不执行 IDENT 查找；执行 IP 到主机名的转换；在 Received: 标题中包含主机名和 IP 地址。
identnonelimited	不执行 IDENT 查找；执行 IP 到主机名的转换，但在通道切换期间不使用主机名；在 Received: 标题中包含主机名和 IP 地址。
identnonenumeric	不执行 IDENT 查找或 IP 到主机名的转换。
identnonesymbolic	不执行 IDENT 查找；执行从 IP 到主机名的转换；在 Received: 标题中仅包含主机名。
identtcp	对外来 SMTP 连接执行 IDENT 查找以及 IP 到主机名的转换；在 Received: 标题中包含标题
identtcplimited	对外来 SMTP 连接执行 IDENT 查找以及 IP 到主机名的转换，但在通道切换期间不使用主机名。在 Received: 标题中包含主机名和 IP 地址。
indenttcpnumeric	对外来 SMTP 连接执行 IDENT 查找，但不执行 IP 到主机名的转换。
identtcpsymbolic	对外来 SMTP 连接执行 IDENT 查找以及 IP 到主机名的转换；在 Received: 标题中仅包含主机名。
MX 记录支持和 TCP/IP 名称服务器	**指定通道是否支持 MX 记录查找以及支持的方式**
mx	TCP/IP 网络和软件支持 MX 记录查找。
nomx	TCP/IP 网络不支持 MX 查找。
defaultmx	通道确定是否从网络中查找 MX。
randommx	执行 MX 查找；对返回的具有同等优先级的条目进行随机化处理。
nonrandomemx	执行 MX 查找；对返回的具有同等优先级的条目不进行随机化处理。
nameservers	指定要查看的名称服务器列表，而不查看 TCP/IP 栈自身选择的名称服务器；nameservers 要求用于名称服务器的以空格分隔的 IP 地址列表。
defaultnameservers	查看 TCP/IP 栈选择的名称服务器。
lastresort	指定最后可用的主机。
切换关键字	**控制外来邮件的备用通道的选定**
allowswitchchannel	允许从 switchchannel 通道切换到此通道
noswitchchannel	停留在服务器通道；不切换到与发件主机关联的通道；不允许被切换。

表 12-5 TCP/IP 连接和 DNS 查找关键字

通道关键字	说明
switchchannel	从服务器通道切换到与发件主机关联的通道。
tlsswitchchannel	TLS 协商成功后，切换到其他通道。
saslswitchchannel	SASL 验证成功后，切换到其他通道。
目标主机的选择和邮件副本的存储	**指定目标主机系统及存储邮件副本的方式。**
daemon	连接到特定主机系统而不考虑信封地址。
single	指定应该为通道中每个目标地址分别创建一个邮件副本。
single_sys	为所用的每个目标系统创建一个邮件副本。

TCP/IP 端口号和接口地址

关键字：port 和 interfaceaddress

发送邮件时，基于 TCP/IP 的 SMTP 通道连接到端口 25。可以使用 port 关键字来指示基于 TCP/IP 的 SMTP 通道连接到非标准端口。请注意，该关键字是分发程序选项 PORT 的补充，该选项控制 MTA 监听的用于接受 SMTP 连接的端口。

interfaceaddress 关键字控制 TCP/IP 通道绑定为外发连接源地址的地址；也就是说，在具有多个接口地址的系统中，当 MTA 发送外发 SMTP 邮件时，此关键字控制用作源 IP 地址的地址。请注意，此关键字是分发程序选项 INTERFACE_ADDRESS 的补充，此选项控制 TCP/IP 通道监听的用于接受外来连接和邮件的通道。

缓存通道连接信息

关键字：cacheeverything、 nocache、 cachefailures 和 cachesuccesses

使用 SMTP 协议的通道保持了一个高速缓存，该缓存中包含以前的连接尝试的历史纪录。使用该高速缓存可以避免多次重新连接到不可访问的主机，多次连接会浪费很多时间并造成其他邮件的延迟。这是基于每个进程的高速缓存，仅存在于外发 SMTP 传送通道的单次运行期间。

高速缓存通常记录连接成功信息和失败信息。（记录成功的连接尝试是为了抵消以后的失败 — 以前成功但现在失败的主机并不保证在进行另一次连接尝试之前的延迟时间会与从未尝试连接或以前曾经连接失败的主机一样长。）

但是 MTA 使用的缓存策略不一定适合所有情况。因此我们提供了通道关键字以调整 MTA 缓存。

cacheeverything 关键字启用所有形式的缓存，也是默认设置。nocache 关键字禁用所有缓存。

cachefailures 关键字启用连接失败的缓存，但不启用连接成功的缓存 — 这比 cacheeverything 对重试的限制更严。最后，cachesuccesses 只对成功连接进行缓存。对于 SMTP 通道，该关键字与 nocache 的效果相同。

反向 DNS 查找

关键字：forwardchecknone、 forwardchecktag 和 forwardcheckdelete

forwardchecknone、 forwardchecktag 和 forwardcheckdelete 通道关键字可以修改进行反向 DNS 查找的结果。上述关键字可以控制 MTA 是否向前查找使用 DNS 反向查找发现的 IP 名，如果请求向前查找，则指定当 IP 名称的向前查找与原来的连接 IP 号不匹配时 MTA 要执行的操作。

forwardchecknone 关键字是默认设置，表示不进行向前查找。 forwardchecktag 关键字通知 MTA 在每次反向查找后进行向前查找，如果使用向前查找发现的号码与原来的连接号码不匹配，则用星号 (*) 标记 IP 名称。 forwardcheckdelete 关键字通知 MTA 在每次反向查找后进行向前查找，如果该名称的向前查找与原来的连接 IP 地址不匹配，则忽略 （删除）反向查找返回的名称；在这种情况下， MTA 使用原来的 IP 地址。

注 在很多站点中，向前查找与原来的 IP 地址不匹配是很正常的，因为这些站点将较为 “普通”的 IP 名称用于多个不同的 IP 地址。

IDENT 查找

关键字：identnone、 identnonelimited、 identtnonnumeric、 identnonesymbolic、 identtcp、 identtcpnumeric、 identtcpsymbolic 和 identtcplimited

IDENT 关键字控制 MTA 使用 IDENT 协议处理连接和查找的方式。 IDENT 协议在 RFC 1413 中有所说明。

关键字 identtcp、 identtcpsymbolic 和 identtcpnumeric 告诉 MTA 执行连接并使用 IDENT 协议进行查找。从 IDENT 协议获取的信息 （通常是进行 SMTP 连接的用户的身份）将按照以下方式被插入到邮件的 Received: 标题中：

- identtcp 插入与外来 IP 号相应的主机名 （如 DNS 反向查找所报告）和 IP 号码本身。

- identtcpsymbolic 插入与外来 IP 号相应的主机名 （如 DNS 反向查找所报告），IP 号码本身不包含在 Received: 标题中。
- identtcpnumeric 插入实际的外来 IP 号 — 不对 IP 号执行 DNS 反向查找。

注 远程系统必须运行 IDENT 服务器， identtcp、 identtcpsymbolic 或 identtcpnumeric 引起的 IDENT 查找才能够有用。

请注意， IDENT 查询尝试可能会使性能下降。不断增加的路由器将使尝试连接到无法识别的端口的操作进入 “黑洞”。如果在 IDENT 查询时出现这种情况，则 MTA 直到连接超时 （TCP/IP 栈控制的超时，一般为大约一至二分钟）后才能收到返回的结果。

当把 identtcp、 indenttcplimited 或 identtcpsymbolic 与 identtcpnumeric 进行比较时，会出现另一个性能方面的因素。用 identtcp、 identtcplimited 或 identtcpsymbolic 调用的 DNS 反向查找为了获得对用户更加友好的主机名会导致额外的开销。

identnone 关键字禁用 IDENT 查找，但是指定 IP 到主机名的转换，并在邮件的 Received: 标题中只包含主机名。

identnonesymbolic 关键字禁用 IDENT 查找，但是执行 IP 到主机名的转换；邮件的 Received: 标题中只包含主机名。

identnonenumeric 关键字禁用 IDENT 查找，并禁止通常的 IP 号到主机名的 DNS 反向查找转换，这可能会使性能得到改善，但会减少 Received: 标题中的用户友好信息。该值为默认值。

就 IDENT 查找、反向 DNS 查找以及 Received: 标题中显示的信息而言，identtcplimited 和 identnonelimited 关键字的效果分别与 identtcp 和 identnone。不同点在于，使用关键字 identtcplimited 或 identnonelimited 时，始终将 IP 字面地址作为所有通道切换 （由于使用 switchchannel 关键字）的基础，而不考虑 DNS 反向查找是否成功确定了主机名。

TCP/IP MX 记录支持

关键字：mx、 nomx、 defaultmx、 randommx 和 nonrandommx

某些 TCP/IP 网络支持使用 MX（邮件转发）记录，某些网络则不支持。如果 MTA 系统连接到的网络未提供 MX 记录，可以将某些 TCP/IP 通道程序配置为不使用 MX 记录。 mx、 nomx、 defaultmx、 randommx 和 nonrandommx 关键字控制 MX 记录支持。

关键字 randommx 指定应该执行 MX 查找，并且应该按随机顺序处理具有同等优先级的 MX 记录的值。关键字 nonrandommx 指定应该执行 MX 查找，并且应该按与接收顺序相同的顺序处理具有同等优先级的 MX 值。

mx 关键字当前与 nonrandommx 等效；在将来的版本中可能将其更改为与 randommx 等效。 nomx 关键字禁用 MX 查找。 defaultmx 关键字指定如果网络声称支持 MX 记录，则应该使用 mx。在支持任何形式的 MX 查找的通道中，关键字 defaultmx 是默认设置。

名称服务器查找

关键字： nameservers 和 defaultnameservers

执行名称服务器查找时，可以使用 nameservers 通道关键字指定要查看的名称服务器列表，而不查看 TCP/IP 栈自身选择的名称服务器。 nameservers 关键字要求用于名称服务器的以空格分隔的 IP 地址列表，如以下示例所示：

```
nameservers 1.2.3.1 1.2.3.2
```

默认设置 defaultnameservers 表示使用 TCP/IP 栈自身选择的名称服务器。

要在 UNIX 中防止名称服务器查找，您可以修改 nsswitch.conf 文件。在 NT 中，请修改 TCP/IP 配置。

最后可用的主机

关键字： lastresort

lastresort 关键字用于指定所有其他连接失败后连接到的主机。实际上，它充当最后可用的 MX 记录。它只在 SMTP 通道中有用。

此关键字需要一个参数，用以指定 “最后可用的系统”的名称。例如：

```
tcp_local single_sys smtp mx lastresort mailhub.siroe.com
TCP-DAEMON
```

外来邮件的备用通道 （切换通道）

关键字： switchchannel、 allowswitchchannel 和 noswitchchannel。另请参见 315 页中的 saslswitchchannel 和 317 页中的 tlsswitchchannel。

以下关键字控制用于外来邮件的备用通道的选择：switchchannel、allowswitchchannel 和 noswitchchannel。

当 MTA 接收来自远程系统的外来连接时，它必须选择将与该连接关联的通道。通常该选择取决于所使用的传输；例如，外来的基于 TCP/IP 的 SMTP 连接将自动与 tcp_local 通道关联。

但是，如果使用具有不同特性的多个外发通道来处理基于相同传输的不同系统时，将无法再使用该约定。这时，外来连接无法关联到与外发连接相同的通道，造成相应的通道特性无法关联到远程系统。

switchchannel 关键字提供了解决上述问题的方法。如果在服务器使用的初始通道中指定了切换通道，则连接 （发件）主机的 IP 地址将与通道表进行匹配，如果匹配，将对源通道进行相应更改。如果未查找到匹配的 IP 地址，或查找到的匹配地址与原来默认的外来通道相同， MTA 可以选择尝试使用进行 DNS 反向查找时查找到的主机名进行匹配。可以将源通道更改为标记为 switchchannel 或 allowswitchchannel （默认设置）的任意通道。 noswitchchannel 关键字指定不对通道或从通道执行通道切换操作。

默认情况下，在与服务器关联的通道以外的通道中指定 switchchannel 将没有效果。目前， switchchannel 只影响 SMTP 通道，但是实际上在任何其他通道中使用 switchchannel 都不合理。

目标主机选择

关键字：daemon、 single 和 single_sys

daemon 关键字的解释和用法取决于应用该关键字的通道的类型。

daemon 关键字用于 SMTP 通道，以控制目标主机的选择。

通常，连接到任意主机的通道都被列在正被处理的邮件的信封地址中。使用 daemon 关键字可以通知通道连接到特定的远程系统 （一般是防火墙或邮件集线器系统），而不考虑信封地址。实际远程系统的名称应该直接出现在 daemon 关键字之后，如以下示例所示：

```
tcp_firewall smtp mx daemon firewall.acme.com
TCP-DAEMON
```

如果 daemon 关键字之后的参数不是全限定域名，则参数将被忽略，通道将连接到它的正式主机。正式主机是与通道相关的全限定主机名。可以在包含三行的通道块的第二行中指定：

```
tcp_firewall smtp mx daemon router
firewall.acme.com
TCP-DAEMON
```

也可以在包含两行的通道块的 TCP-DAEMON 之后指定正式主机，这样，外发连接便可以将其自身识别为特定的主机：

```
tcp_firewall smtp mx daemon router
TCP-DAEMON firewall.acme.com
```

如果将防火墙或网关系统名称指定为正式主机名，通常将 daemon 关键字的给定参数指定为路由器，如以下示例所示：

```
tcp_firewall smtp mx daemon router
firewall.acme.com
TCP-DAEMON
```

其他重要关键字包括 single 和 single_sys。 single 关键字指定应该为通道中的每个目标地址分别创建一个邮件副本。 single_sys 关键字为所用的每个目标系统创建一个邮件副本。请注意，不管使用哪个关键字，至少为邮件在其排队的每个通道创建每个邮件的一个副本。

SMTP 验证、 SASL 和 TLS

关键字：maysaslserver、mustsaslserver、nosasl、nosaslserver、saslswitchchannel 和 nosaslswitchchannel

您可以控制 Messaging Server 是否支持使用 SASL （简单验证和安全层）对 SMTP 服务器进行验证。 SASL 在 RFC 2222 中定义，第 19 章 “配置安全和访问控制”中提供了有关 SASL、 SMTP 验证和安全性的详细信息。

maysaslserver、 mustsaslserver、 nosasl、 nosaslserver、 switchchannel 和 saslswitchchannel 通道关键字用于配置 SMTP 协议期间 SMTP 通道（例如 TCP/IP 通道）对 SASL (SMTP AUTH) 的使用。

nosasl 是默认设置，表示不允许或不尝试 SASL 验证。它包括 nosaslserver，表示不允许 SASL 验证。指定 maysaslserver 使 SMTP 服务器允许客户机尝试使用 SASL 验证。指定 mustsaslserver 使 SMTP 服务器坚持让客户机使用 SASL 验证；除非远程客户机验证成功，否则 SMTP 服务器不接受邮件。

使用 saslswitchchannel 使外来连接在客户机成功使用 SASL 后切换到指定的通道。它使用一个必需的值，以指定将切换到的通道。

在标题中使用来自 SMTP AUTH 的已验证的地址

关键字：authrewrite

authrewrite 通道关键字和相关的 AUTH_REWRITE 映射表允许使用从验证操作中获得的寻址信息修改标题和信封地址。特别是，可以将 SASL 验证配置为提供授权的电子邮件地址。通常使用 SMTP AUTH 信息，尽管通过 FROM_ACCESS 映射可能会覆盖该信息。 authrewrite 关键字使用要求的位值 （如表 12-6）。

表 12-6 authrewrite 位值

位	值	说明
0	1	不做任何更改 （默认）
1	2	添加 Sender: 或 Resent-sender: 标题字段，其中包含验证操作提供的地址。 Resent- 变量在具有其他 resent- 字段时使用。
2	4	添加 Sender: 标题字段，其中包含验证操作提供的地址。
3	8	在映射表中构造具有以下格式的名为 AUTH_REWRITE 的探测： *mail-from*|*sender*|*from*|*auth-sender* 其中， *mail-from* 是信封 From: 地址， *sender* 是来自 Sender: 或 Resent-sender: 标题字段的地址， *from* 是来自 From: 或 Resent-From: 标题字段的地址， *auth-sender* 是验证操作提供的地址。 结果是通过 AUTH_REWRITE 映射运行得到的。该映射应返回一个用垂直条 (|) 分隔的项目列表。这些项目通过设置下列标志并按顺序使用： $J $K 替换邮件的信封 From: 地址 $Y $T 添加合适的 Sender: 或 Resent-sender: 标题字段。 $N 拒绝邮件。映射结果提供错误消息的文本。如果未提供文本，则显示使用的创始者地址无效错误消息。 $Z 添加合适的 From: 或 Resent-from: 标题字段。（请注意，一般情况下，覆盖 From: 字段是很不可取的做法。） Resent- 变量在标题中具有其他 Resent- 字段时使用。
4	16	即使验证未提供已验证的地址，也应用 AUTH_REWRITE 映射。如果清除了此位，则仅在已验证的地址可用时才应用映射。
5	32	包含位于 AUTH_REWRITE 映射探测开头的源通道，该位以 | 与其他信息分隔开。如果清除了此位，则不包含通道。

注意 应严格限制 $Z 标志，因为很少合法地用它们来修改信封和标题地址。

指定 Microsoft Exchange 网关通道

关键字：msexchange 和 nomsexchange

msexchange 通道关键字可以用于 TCP/IP 通道，它通知 MTA 此通道是与 Microsoft Exchange 网关及客户机通信的通道。当被放置到已启用 SASL （通过 maysaslserver 或 mustsaslserver 关键字）的外来 TCP/IP 通道中时，它使 MTA 的 SMTP 服务器公布 AUTH 使用的是 “不正确” 格式 （基于原来的 ESMTP AUTH 规范，该规范实际上与正确的 ESMTP 用法不兼容，而不是基于新的正确的 AUTH 规范）。例如，某些 Microsoft Exchange 客户机不能识别正确的 AUTH 格式，只能识别错误的 AUTH 格式。

msexchange 通道关键字还使损坏的 TLS 命令得以公布 （和识别）。

nomsexchange 是默认设置。

传输层安全性

关键字：maytls、 maytlsclient、 maytlsserver、 musttls、 musttlsclient、 musttlsserver、 notls、 notlsclient、 notlsserver 和 tlsswitchchannel

maytls、 maytlsclient、 maytlsserver、 musttls、 musttlsclient、 musttlsserver、 notls、 notlsclient、 notlsserver 和 tlsswitchchannel 通道关键字用于配置 SMTP 协议期间基于 SMTP 的通道 （例如 TCP/IP 通道）对 TLS 的使用。

默认设置是 notls，表示不允许或不尝试 TLS。它包括 notlsclient 关键字和 notlsserver 关键字，前者表示 MTA SMTP 客户机不对外发连接尝试使用 TLS （外发连接期间不发出 STARTTLS 命令），后者表示 MTA SMTP 服务器不允许对外来连接使用 TLS （SMTP 服务器不公布 STARTTLS 扩展，也不接收命令本身）。

指定 maytls 将使 MTA 向外来连接提供 TLS，并对外发连接尝试 TLS。它包括 maytlsclient 和 maytlsserver，前者表示发送外发邮件时，如果是发送到支持 TLS 的 SMTP 服务器， MTA SMTP 客户机将尝试使用 TLS，后者表示 MTA SMTP 服务器将公布支持 STARTTLS 扩展，并允许在接收邮件时使用 TLS。

请注意，要使 TLS 正常工作，以下条件必须就位：

- 必须设置证书的保护 / 拥有权，以使 mailsrv 帐户可以访问文件。
- 存储证书的目录需要设置保护 / 拥有权以便 mailsrv 帐户可以访问该目录内的文件。

指定 musttls 将使 MTA 坚持在外来和外发连接中使用 TLS；电子邮件将不与未能成功协商 TLS 使用的远程系统进行交换。它包括 musttlsclient，表示 MTA SMTP 客户机坚持在发送外发邮件时使用 TLS，并且不对未能成功协商 TLS 使用的 SMTP 服务器发送邮件 （MTA 将发出 STARTTLS 命令，并且该命令必须成功）。它还包括 musttlsserver，表示 MTA SMTP 服务器将公布支持 STARTTLS 扩展，并坚持在接收外来邮件时使用 TLS，来自未能成功协商 TLS 使用的客户机的邮件将不被接收。

tlsswitchchannel 关键字用于使外来连接在客户机的 TLS 协商成功后切换到指定的通道。它使用一个必需的值，以指定将切换到的通道。

配置邮件处理和传送

您可以配置服务器何时基于特定条件尝试传送邮件。您也可以为作业处理指定参数，例如服务作业的处理限制或何时产生新的 SMTP 通道线程。本节说明了以下内容：

- 第 320 页的 “设置通道方向性”
- 第 320 页的 “实现延迟传送日期”
- 第 321 页的 “为传送失败的邮件指定重试频率。”
- 第 322 页的 “用于通道执行作业的处理池”
- 第 322 页的 “服务作业限制”
- 第 324 页的 “基于大小的邮件优先级”
- 第 325 页的 “SMTP 通道线程”
- 第 326 页的 “多个地址扩展”
- 第 326 页的 “启用服务转换”

有关邮件处理和传送的概念信息，请参见第 179 页的 “作业控制器”和第 225 页的 “作业控制器文件”。

表 12-7 汇总了本节中说明的关键字。

表 12-7 邮件处理和传送关键字

关键字	定义
立即传送	**定义邮件立即传送的规范。**
immnonurgent	紧急、正常和不紧急邮件提交后，立即开始传送。
通道方向性	**指定为通道服务的程序的类型。**

表 12-7 邮件处理和传送关键字

关键字	定义
bidirectional	主程序和从程序为通道服务。
master	主程序 (master) 为通道服务。
slave	从程序 (slave) 为通道服务。
延迟传送	**定义延迟作业的传送规范。**
backoff	指定尝试重新传送延迟邮件的频率。可以被 normalbackoff、nonurgentbackoff、 urgentbackoff 覆盖。
deferred	实现 Deferred-delivery: 标题行的识别和生效。
nodeferred	默认设置。指定不使 Deferred-delivery: 标题行生效。
nonurgentbackoff	尝试重新传送非紧急邮件的频率。
normalbackoff	尝试重新传送普通邮件的频率。
urgentbackoff	尝试重新传送紧急邮件的频率。
基于大小的邮件优先级	**基于邮件大小定义邮件优先级**
nonurgentblocklimit	将超过此大小的邮件强制降到非紧急优先级 （二类优先级）以下，意味着邮件将始终等待下一个周期的作业以进一步处理。
normalblocklimit	将超过此大小的邮件强制降到非紧急优先级。
urgentblocklimit	将超过此大小的邮件强制降至普通优先级。
用于通道执行作业的处理池	**指定用于处理具有不同紧急程度和延迟时间的邮件的池。**
pool	指定通道在其中运行的池。
after	指定通道运行前的时间延迟。
服务作业限制	**指定服务作业的数量和每个作业中处理的邮件文件的最大数量。**
maxjobs	指定可以同时为通道运行的作业的最大数量。
filesperjob	指定将由单个作业处理的队列条目的数量。
SMTP 通道线程	
threaddepth	使用多线程 SMTP 客户机触发新线程的邮件的数目。
多个地址扩展	**定义对于具有多个收件人的邮件的处理**
expandlimit	地址数目超过此限制时，“脱机”处理外来邮件。
expandchannel	指定由于应用 expandlimit 而在其中执行延迟扩展的通道。
holdlimit	地址数目超过此限制时，保留外来邮件。
事务限制	**指定连接事务限制**
transactionlimit	限制每个连接允许的邮件数目。

表 12-7 邮件处理和传送关键字

关键字	定义
无法传送邮件的通知	**指定何时发送无法传送邮件的通知。**
notices	指定在发送通知和返回邮件之前可能经过的时间。
nonurgentnotices	指定在发送通知和返回非紧急优先级邮件前可能经过的时间。
normalnotices	指定在发送通知和返回普通优先级邮件前可能经过的时间。
urgentnotices	指定在发送通知和返回紧急优先级邮件之前可能经过的时间。

设置通道方向性

关键字：master、 slave 和 bidirectional

这三个关键字用以指定通道是由主程序 (master)、从程序 (slave)，还是两者 (bidirectional) 为其服务。如果不指定关键字，则默认设置为 bidirectional。这些关键字确定当邮件在通道中排队时， MTA 是否启动传送活动。

这些关键字的使用反映了相应通道程序的某些基本特性。MTA 支持的各种通道的说明表明了应该在何时何处使用这些关键字。

实现延迟传送日期

关键字：deferred、 nodeferred、 immnonurgent

deferred 通道关键字实现对 Deferred-delivery:。具有 deferred 将来传送日期的邮件将被保留在通道队列中，直到过期并被返回，或者到达延迟传送日期。有关 Deferred-delivery: 标题行格式和操作的详细信息，。

关键字 nodeferred 是默认设置。请务必注意，尽管 RFC 1327 强制支持对延迟邮件的处理，但事实上该功能的实际实现使人们将邮件系统用做磁盘配额的扩展。

紧急、正常和不紧急邮件提交后，关键字 immnonurgent 将立即开始传送。

为传送失败的邮件指定重试频率。

关键字：backoff、 nonurgentbackoff、 normalbackoff、 urgentbackoff 和 notices

默认情况下，曾经传送失败的邮件的传送重试的频率取决于邮件的优先级。传送尝试之间的默认间隔 （以分钟计）如下所示。优先级后面的第一个数字表示初始传送失败后经过多少分钟进行第一次传送重试：

紧急：30, 60, 60, 120, 120, 120, 240
正常：60, 120, 120, 240, 240, 240, 480
不紧急：120, 240, 240, 480, 480, 480, 960

对于紧急邮件，初始传送失败后过 30 分钟尝试重试，第一次传送重试后过 60 分钟重试，第二次重试后过 60 分钟重试，第三次重试后过 120 分钟重试，等等。指定的最后一次尝试之后的重试将以同样的间隔进行。因此，对于紧急邮件来说，每 240 分钟重试一次。

传送尝试将在一定的时间周期内继续，该时间周期由关键字 notices、nonurgentnotices、 normalnotices 或 urgentnotices 指定。如果无法进行成功的传送，则生成**传送失败通知**并将邮件返回给发件人。（有关 notices 关键字的详细信息，请参见第 246 页的 “设置通知邮件传送间隔”。）

使用关键字 backoff 可以为不同优先级的邮件指定传送重试间隔的自定义设置。nonurgentbackoff 指定不紧急邮件的间隔。 normalbackoff 指定正常邮件的间隔。urgentbackoff 指定紧急邮件的间隔。如果不指定上述关键字， backoff 将为所有邮件指定间隔，而不考虑优先级。

下面显示了一个示例：

```
urgentbackoff "pt30m" "pt1h" "pt2h" "pt3h" "pt4h" "pt5h" "pt8h" "pt16h"
```

此实例中，紧急邮件在初始传送失败后过 30 分钟尝试重新传送，第一次传送尝试后过 1 小时 （初始失败后 1 小时 30 分钟）重试，第二次传送尝试后过 2 小时重试，第三次传送尝试后过 3 小时重试，第四次传送尝试后过 4 小时重试，第五次传送尝试后过 5 小时重试，第六次传送尝试后过 8 小时重试，第七次传送尝试后过 16 小时重试。之后每 16 小时进行一次尝试，直到 notices 关键字指定的时间周期结束。如果无法进行成功的传送，则生成传送失败通知并将邮件返回发件人。请注意，间隔语法位于 ISO 8601P 中， Sun Java System Messaging Server Administration Reference 中对其进行了说明。

在接下来的示例中，

```
normalbackoff "pt30m" "pt1h" "pt8h" "p1d" "p2d" "p1w"
```

正常邮件在初始传送失败后过 30 分钟尝试重新传送，第一次传送尝试后过 1 小时重试，第二次尝试后过 8 小时重试，第三次尝试后过 1 天重试，第四次尝试后过 2 天重试，第五次尝试后过 1 周重试，之后每周重复一次，直到 notices 关键字指定的时间周期结束。如果无法进行成功的传送，则生成传送失败通知并将邮件返回发件人。

在最后的示例中，

```
backoff "pt30m" "pt120m" "pt16h" "pt36h" "p3d"
```

无论邮件的优先级是什么，所有传送失败的邮件 （除非被 nonurgentbackoff、normalbackoff 或 urgentbackoff 覆盖）将在初始传送失败后过 30 分钟重试，第一次重试后过 2 小时重试，第二次尝试后过 16 小时重试，第三次尝试后过 36 小时重试，第四次尝试后过 3 天重试，之后每 3 天重复一次，直到 notices 关键字指定的时间周期结束。如果无法进行成功的传送，则生成传送失败通知并将邮件返回发件人。

用于通道执行作业的处理池

关键字：pool

通过让通道在同一池中运行，您可以将各种通道配置为能够共享资源。您可能还希望配置其他通道，使其能够在专用于特定通道的池中运行。在每个池中，根据邮件的优先级将邮件自动分成不同的处理队列。池中高优先级的邮件在低优先级的邮件之前处理。（请参见第 324 页的 “基于大小的邮件优先级”。）

通过使用 pool 关键字，可以基于通道在通道中选择创建作业的池。 pool 关键字后面必须跟池名称，当前通道的传送作业将被置于该池名称中。池的名称不能多于 12 个字符。

有关作业控制器的概念和配置的详细信息，请参见第 225 页的 “作业控制器文件”、第 179 页的 “作业控制器”和第 322 页的 “服务作业限制”。

服务作业限制

关键字：maxjobs 和 filesperjob

每次将邮件加入通道队列时，作业控制器均确保有一个运行的作业以传送该邮件。这可能涉及启动一个新作业进程、添加一个线程或只是通知一个作业已经在运行。但是，单个服务作业可能不足以确保所有邮件的及时传送。（有关作业控制器的概念和配置的详细信息，请参见第 225 页的 “作业控制器文件”、第 322 页的 “用于通道执行作业的处理池”和第 179 页的 “作业控制器”。）

对于任何给定安装，都存在一个合理的为传送邮件而启动的进程和线程的最大数量。该最大数量取决于诸如处理器的数量、磁盘的速度以及连接的特性等因素。在 MTA 配置中，可以控制以下内容：

- 为给定通道启动运行的最大进程数 （maxjobs 通道关键字）
- 为一组通道启动运行的最大进程数 （作业控制器配置文件中相关的池部分的 JOB_LIMIT 参数）
- 启动新线程或新进程之前接收的排队邮件的数量 （threaddepth 通道关键字）
- 对于某些通道，将在给定传送程序中运行最大的线程数 （通道选项文件中的 max_client_threads 参数）

为给定通道启动运行的最大进程数是通道中 maxjobs 设置的最小值，也是通道在其中运行的池的 JOB_LIMIT 设置的最小值。

假定需要处理一个邮件。通常作业控制器按照以下方法启动新进程：

- 如果不存在为通道运行的进程，而且未达到池作业限制，则作业控制器将启动新进程。
- 如果通道程序是单线程的，或者已经达到线程限制，并且待办事项增加到超过多个线程 （由 threaddepth 指定），而通道和池作业限制均未达到，则作业控制器将启动新进程。
- 如果通道程序是多线程的，未达到线程限制，而待处理邮件增加到超过多个 threaddepth，则启动新线程。

特定于 SMTP 通道而言，当邮件加入不同主机的队列时，将启动新线程或新进程。因此，对于 SMTP 通道，作业控制器按照以下方法启动新进程。假定需要处理一个邮件，将进行以下操作：

- 如果不存在为 SMTP 通道运行的进程，并且未达到池限制，则作业控制器将启动新进程。
- 如果已经达到线程限制 (MAX_CLIENT_THREADS)，邮件加入未被服务的主机队列，而且通道限制 (maxjobs) 和池作业限制 (JOB_LIMIT) 均未达到，则启动新进程。
- 如果未达到线程限制，邮件加入未被服务的主机队列，则启动新线程。
- 如果未达到线程限制，而加入队列的邮件使该主机的待处理邮件增加到超过多个 threaddepth，则启动新线程。

另请参见第 325 页的 “SMTP 通道线程”。

filesperjob 关键字可用于使 MTA 创建附加服务作业。该关键字使用一个正整数参数，指定必须将多少队列条目 （即文件）发送到关联的通道之后才能创建一个以上的服务作业用以处理队列条目。如果给定的值小于或等于零，则被解释为请求仅加入一个服务作业。不指定关键字等效于指定零。该关键字的效果将被最大化；计算的较大数量为实际创建的服务作业的数量。

filesperjob 关键字按给定值划分实际队列条目 （或文件）的数量。请注意，给定邮件产生的队列条目的数量由许多因素控制，包括但不仅限于关键字 single 和 single_sys 的使用以及邮件列表中标题修改操作的规范。

maxjobs 关键字对于可以同时运行的服务作业的总数设置了上限。此关键字后面必须跟一个整数值，如果计算的服务作业的数量大于该值，则实际只创建 maxjobs 作业。如果未指定 maxjobs，则默认值为 100。通常将 maxjobs 值设置为小于或等于可以在任意服务池或通道使用的池中同时运行的作业的总数。

设置连接事务限制

关键字：transactionlimit

transactionlimit 限制每个连接允许的邮件数量。可以按照以下的方式使用此关键字来阻止攻击者：

攻击者可以通过 SMTP 进行连接并发送大量 RCPT TO 命令以尝试猜出合法电子邮件地址。通过限制事务中允许的无效 RCPT TO 的数量可以阻止这样的攻击。攻击者可能使用多个事务进行应答，但是通过 transactionlimit，您可以限制 SMTP 会话中允许的事务数量。攻击者可以使用多个会话，但是其成本是高昂的。可以使用连接限制以各种方式来限制会话的数量，使其成本在大多数情况下真正变得高昂。

但是，我们也必须付出代价。某些 SMTP 客户机对收件人限制、事务限制或二者的响应相当差。需要对这些客户机设置例外。但是， TCP 通道选项将无条件应用到 SMTP 服务器。解决方案是使用通道关键字和 switchchannel 将有问题的代理路由到限制数量更大的通道。

基于大小的邮件优先级

关键字：urgentblocklimit、 normalblocklimit 和 nonurgentblocklimit

关键字 urgentblocklimit、 normalblocklimit 和 nonurgentblocklimit 可用于指示 MTA 根据邮件大小对邮件的优先级进行降级处理。这些关键字影响作业控制器处理邮件时应用的优先级。

SMTP 通道线程

关键字：threaddepth

多线程 SMTP 客户机将发向不同目标的外发邮件分到不同的线程中。threaddepth 关键字可用于指示多线程 SMTP 客户机在任何一个线程中只处理指定数量的邮件，即使所有邮件都发向同一目标 （因此通常在一个线程中进行处理），也对其使用附加线程。此关键字的默认值为 10。

每当通道的待办事项增加到超过多个 threaddepth 时，作业控制器将试图增加专用于处理在该通道排队的邮件的处理的数量。对于多线程通道，作业控制器建议处理该通道邮件的任意作业启动新线程，或者，如果所有作业都具有允许用于此通道的最大线程数 （tcp_* 通道的选项中的 MAX_CLIENT_THREADS），则启动新进程。对于单线程通道，将启动新进程。请注意，如果已达到通道的作业限制 (maxjobs) 或池的作业限制 (JOB_LIMIT)，作业控制器将不启动新作业。

实质上， threaddepth 控制如何安排主动作业。让我们考虑两种不同的情况：

(1) 正常 （外发） SMTP 通道

(2) 转发到智能主机的 SMTP 通道

作业控制器将按照目标主机对发往特定通道的邮件进行排序，并基于这些目标主机上的待办事项安排作业处理邮件的顺序。

在第一个实例中，将有大量目标主机，而且大部分目标主机的代办事项都比较小。将有大量线程处于运行状态并且一切都运行良好，不过，对于像 aol、 yahoo、 hotmail 这样的通信量非常大的目标主机可能会出现例外。如果使用 128 的线程深度，则当代办事项达到 128 时，您只能将第二个线程传送到 yahoo。这不是一种理想的状况。

在第二个实例中，只有一个目标主机，将多个线程传送到该主机是比较理想的。美中不足的是，默认值 10 可能太小。

当通道连接到的 SMTP 服务器可以处理多个同时连接时，使用 threaddepth 对于在守护程序路由器 TCP/IP 通道 （连接到单个特定 SMTP 服务器的 TCP/IP 通道）中实现多线程可能会尤其有用。

多个地址扩展

关键字：expandlimit、 expandchannel 和 holdlimit

大多数通道支持在每个外来邮件的传输中指定多个收件人地址。在一个邮件中指定多个收件人地址可能会导致邮件传输处理的延迟 （联机延迟）。如果延迟时间太长，则可能出现网络超时，这又会导致重复的邮件提交和其他问题。

MTA 提供了一种特殊的功能，如果为一个邮件指定了超过给定数量的地址，则强制执行延迟 （脱机）处理。邮件处理的延迟可以大幅度减少联机延迟。但是请注意，处理开销是被延迟，而不是被完全避免了。

通过结合使用，例如说，普通的 reprocessing 通道和 expandlimit 关键字，可以激活这一特殊功能。 expandlimit 关键字使用整数参数，该参数指定进行延迟处理之前来自通道的邮件中应被接受的地址数。如果不指定 expandlimit 关键字，则默认值为无穷大。如果值为 0，则对来自通道的所有外来地址强制执行延迟处理。

在本地通道或 reprocessing 通道本身中不应指定 expandlimit 关键字，如果指定，将产生不可预料的结果。

可以使用 expandchannel 关键字指定用以实际执行延迟处理的通道；如果不指定 expandchannel，将默认使用 reprocessing 通道，但是使用其他某个重新处理通道或处理通道对于某些特殊目的会很有用。如果通过 expandchannel 指定了用于延迟处理的通道，则该通道应为重新处理通道或处理通道；指定其他种类的通道可能会导致不可预料的结果。

必须将 reprocessing 通道或用于执行延迟处理的任意其他通道添加到 MTA 配置文件中，以使 expandlimit 关键字生效。如果您的配置是通过 MTA 配置实用程序构建的，那么您应该已经具有重新处理通道。

收件人地址列表非常大通常是主动提供的批量电子邮件的特点。 holdlimit 关键字告诉 MTA，如果进入通道的邮件使收件人超过指定数量，则应该将其标记为 .HELD 邮件，并让其加入 reprocess 通道 （或通过 expandchannel 关键字指定的任意通道）队列。该文件将不被处理，它将在 reprocess 队列中等待 MTA 邮寄主管手动介入。

启用服务转换

关键字：service 和 noservice

service 关键字无条件启用服务转换，不考虑 CHARSET-CONVERSION 条目。如果设置了 noservice 关键字，则必须通过 CHARSET-CONVERSION 为进入该通道的邮件启用服务转换。

配置地址处理

本节说明了涉及地址处理的关键字。其中包括以下各节：

- 第 326 页的 “启用服务转换”
- 第 327 页的 “地址类型和约定”
- 第 329 页的 “解释使用 ! 和 % 的地址”
- 第 329 页的 “在地址中添加路由信息”
- 第 330 页的 “禁用显式路由地址的重写”
- 第 330 页的 “邮件出队后的地址重写”
- 第 331 页的 “指定修正不完整地址时使用的主机名”
- 第 331 页的 “使缺少收件人标题行的邮件合法化”
- 第 332 页的 “删除非法的空收件人标题”
- 第 332 页的 “启用特定于通道的反向数据库使用”
- 第 333 页的 “启用限制的邮箱编码”
- 第 333 页的 “生成 Return-path: 标题行”
- 第 334 页的 “从信封 To: 和 From: 地址设置限制”
- 第 334 页的 “处理地址标题行中的注释”
- 第 335 页的 “处理地址标题行中的个人名称”
- 第 336 页的 “指定别名文件和别名数据库探测”
- 第 336 页的 “子地址处理”
- 第 337 页的 “启用特定于通道的重写规则检查”
- 第 337 页的 “删除源路由”
- 第 337 页的 “必须从别名指定地址”

地址类型和约定

关键字：`822`、 `733`、 `uucp`、 `header_822`、 `header_733` 和 `header_uucp`

这组关键字控制通道支持的地址类型。传输层 （邮件信封）中使用的地址和邮件标题中使用的地址是有区别的。

822 (sourceroute)

源路由信封地址。此通道支持完整的 RFC 822 格式的信封寻址约定 （包含源路由）。也可以使用关键字 `sourceroute`，它是 822 的同义词。如果不指定其他信封地址类型关键字，则此关键字为默认设置。

733 (percents)

百分号信封地址。此通道支持完整的 RFC 822 格式的信封寻址 （源路由除外）；应该使用百分号约定重写源路由。也可以使用关键字 `percents`，它是 733 的同义词。

注 在 SMTP 通道中使用 733 地址约定将导致在 SMTP 信封的传输层地址中继续使用这些约定。这可能违反 RFC 821。请仅在确实必要时才使用 733 地址约定。

uucp (bangstyle)

bang 式样的信封地址。此通道在信封中使用符合 RFC 976 bang 式样地址约定的地址（例如，这是 UUCP 通道）。也可以使用关键字 `bangstyle`，它是 uucp 的同义词。

header_822

源路由标题地址。此通道支持完整的 RFC 822 格式的标题寻址约定 （包含源路由）。如果不指定其他标题地址类型关键字，则此关键字为默认设置。

header_733

百分号标题地址。此通道支持 RFC 822 格式的标题寻址 （源路由除外）；应该使用百分号约定重写源路由。

注 在邮件标题中使用 733 地址约定可能会违反 RFC 822 和 RFC 976。请仅在确保通道连接到无法处理源路由地址的系统时才使用该关键字。

header_uucp

UUCP 或 bang 式样标题地址。不建议使用此关键字。使用此关键字违反 RFC 976。

解释使用！和 % 的地址

关键字：bangoverpercent、 nobangoverpercent 和 percentonly

地址始终依据 RFC 822 和 RFC 976 进行解释。但是，处理上述标准未涉及的某些复合地址时会有歧义。尤其是， A!B%C 格式的地址可以被解释为：

- A 是路由主机， C 是最终目标主机

或

- C 是路由主机， A 是最终目标主机

尽管 RFC 976 表示邮件程序可以使用后一种约定解释地址，但却没有说这种解释是必需的。某些情况下使用前一种解释反而更好。

bangoverpercent 关键字强制执行前一种 A!(B%C) 解释。 nobangoverpercent 关键字强制执行后一种 (A!B)%C 解释。 nobangoverpercent 是默认设置。

注	此关键字不影响对 A!B@C 格式的地址的处理。这些地址将始终被处理为 (A!B)@C。 RFC 822 和 RFC 976 均强制使用这种处理。

percentonly 关键字忽略 bang 路径。如果设置了此关键字，百分号将被解释为路由。

在地址中添加路由信息

关键字：exproute、 noexproute、 improute 和 noimproute

MTA 使用的寻址模式假定所有系统都知道所有其他系统的地址并知道如何到达这些地址。不幸的是，这一理想并非在所有情况下都可行，例如当通道连接到一个或多个不为外界所知的系统 （例如专用 TCP/IP 网络中的内部计算机）时就不可行。该通道中的系统的地址对于站点以外的远程系统来说可能是非法的。如果希望能够回复上述地址，则地址中必须包含源路由，源路由将通知远程系统通过本地计算机路由邮件。然后本地计算机可以 （自动）将邮件路由到上述计算机中。

exproute 关键字 （"explicit routing" 的缩写）告诉 MTA，当通道地址传递到远程系统时，关联的通道要求显式路由。如果在通道中指定了此关键字， MTA 会将包含本地系统名称 （或本地系统的当前别名）的路由信息添加到与该通道匹配的所有标题地址和所有信封 From: 地址。默认设置 noexproute 指定不应该添加路由信息。

EXPROUTE_FORWARD 选项可用于限制 exproute 操作，以反向指向地址。当 MTA 通过无法为自身执行正确路由的通道连接到系统时，将出现另一种情况。在这种情况下，当邮件被发送到与无法胜任路由的系统相连接的通道中时，所有该邮件中使用的与其他通道关联的地址均需要指明路由。

隐式路由和 improute 关键字用于处理这种情况。 MTA 知道，当邮件被发送到标记为 improute 的通道中时，邮件中使用的所有与其他通道匹配的地址都需要路由。默认设置 noimproute 指定不应该将路由信息添加到发出到指定通道的邮件的地址中。IMPROUTE_FORWARD 选项可用于限制对后指地址进行 improute 操作。

关键字 exproute 和 improute 应谨慎使用。它们会使地址变得长而且复杂，并可能破坏其他系统使用的智能路由模式。显式和隐式路由不应与指定的路由混淆。指定的路由用于将来自重写规则的路由信息插入到地址中。此功能由特殊的 A@B@C 重写规则模板激活。

激活指定路由后，它将被应用到标题和信封的所有地址。由于指定路由是被特定的重写规则激活的，因此它们通常独立于当前使用的通道。但显式路由和隐式路由却是基于每个通道进行控制的，插入的路由地址始终是本地系统。

禁用显式路由地址的重写

关键字：routelocal

向通道重写地址时， routelocal 通道关键字使 MTA 尝试让地址中所有显式路由“短路”。显式路由地址 （使用 !、 % 或 @ 字符）将被简化。

在 “内部”通道 （如内部 TCP/IP 通道）中使用此关键字可以简化 SMTP 中继阻止的配置。

请注意，在可能需要显式 % 路由或其他路由的通道中不应该使用此关键字。

邮件出队后的地址重写

关键字：connectalias 和 connectcanonical

将邮件加入通道队列时， MTA 通常重写地址。邮件出队期间，不再执行其他重写操作。当主机名已更改，而通道队列中却仍然存在发送到旧主机名的邮件时，上述做法将导致潜在的问题。

connectalias 关键字通知 MTA 将邮件传送到收件人地址中列出的任意主机。该值为默认值。关键字 connectcanonical 通知 MTA 连接到 MTA 原本应该连接的系统的主机别名。

指定修正不完整地址时使用的主机名

关键字：remotehost、 noremotehost、 defaulthost 和 nodefaulthost

MTA 常收到来自配置错误或不兼容的邮件程序和 SMTP 客户机的不包含域名的地址。在允许进一步传递这类邮件之前， MTA 将尝试使其合法。 MTA 通过在地址中附加域名来达到上述目的 （例如，将 @siroe.com 附加到 mrochek 后面）。

对于缺少域名的信封 To: 地址， MTA 始终假定应该附加本地主机名。但是对于其他地址 （例如 From: 地址），就 MTA SMTP 服务器而言至少有两个合理的域名选择：本地 MTA 主机名和客户机 SMTP 报告的远程主机名。或者在某些情况下，可能还有第三种合理的选择 — 将添加到进入该通道的邮件中的特定域名。现在，前两种选择都可能是正确的，因为两种情况都可能在运行时以一定的频率出现。当处理配置不正确的 SMTP 客户机时，使用远程主机的域名比较合适。当处理轻量远程邮件客户机 （例如使用 SMTP 收发邮件的 POP 或 IMAP 客户机）时，使用本地主机的域名可能比较合适。或者，如果是轻量远程邮件客户机 （例如 POP 或 IMAP 客户机），则客户机具有不属于本地主机的自己的特定域名。那么添加上述不同的特定域名可能会比较合适。 MTA 最好基于每个通道在通道中作选择。

noremotehost 通道关键字指定应该使用本地主机的名称。关键字 noremotehost 是默认设置。

defaulthost 通道关键字用于指定特定的主机名，以将其附加到外来的缺少域名的用户 ID 的地址中。它后面必须跟域名，将使用该域名完成进入通道的地址 （信封 From: 中的地址和标题中的地址）。（就提交通道而言， defaulthost 关键字的第一个参数还影响缺少域名的信封 To: 地址。）可以指定第二个可选域名 （其中至少有一个句点），用来完成信封 To: 地址。 nodefaulthost 是默认设置。

switchchannel 关键字 （如前面的第 313 页的 “外来邮件的备用通道 （切换通道）”一节中所述）可用于将外来 SMTP 连接与特定通道相关联。该功能可用于在通道中对远程邮件客户机进行分组，以便对它们进行适当的处理。或者，您可以部署与标准兼容的远程邮件客户机 （即使多个不兼容的客户机正在使用中），这比尝试解决 MTA 主机中网络范围的问题简单。

使缺少收件人标题行的邮件合法化

关键字：missingrecipientpolicy

RFC 822 (Internet) 邮件需要包含收件人标题行：To:、 Cc: 或 Bcc: 标题行。缺少上述标题行的邮件是非法的。然而，某些损坏的用户代理和邮件程序 （例如，许多老版本的 sendmail）却发送非法邮件。

missingrecipientpolicy 关键字使用整数值，该值指定用于此类邮件的处理方法；如果未明确指定该关键字，则默认值为 1 （传递非法邮件，不进行更改）。

表 12-8 missingrecipientpolicy 的值

值	操作
0	将信封 To: 收件人置于 To: 标题行。
1	传递非法邮件，不进行更该。
2	将信封 To: 收件人置于 To: 标题行。
3	将所有信封 To: 收件人置于一个 Bcc: 。
4	生成一个组构建 （例如 ";") To: 标题行："To: Recipients not specified: ;"
5	生成空的 Bcc: 。
6	拒绝邮件。

请注意，可以使用 MISSING_RECIPIENT_POLICY 选项为此行为设置 MTA 系统默认值。初始 Messaging Server 配置将 MISSING_RECIPIENT_POLICY 设置为 1。

删除非法的空收件人标题

关键字：dropblank 和 nodropblank

在 RFC 822 (Internet) 邮件中，所有 To:、Resent-To:、Cc: 或 Resent-Cc: 标题都需要至少包含一个地址 — 上述标题不能包含空值。然而，某些邮件程序却可能发出这种非法标题。如果在源通道中指定 dropblank 通道关键字，它将使 MTA 删除外来邮件中所有上述非法空标题。

启用特定于通道的反向数据库使用

关键字：reverse 和 noreverse

reverse 关键字通知 MTA，应该使用地址反向数据库或 REVERSE 映射 （如果其中任何一个存在的话）对在通道中排队的邮件的地址进行反向检查并 （如果可能）进行修改。 noreverse 免除对在通道中排队的邮件的地址反向处理。 reverse 关键字是默认设置。有关更多信息，请参阅第 234 页的 “将地址由内部格式转换为公用格式”。

启用限制的邮箱编码

关键字：`restricted` 和 `unrestricted`

某些邮件系统处理 RFC 822 所允许的所有地址时会有困难。尤其常见的例子是基于 sendmail 的带有错误配置文件的邮件程序。用引号引起的本地部分 （或指定的邮箱）是问题的常见根源：

```
"smith, ned"@siroe.com
```

这是引起问题的如此主要的根源，以致于 RFC 1137 制订了解决该问题的方法。基本的处理方法是从地址中删除引号，然后应用转换，将需要引号的字符映射为原子中允许的字符 （有关本文中使用的 “原子”的定义，请参见 RFC 822）。例如，前面的地址将变成：

```
smith#m#_ned@siroe.com
```

`restricted` 通道关键字通知 MTA，通道将连接到要求此编码的邮件系统。然后，当邮件被写入通道时， MTA 对标题和信封地址中用引号引起的部分进行编码。通道中的外来地址将被自动解码。 `unrestricted` 关键字通知 MTA 不执行 RFC 1137 编码和解码。关键字 `unrestricted` 是默认设置。

注 如果与通道连接的系统无法接受用引号引起的本地部分，则应该对该通道应用 `restricted` 关键字。如果通道实际生成用引号引起的本地部分，则不应该对其应用该关键字。（我们认为能够生成这种地址的通道也能够处理这种地址。）

生成 Return-path: 标题行

关键字：`addreturnpath` 和 `noaddreturnpath`

通常，添加 `Return-path:` 标题行是执行最终传送的通道的责任。但是对于某些通道（例如 ims-ms 通道），由 MTA 添加 `Return-path:` 标题比允许通道执行添加操作效率更高。 `addreturnpath` 关键字使 MTA 在邮件在该通道排队时添加 `Return-path:` 标题。

从信封 To: 和 From: 地址设置限制

关键字：receivedfor、 noreceivedfor、 receivedfrom、 noreceivedfrom

receivedfor 关键字指示 MTA，如果邮件只发给一个信封收件人，则将该信封 To: 地址包含在它所构建的 Received: 标题行中。关键字 receivedfor 是默认设置。noreceivedfor 关键字指示 MTA 构建 Received: 标题行，但不包含任何信封地址信息。

receivedfrom 关键字指示 MTA，为外来邮件构建 Received: 标题行时，如果 MTA 由于，例如说，某些类型的邮件列表扩展更改了信封 From: 地址，则在 Received: 标题行中包含原来的信封 From: 地址。 receivedfrom 是默认设置。 noreceivedfrom 关键字指示 MTA 构建 Received: 标题行，但不包含原来的信封 From: 地址。

处理地址标题行中的注释

关键字：commentinc、 commentmap commentomit、 commentstrip、 commenttotal、 sourcecommentinc、 sourcecommentmap、 sourcecommentomit、 sourcecommentstrip 和 sourcecommenttotal

MTA 仅在必要时才解释标题行的内容。但是，必须对所有包含地址的已注册的标题行进行分析，以重写并消除缩写格式的地址，或者将其转换为合法地址。此进程期间，将在重建标题行时提取注释 （括号中的字符串），并可能对其进行修改或将其排除。

使用关键字 commentinc、commentmap、commentomit、commentstrip 和 commenttotal 可以控制此行为。 commentinc 关键字通知 MTA 保留标题行中的注释。这是默认设置。关键字 commentomit 通知 MTA 从寻址标题 （例如， To:、 From: 或 Cc: 标题行）中标题行。

关键字 commenttotal 通知 MTA 从除 Received: 标题行之外的所有标题行中删除所有注释；通常该关键字没有用处，不建议使用。commentstrip 通知 MTA 从所有注释字段中删除所有非原子字符。commentmap 关键字通过 COMMENT_STRINGS 映射表运行注释字符串。

在源通道中，使用关键字 sourcecommentinc、sourcecommentmap、sourcecommentomit、sourcecommentstrip 和 sourcecommenttotal 可以控制此行为。 sourcecommentinc 关键字指示 MTA 保留标题行中的注释。这是默认设置。 sourcecommentomit 关键字指示 MTA 从寻址标题 （例如 To:、 From: 和 Cc: 标题）中删除所有注释。sourcecommenttotal 关键字指示 MTA 从除 Received: 标题行之外的所有标题行中删除所有注释；因此，通常该关键字没有用处，不建议使用。最后，sourcecommentstrip 关键字指示 MTA 从所有注释字段中删除所有非原子字符。sourcecommentmap 关键字通过源通道运行注释字符串。

上述关键字可以应用到所有通道中。

COMMENT_STRINGS 映射表的语法如下：

（comment_text） | *address*

如果条目模板设置了 $Y 标志，则使用指定的文本 （应该用括号括起）替换原来的注释。

处理地址标题行中的个人名称

关键字：personalinc、 personalmap、 personalomit、 personalstrip、 sourcepersonalinc、 sourcepersonalmap、 sourcepersonalomit 和 sourcepersonalstrip

在重写进程期间，必须对所有包含地址的标题行进行分析，以重写并消除缩写格式的地址，或者将其转换为合法地址。在此进程期间，将在重建标题行时提取个人名称 （尖括号分隔的地址前面的字符串），并可以选择对其进行修改或将其排除。

使用关键字 personalinc、personalmap、personalomit 和 personalstrip 可以控制此行为。关键字 personalinc 通知 MTA 保留标题中的个人名称。这是默认设置。关键字 personalomit 通知 MTA 删除所有个人名称。关键字 personalstrip 通知 MTA 从所有个人名称字段中删除所有非原子字符。 personalmap 关键字指示 MTA 通过 PERSONAL_NAMES 映射表运行个人名称。

在源通道中，使用关键字 sourcepersonalinc、 sourcepersonalmap、 sourcepersonalomit 或 sourcepersonalstrip 可以控制此行为。 sourcepersonalinc 关键字指示 MTA 保留标题中的个人名称。这是默认设置。 sourcepersonalomit 关键字指示 MTA 删除所有个人名称。最后，sourcepersonalstrip 指示 MTA 从所有个人名称字段中删除所有非原子字符。 sourcepersonalmap 关键字指示 MTA 通过源通道运行个人名称。

上述关键字可以应用到所有通道中。

PERSONAL_NAMES 映射表探测的语法是：

personal_name | *address*

如果模板设置了 $Y 标志，则用指定的文本替换原来的个人名称。

指定别名文件和别名数据库探测

关键字：aliaslocal

通常只在别名文件和别名数据库中查找被重写到本地通道 （即 UNIX 中的 L 通道）的地址。可以将 aliaslocal 关键字置于通道中，以在别名文件和别名数据库中查找被重写到该通道的地址。然后 ALIAS_DOMAINS 选项将控制所进行的查找探测的确切形式。

子地址处理

关键字：subaddressexact、 subaddressrelaxed 和 subaddresswild

作为子地址概念的背景，本地和 ims-ms 通道对地址本地部分 （邮箱部分）中的 + 字符有各自的特殊解释：在 *name+subaddress@domain* 形式的地址中， MTA 将邮箱中加号后面的部分看作子地址。本地通道将子地址看作附加的装饰性信息，它将邮件实际发送给帐户名，而不考虑子地址； ims-ms 通道将子地址解释为向其传送邮件的文件夹名。

子地址还影响本地通道 （即 UNIX 中的 L 通道）对别名的查找、所有使用 aliaslocal 关键字标记的通道对别名的查找以及目录通道对邮箱的查找。上述查找匹配中对子地址的确切处理方式是可以配置的：将地址与条目进行比较时， MTA 将始终首先检查整个邮箱 （包含子地址）以获得完全匹配；此后 MTA 是否执行其他检查是可以配置的。

subaddressexact 关键字指示 MTA 在条目匹配期间不执行特别的子地址处理；整个邮箱 （包含子地址）与条目匹配时才认为该别名匹配。不执行其他比较 （尤其是，不执行通配符比较或删除子地址后的比较）。 subaddresswild 关键字指示 MTA，对完全匹配 （包含整个子地址）进行查找后，接下来 MTA 应查找名称 +* 格式的条目。 subaddressrelaxed 关键字指示 MTA，对完全匹配以及名称 +* 格式的匹配进行查找后， MTA 应另外检查仅名称部分相同的匹配。使用 subaddressrelaxed 时，以下格式的别名条目将与名称或名称 + 子地址匹配，名称将被转换为新名称，名称 + 子地址将被转换为新名称 + 子地址。 subaddressrelaxed 关键字是默认设置。

```
name:newname+*
```

因此，当使用别名或目录通道，而用户希望接收使用任意子地址的邮件地址时， subaddresswild 关键字或 subaddressrelaxed 关键字会很有用。使用上述关键字后，将无需再为地址中的每个子地址变量分别指定条目。

请注意，上述关键字只对本地通道 （即 UNIX 中的 L 通道）、目录通道或使用 aliaslocal 关键字标记的任意通道有意义。

标准的 Messaging Server 配置通过实际具有 subaddressrelaxed 行为的 L 通道进行中继操作 （未明确指定其他关键字时使用的默认设置）。

启用特定于通道的重写规则检查

关键字：rules 和 norules

rules 关键字告诉 MTA 对该通道强制执行特定于通道的重写规则检查。该值为默认值。 norules 关键字通知 MTA 不对该通道进行检查。这两个关键字通常用于调试，很少在实际应用程序中使用。

删除源路由

关键字：dequeue_removeroute

dequeue_removeroute 关键字在邮件出队时从信封 To: 地址中删除源路由。此关键字当前仅在 tcp-* 通道中得以实现。将邮件传输到不能正确处理源路由的系统中时，此关键字会很有用。

必须从别名指定地址

关键字：viaaliasoptional 和 viaaliasrequired

viaaliasrequired 指定所有与通道匹配的最终收件人地址都必须由别名生成。最终收件人地址是指执行别名扩展 （如果相关）后的匹配。不能将地址作为收件人地址直接传递给 MTA，也就是说，仅将地址重写到通道是不够的。重写到通道后，地址必须通过别名进行扩展，然后才能被认为与通道真正匹配。

viaaliasrequired 关键字可以用于 （例如在本地通道中）阻止任意帐户 （例如 UNIX 系统中的任意本地 Berkeley 邮箱）的传送。

viaaliasoptional 是默认设置，表示不要求与通道匹配的最终收件人地址由别名生成。

配置标题处理

本节说明了涉及标题和信封信息的关键字。其中包括以下各节：

- 第 338 页的 “重写嵌入式标题”
- 第 339 页的 “删除选定的邮件标题行”
- 第 340 页的 “生成 / 删除 X-Envelope-to: 标题行”
- 第 340 页的 “将日期转换为两位数或四位数”
- 第 340 页的 “在日期中指定星期几”
- 第 341 页的 “自动分割长标题行”
- 第 341 页的 “标题对齐和折叠”
- 第 342 页的 “指定标题行最大长度”
- 第 342 页的 “敏感度检查”
- 第 342 页的 “设置标题中的默认语言”

重写嵌入式标题

关键字：noinner 和 inner

仅在必要时才解释标题行内容。但是，由于具有在邮件中嵌入邮件的功能 (message/RFC822)，因此 MIME 邮件可能包含多组邮件标题。 MTA 通常只解释和重写最外面那组邮件标题。但也可以选择通知 MTA 对邮件中的内部标题应用标题重写。

使用关键字 noinner 和 inner 可以控制此行为。关键字 noinner 通知 MTA 不重写内部邮件标题行。这是默认设置。关键字 inner 通知 MTA 对邮件进行分析，并重写内部标题。上述关键字可以应用到所有通道中。

删除选定的邮件标题行

关键字：headertrim、 noheadertrim、 headerread、 noheaderread、 innertrim 和 noinnertrim

MTA 提供了基于每个通道的功能，可以从邮件中剪裁或删除选定的邮件标题行。通过将通道关键字和一至两个关联的标题选项文件结合使用可以实现此功能。 Sun Java System Messaging Server Administration Reference 中的 MTA 一章说明了标题选项文件的格式。

headertrim 关键字指示 MTA，**对原来的邮件标题进行处理之后**，应查看与通道关联的标题选项文件，并对在该目标通道排队的邮件的标题进行相应的剪裁。 noheadertrim 关键字不进行标题剪裁。关键字 noheadertrim 是默认设置。

innertrim 关键字指示 MTA 对内部邮件部分 （即嵌入的 MESSAGE/RFC822 部分）也执行标题剪裁。 noinnertrim 关键字是默认设置，它通知 MTA 不对内部邮件部分执行标题剪裁。

headerread 关键字指示 MTA，**对原来的邮件标题进行处理之前**，查看与通道关联的标题选项文件，并对加入该源通道队列的邮件的标题进行相应的剪裁。请注意，headertrim 标题剪裁是在对邮件进行处理之后应用的，而且是应用于目标通道而不是源通道。noheaderread 关键字不对加入队列的邮件进行标题剪裁。noheaderread 是默认设置。

与关键字 headeromit 和 headerbottom 不同，关键字 headertrim 和 headerread 可以应用到任意通道中。但是请注意，从邮件中删除重要的标题信息可能会导致 MTA 无法正常操作。选择要删除或要对其进行限制的标题时请特别小心。存在该功能是因为在极少的某些情况下必须删除或限制选定的标题行。

注意 从邮件中删除标题信息可能会导致 MTA 无法正常操作。选择要删除或要对其进行限制的标题时请小心。提供这些关键字是因为在极少的某些情况下必须删除或限制选定的标题行。对任何标题行进行剪裁或删除之前，您必须了解该标题行的用途，并考虑删除操作可能带来的后果。

用于关键字 headertrim 和 innertrim 的标题选项文件的名称格式为 *channel*_headers.opt，其中 channel 是标题选项文件与之关联的通道的名称。与之相仿，用于 headerread 关键字的标题选项文件的名称格式为 channel_read_headers.opt。上述文件存储在 MTA 配置目录 *instance_root*/imta/config/ 中。

生成 / 删除 X-Envelope-to: 标题行

关键字：x_env_to 和 nox_env_to

关键字 x_env_to 和 nox_env_to 控制在特定通道排队的邮件副本中的 X-Envelope-to 标题行的生成和取消。在使用 single 关键字标记的通道中， x_env_to 关键字启用上述标题行的生成，而 nox_env_to 则从加入队列的邮件中删除上述标题。 nox_env_to 是默认设置。

x_env_to 关键字还需要 single 关键字才能生效。

将日期转换为两位数或四位数

关键字：datefour 和 datetwo

原来的 RFC 822 规范要求邮件标题中日期字段的年份必须是两位数。后来 RFC 1123 将其更改为四位数。但是某些旧邮件系统无法容纳四位数日期。此外，某些新邮件系统不再允许两位数日期。

注 无法同时处理这两种格式的系统将遇到标准相互违背的问题。

关键字 datefour 和 datetwo 控制 MTA 对邮件标题日期中年份字段的处理。关键字 datefour 是默认设置，它指示 MTA 将所有年份字段扩展为四位数。对小于 50 的两位数日期添加 2000，对大于 50 的值则添加 1900。

注意 关键字 datetwo 指示 MTA 删除四位数日期中的前两位数。此功能是为了与要求两位数日期的不兼容的邮件系统兼容；不得用于其他用途。

在日期中指定星期几

关键字：dayofweek 和 nodayofweek

RFC 822 规范允许在邮件标题中日期字段的开头指定星期几。但是某些系统不能容纳星期几的信息。这使某些系统不愿包含此信息，尽管在标题中使用这些信息很有用。

关键字 dayofweek 和 nodayofweek 控制 MTA 对星期几信息的处理。关键字 dayofweek 是默认设置，它指示 MTA 保留所有星期几信息，如果缺少此信息，则将其添加到日期和时间标题中。

注意 关键字 nodayofweek 指示 MTA 删除日期和时间标题中开头的星期几信息。此功能是为了与不能正确处理此信息的不兼容的邮件系统兼容；不得用于其他用途。

自动分割长标题行

关键字：maxheaderaddrs 和 maxheaderchars

某些邮件传输 （尤其是某些 sendmail 实现）不能正确处理长标题行。通常这不仅会导致标题行损坏，而且会导致错误的邮件拒绝。尽管这一现象严重违背标准，却是个常见的问题。

MTA 提供了基于每个通道的功能，可以将长标题行分割 （断开）为多个独立的标题行。 maxheaderaddrs 关键字控制一行中可以显示的地址的数量。 maxheaderchars 关键字控制一行中可以显示的字符的数量。这两个关键字都要求一个整数参数，用以指定关联的限制。默认情况下，不对标题行的长度和可以显示的地址数实施任何限制。

标题对齐和折叠

关键字：headerlabelalign 和 headerlinelength

headerlabelalign 关键字控制加入此通道队列的邮件标题的对齐点，它使用整数参数。对齐点是指标题内容对齐的边界。例如，对齐点为 10 的实例标题行外观如下：

```
To:       joe@siroe.com
From:     mary@siroe.com
Subject:  Alignment test
```

默认的 headerlabelalign 为 0，表示不对标题进行对齐。 headerlinelength 关键字控制加入此通道队列的邮件标题行的长度。将依据 RFC 822 折叠规则对大于该长度的标题行进行折叠。

上述关键字只控制邮件队列中邮件标题的格式，标题的实际显示通常由用户代理控制。此外，通过 Internet 传输标题时，将对其进行例行的重新格式化处理，因此即使将这些关键字与简单用户代理一起使用，如果用户代理不对邮件标题进行重新格式化的，则可能也没有可见的效果。

指定标题行最大长度

关键字：maxprocchars

处理包含许多地址的长标题行会消耗大量系统资源。maxprocchars 关键字用于指定 MTA 能够处理和重写的最大长度的标题行。标题超过此长度的邮件将仍然被接受和传送，唯一的区别在于将不以任何方式重写长标题行。此关键字需要整数参数。默认设置为处理任意长度的标题。

敏感度检查

关键字：sensitivitynormal、sensitivitypersonal 和 sensitivityprivate sensitivitycompanyconfidential

敏感度检查关键字设置通道可以接受的邮件敏感度的上限。sensitivitycompanyconfidential 是默认设置；任意敏感度的邮件都可以通过。没有 Sensitivity: 标题的邮件被认为是正常邮件，即敏感度最低的邮件。如果邮件的敏感度高于上述关键字的指定，则当其排入通道时将被拒绝，并显示错误消息：

```
message too sensitive for one or more paths used
```

请注意， MTA 进行此类敏感度检时以每个邮件为级别而不是以每个收件人为级别：如果某个收件人的目标通道未能通过敏感度检查，则所有收件人的邮件都将退回，而不仅是与敏感通道关联的收件人。

设置标题中的默认语言

关键字：language

经过编码的标题内容可以显示为特定语言。language 关键字指定默认语言。

附件和 MIME 处理

本节说明了涉及附件和 MIME 处理的关键字。其中包括以下各节：

- 第 343 页的 “忽略 Encoding: 标题行”
- 第 343 页的 “Message/Partial 邮件的自动片段整理”
- 第 344 页的 “大型邮件的自动分段”
- 第 345 页的 “实施邮件行长度限制”

忽略 Encoding: 标题行

关键字：ignoreencoding 和 interpretencoding

MTA 可以使用 Yes CHARSET-CONVERSION 将各种非标准邮件格式转换为 MIME。尤其是， RFC 1154 格式使用非标准 Encoding: 标题行。但是某些网关在此标题行中发出不正确信息，导致有时需要忽略此标题行。 ignoreencoding 关键字指示 MTA 忽略所有 Encoding: 标题行。

注	除非 MTA 已启用 CHARSET-CONVERSION，否则任何情况下都将忽略此标题。 interpretencoding 关键字指示 MTA 注意所有 Encoding: 标题行 （如果配置为执行此操作），这是默认设置。

Message/Partial 邮件的自动片段整理

关键字：defragment 和 nodefragment

MIME 标准提供了 message/partial 内容类型，用于将邮件分成较小的部分。当邮件必须在具有大小限制的网络中传输，或者在不可靠的网络中传输时，此功能会很有用。在后一种情况下，邮件分段可以提供某种形式的 “检查点”，当邮件传输期间出现网络故障时可以减少随后的复制工作。每一部分中都将包含信息，以便邮件到达目的地后可以自动重新组合邮件。

defragment 通道关键字和片段整理通道提供了在 MTA 中重新组合邮件的方法。当通道被标记为 defragment 时，在通道排队的所有部分邮件将被置于片段整理通道队列中。所有部分都到达之后，将重新组合邮件并进行发送。 nodefragment 禁用此特殊处理功能。关键字 nodefragment 是默认设置。

片段整理通道保留时间

在片段整理通道队列中将邮件仅保留有限时间。如果发送第一个未传送通知之前时间已过去一半，将发送邮件的各个部分，不进行重新组合。选择此时间值排除了为片段整理通道队列中的邮件发送未传送通知的可能性。

通道关键字 notices 将控制发送未传送通知之前所经过的时间，因此也控制着邮件在分块发送之前被保留的时间。将通道关键字 notices 的值设置为希望保留邮件以进行可能的片段整理的时间的两倍。例如， notices 的值为 4 可以使邮件片段保留两天：

```
defragment notices 4
DEFRAGMENT-DAEMON
```

大型邮件的自动分段

关键字：maxblocks 和 maxlines

某些电子邮件系统或网络传输无法处理超过特定大小限制的邮件。MTA 基于各个通道提供了实施此类限制的功能。大于所设置的限制的邮件将被自动分割 （分段）成多个较小的邮件。用于这种分段的内容类型为 message/partial，并添加唯一的 ID 参数，以便同一邮件的不同部分可以彼此关联，并在可能的情况下由接收邮件程序自动重新组合。

maxblocks 和 maxlines 关键字用于实施大小限制，超过此限制时将激活自动分段功能。这两个关键字后面都必须跟一个整数值。关键字 maxblocks 指定邮件中允许的最大块数。 MTA 块通常为 1024 字节，可以使用 MTA 选项文件中的 BLOCK_SIZE 选项对其进行更改。关键字 maxlines 指定邮件中允许的最大行数。如果必要，可以同时实施上述两个限制。

某种程度上，邮件标题也包含在邮件大小中。由于不能将邮件标题分割成多个邮件，但是标题本身有可能超过指定的大小限制，因此使用一种相当复杂的机制来解释邮件标题大小。该逻辑由 MTA 选项文件中的 MAX_HEADER_BLOCK_USE 和 MAX_HEADER_LINE_USE 选项控制。

MAX_HEADER_BLOCK_USE 用于指定 0 到 1 之间的实数。默认值为 0.5。在邮件可以使用的总块数 （由 maxblocks 关键字指定）中，邮件标题可以占用该比例的块数。如果邮件标题大于该值， MTA 将以 MAX_HEADER_BLOCK_USE 和 maxblocks 的乘积作为 * MAX_HEADER_BLOCK_USE 标题的大小 （标题大小取实际标题大小和 maxblocks 中较小的值）。

例如，如果 maxblocks 为 10， MAX_HEADER_BLOCK_USE 为默认值 0.5，则所有大于 5 个块的邮件标题将按 5 个块的标题来处理，如果邮件大小等于或小于 5 个块，则不对其进行分段。如果值为 0，将不对标题做任何邮件大小限制方面的处理。

如果值为 1，则标题可以使用所有可用大小。每个分段将始终至少包含一个邮件行，无论这样做是否导致超过大小限制。MAX_HEADER_LINE_USE 与 maxlines 关键字结合使用的方式与上述相似。

实施邮件行长度限制

关键字：linelength

SMTP 规范允许文本行最多包含 1000 字节。但是，某些传输对行的长度可能会实施更为严格的限制。linelength 关键字提供了基于各个通道的机制，用于限制允许的最大邮件行长度。如果在给定通道排队的邮件的行长于为该通道指定的限制，则对邮件进行自动编码。

MTA 中可用的各种编码方式均将行的长度降到少于 80 个字符。编码后可以应用适当的解码过滤器来恢复原来的邮件。

注	编码只能将行的长度降低到少于 80 个字符。将行的长度值指定为小于 80 可能不会实际生成长度符合该限制的行。

linelength 关键字使数据编码执行 “软”自动换行以用于传输。通常在接收端对编码进行解码，以便恢复原来的 “长”行。有关 “硬”换行的信息，请参见 CHARSET-CONVERSION 中的 "Record, text"。

对邮件、配额、收件人和验证尝试次数的限制

本节说明了设置邮件大小限制、用户配额和权限的关键字。其中包括以下各节：

- 第 346 页的 “对不成功验证尝试的次数的限制”
- 第 346 页的 “指定绝对邮件大小限制”
- 第 347 页的 “重新定向超过大小限制或收件人限制的邮件。”
- 第 348 页的 “处理对超过配额用户的邮件传送”
- 第 349 页的 “处理包含超过 1000 个字符的行的 SMTP 邮件”
- 第 349 页的 “控制通用内容类型参数、文件名内容类型参数和内容处理参数的长度”
- 第 349 页的 “对邮件收件人进行限制”

- 第 350 页的 “限制标题大小”

对不成功验证尝试的次数的限制

关键字：disconnectbadauthlimit

断开会话连接之前，此关键字可以用于对允许在会话中进行的不成功验证尝试的次数进行限制。此选项的默认值为 3。

指定绝对邮件大小限制

关键字：blocklimit、 noblocklimit、 linelimit、 nolinelimit 和 sourceblocklimit

尽管分段功能可以自动将邮件分成较小的部分，但某些情况下应该拒绝大于某个出于管理目的定义的限制的邮件 （例如，为了避免服务拒绝攻击）。

关键字 blocklimit、 linelimit 和 sourceblocklimit 用于实施绝对大小限制。上述所有关键字后面都必须跟一个整数值。

关键字 blocklimit 指定邮件中允许的最大块数。 MTA 拒绝将块数大于该值的邮件在通道排队的尝试。 MTA 块通常为 1024 字节，可以使用 MTA 选项文件中的 BLOCK_SIZE 选项对其进行更改。

关键字 sourceblocklimit 指定外来邮件中允许的最大块数。MTA 拒绝向通道提交块数大于该值的邮件的尝试。也就是说， blocklimit 应用于目标通道，而 sourceblocklimit 应用于源通道。MTA 块通常为 1024 字节，可以使用 MTA 选项文件中的 BLOCK_SIZE 选项对其进行更改。

也可以根据每个发件人来指定源块限制，方法是：使用 MTA 选项 LDAP_SOURCEBLOCKLIMIT 指定用户 LDAP 属性并将此属性添加到发件人 LDAP 条目。还可以基于发件人域来支持源块限制。用 MTA 选项 LDAP_DOMAIN_ATTR_SOURCEBLOCKLIMIT 指定域 LDAP 属性，并将此属性添加到发件人的域 LDAP 条目。这些值都没有默认值。

关键字 linelimit 指定邮件中允许的最大行数。 MTA 拒绝将行数大于该值的邮件在通道排队的尝试。如果必要，可以同时实施关键字 blocklimit 和 linelimit。

MTA 选项 LINE_LIMIT 和 BLOCK_LIMIT 可用于在所有通道中实施相似的限制。这些限制的优点是可以应用于所有通道。因此， MTA 服务器可以在获取邮件收件人信息之前使邮件客户机了解这些限制。这就简化了某些协议中邮件拒绝的进程。

通道关键字 nolinelimit 和 noblocklimit 是默认设置，表示除了通过 MTA 选项 LINE_LIMIT 或 BLOCK_LIMIT 实施的全局限制外，不实施任何限制。

重新定向超过大小限制或收件人限制的邮件。

关键字：alternatechannel、 alternateblocklimit、 alternatelinelimit 和 alternaterecipientlimit

MTA 可以将超过指定的收件人数量限制、邮件大小限制或邮件行数限制的邮件重新定向到备用目标通道。通过设置以下通道关键字可以实现此功能：alternatechannel、 alternateblocklimit、 alternatelinelimit 和 alternaterecipientlimit。可以将上述关键字置于任意目标通道中。alternatechannel 关键字使用一个参数，指定要使用的备用通道的名称。其他每个关键字都接受整数参数，指定一个相应的阈值。超过上述任意阈值的邮件将被加入备用通道 （而不是原来的目标通道）队列中。

在以下的通道块示例中，超过 5000 块的大型邮件本来应该通过 tcp_local 通道进入 Internet，现在却通过 tcp_big 通道进入 Internet：

```
tcp_local smtp ... rest of keywords ...   alternatechannel tcp_big
alternateblocklimit 5
tcp-daemon


tcp_big smtp ...rest of keywords...
tcp-big-daemon
```

以下示例说明了可以如何使用 alternate* 通道关键字：

- 如果要延迟传送大型邮件或在非高峰时间传送大型邮件，您可以控制 alternatechannel （例如 tcp_big）的运行时间。

  一种方法是使用 imsimta qm 实用程序的 STOP channel_name 和 START channel_name 命令，您可以通过自己的自定义周期性作业 （由作业控制器运行）或通过 cron 作业定期执行这些命令。

- 如果要让作业控制器处理大型邮件或自身的池中有很多收件人的邮件，您也可以使用 alternatechannel。

  您可以将小型邮件或收件人较少的邮件与大型邮件或有很多收件人的邮件分开，因为远程 SMTP 服务器处理和接收后者将花费较长时间；您可能不愿意让大型邮件延迟小型邮件的传送。

  请注意，大多数配置中都可以接受作业控制器的常规邮件调度以及将邮件指定到线程和进程。

- 如果要为大型邮件或有很多收件人的邮件设置特殊的 TCP/IP 通道超时值，则可以使用 alternatechannel。

  尤其是，如果要将邮件发送给远程主机，则设置特殊的 TCP/IP 通道超时值会很有用，因为远程主机接收大型邮件或有很多收件人的邮件会花费大量时间。

  请注意，对于大多数配置，默认的自动超时调整应该已经足够。至多您可能希望对默认值进行调整，不使用某个特殊通道。有关详细信息，请参见 Messaging Server Reference Manual 中的通道选项 STATUS_DATA_RECV_PER_ADDR_TIME 和 STATUS_DATA_RECV_PER_BLOCK_TIME。

- 如果要对特别大的邮件进行特殊的 MIME 邮件分段处理，则可以将通道关键字 alternatechannel 和 alternateblocklimit 与 maxblocks 通道关键字一起使用。

  一般情况下，如果要对超过指定大小的邮件进行分段，您应该将所需的 maxblocks 大小置于常规的外发 TCP/IP 通道中。通常 maxblocks 通道关键字既是执行分段的阈值，又是分段的大小。

  但是，如果要触发较大的阈值，并使实际分段较小，则可以在外发 TCP/IP 通道中使用 alternatechannel 和 alternateblocklimit。然后可以在备用通道中使用 maxblock 大小，对超过特定大小的邮件进行分段。

- 可以将 alternatechannel 与特殊的过滤功能结合使用。例如，可能需要对有很多收件人的邮件的内容进行更为仔细的检查，以防它是垃圾邮件。您有可能希望基于外发通道进行不同的过滤 （请参见 Sun Java System Messaging Server Administration Reference 中的 destinationfilter 通道关键字）。

  如果通过转换通道执行相对资源密集的扫描 （例如病毒过滤），非常的大邮件可能会有资源问题。您可能希望使用备用转换通道。或者，您可能希望基于外发通道在常规转换通道中执行特殊的转换过程。

- 如果希望大型外发邮件离开其自己的通道，则可以使用 alternatechannel，以便在分析 mail.log* 文件时或在计数器显示中突出它们。

  而且，如果试图对传送统计进行仔细分析，则在大型邮件自己的通道内对其进行处理会很有用。这是因为发送给远程 SMTP 主机的大型邮件或有很多收件人的邮件可能会花费较长时间才能完成处理，因此为大型邮件创建的传送统计不同于一般邮件。

处理对超过配额用户的邮件传送

关键字：holdexquota 和 noexquota

noexquota 和 holdexquota 关键字控制发送给 Berkeley 邮箱用户 (UNIX) 的邮件的处理，即传送到 uid 本地通道且超过其磁盘配额的用户。

noexquota 告诉 MTA 将发送给超过配额用户的邮件返回邮件的发件人。holdexquota 告诉 MTA 保留发送给超过配额用户的邮件，该邮件将保留在 MTA 队列中，直到可以被传送，或邮件超时并由邮件返回作业返回给发件人。

处理包含超过 1000 个字符的行的 SMTP 邮件

关键字：rejectsmtplonglines、 wrapsmtplonglines 和 truncatesmtplonglines

rejectsmtplonglines 添加拒收邮件选项，拒绝包含超过 1000 个字符 （包括 CRLF）的行 （这在 SMTP 中是允许的）的邮件。此区域中的其他选项包括 wrapsmtplonglines （将过长的行换行）和默认的 truncatesmtplonglines （截断过长的行）。这两个关键字均必须应用到用于提交的初始通道 （例如 tcp_local）。它不会影响后续切换到的任何通道。

控制通用内容类型参数、文件名内容类型参数和内容处理参数的长度

关键字：parameterlengthlimit 和 nameparameterlengthlimit

parameterlengthlimit 控制通用内容类型和内容处理参数的截断点。默认值为 1024。nameparameterlengthlimit 控制名称内容类型参数和文件名内容处理参数的截断点。默认值为 128。请注意，除非正在对邮件进行 MIME 处理，否则将仅处理最外层邮件标题。可以用各种方法启用 MIME 处理，包括 （但不限于） inner 关键字或字符集转换的使用。

对邮件收件人进行限制

关键字：recipientlimit 和 recipientcutoff

recipientlimit 指定邮件可接受的收件人地址总数。recipientcutoff 将提交给 MTA 的收件人总数与指定值相比较。如果超过限制值，则不会接受邮件进行传送。两个关键字均接受整数参数。如果未指定相应的通道关键字，则两者的默认值均为无穷大。

也可以针对发件人或发件人域设置收件人限制。可通过使用相应的 MTA 选项指定用户或域 LDAP 属性来完成此操作：LDAP_RECIPIENTLIMIT、 LDAP_RECIPIENTCUTOFF、LDAP_DOMAIN_ATTR_RECIPIENTLIMIT、 LDAP_DOMAIN_ATTR_RECIPIENTCUTOFF 以及将属性添加到发件人的用户条目或域条目。

限制标题大小

关键字：headerlimit

对主 （最外层）邮件标题的最大值强加限制。当主邮件标题达到限制时将被截断并且不会出现提示。如果已设置全局 MTA 选项 (HEADER_LIMIT)，该选项将覆盖此通道级别限制。默认值为没有限制。

MTA 队列中的文件创建

本节说明了允许通过指定 MTA 队列中的文件创建来控制磁盘资源的关键字。其中包括以下各节：

- 第 350 页的 “控制邮件中多个地址的处理方式”
- 第 351 页的 “将通道邮件队列分布到多个子目录中”

控制邮件中多个地址的处理方式

关键字：multiple、 addrsperfile、 single 和 single_sys

MTA 允许每个排队的邮件中出现多个目标地址。某些通道程序可能只能处理带有一个收件人的邮件、或带有有限数量的收件人的邮件、或每个邮件副本带有一个目标系统的邮件。例如， SMTP 通道主程序在给定的事务中只创建与一个远程主机的连接，因此只能处理到该主机的地址 （尽管通常将一个通道用于所有 SMTP 通信）。

另一个示例是某些 SMTP 服务器可能会对一次能够处理的收件人数量施加限制，它们可能无法处理这类错误。

关键字 multiple、addrsperfile、single 和 single_sys 可以用于控制对于多个地址的处理方式。关键字 single 表示应该为通道中的每个目标地址分别创建一个邮件副本。关键字 single_sys 为使用的每个目标系统创建一个邮件副本。关键字 multiple 是默认设置，它为整个通道创建一个邮件副本。

注	不管使用哪个关键字，至少为邮件在其排队的每个通道创建每个邮件的一个副本。

addrsperfile 关键字用于限制可与通道队列中一个邮件关联的最大收件人数量，从而限制了一次操作中处理的收件人数量。该关键字要求一个整数参数，该参数指定邮件文件中允许的最大收件人地址数量；如果收件人地址达到该数量，则 MTA 自动创建其他邮件文件来容纳它们。（默认的 multiple 关键字通常不对邮件文件中的收件人数量实施限制，但是 SMTP 通道的默认值为 99。）

将通道邮件队列分布到多个子目录中

关键字：subdirs

默认情况下，在通道排队的所有邮件都作为文件存储在目录 /imta/queue/*channel-name* 中，其中 *channel-name* 为通道的名称。处理大量邮件的通道 （例如 TCP/IP 通道）倾向于建立一个很大的等待处理的邮件文件的存储，但是如果将这些邮件文件分布到多个子目录中，则通道将可以获取更好的文件系统性能。 subdirs 通道关键字提供了以下功能：它后面应该跟一个整数，指定将在其中分布通道邮件的子目录的数量。例如：

```
tcp_local single_sys smtp subdirs 10
```

设置会话限制

关键字：disconnectbadcommandlimit、 disconnectrecipientlimit、 disconnectrejectlimit 和 disconnecttransactionlimit

四个新通道关键字提供当检测到一定数量的错误后使 SMTP 服务器从客户机断开连接的功能。

disconnectrecipientlimit — 限制会话收件人的数量。

disconnectrejectlimit — 限制被拒绝的收件人的数量。

disconnecttransactionlimit — 限制事务的数量。

disconnectbadcommandlimit — 限制错误命令的数量。

这些均属于会话限制。除 disconnectbadcommandlimit 外，发出 MAIL FROM 或 RSET 命令后，将检查所有这些限制。如果其中任何一个超过限制，服务器将发出 4xy 错误并断开连接。错误命令限制仅在发出错误命令时进行检查方面不同。

配置记录和调试

本节说明了记录和调试关键字。

- 第 352 页的 “记录关键字”
- 第 352 页的 “调试关键字”
- 第 353 页的 “设置 Loopcheck”

记录关键字

关键字：logging、 nologging 和 logheader

MTA 提供了记录每个入队和出队的邮件的功能。关键字 logging 和 nologging 基于每个通道控制对邮件的记录。默认情况下，初始配置打开所有通道的记录功能。通过在通道定义中使用 nologging 关键字进行替换，您可以禁用特定通道的记录功能。

logheader 基于通道替换 LOG_HEADER MTA 选项。值 0 （默认值）将禁用邮件标题日志。有关更多信息，请参见 Sun Java System Messaging Server Administration Reference。

有关日志记录的更多信息，请参见第 21 章 “管理日志记录”。

调试关键字

关键字：master_debug、 slave_debug、 nomaster_debug 和 noslave_debug

某些通道程序包含可选代码，可通过生成附加诊断输出来帮助调试。可以使用两个通道关键字，以便可以为每个通道都生成这种调试输出。它们是 master_debug 和 slave_debug，前者启用主程序中的调试输出，后者启用从程序中的调试输出。默认情况下禁用这两种类型的调试输出，相当于 nomaster_debug 和 noslave_debug。

如果激活调试输出，将生成与通道程序关联的日志文件。日志文件的位置因程序不同而不同。日志文件通常保存在日志目录中。主程序的日志文件名称格式通常为 *x*_master.log，其中 *x* 是通道名。从程序的日志文件名称格式通常为 *x*_slave.log。

在 UNIX 系统中，如果为 l 通道启用了 master_debug 和 slave_debug，则用户将在包含 MTA 调试信息的当前目录中收到 imta_sendmail.log-*uniqueid* 文件 （如果具有对该目录的写权限，否则调试输出进入 stdout）。

设置 Loopcheck

关键字：loopcheck 和 noloopcheck

loopcheck 关键字在 SMTP EHLO 响应标题中放入字符串，以便 MTA 检查它是否在与自身通信。设置 loopcheck 后， SMTP 服务器将公布 XLOOP 扩展。

与支持 XLOOP 的 SMTP 服务器通信时， MTA 的 SMTP 客户机将公布的字符串与其 MTA 值进行比较，并立即返回信息，说明客户机实际上是否在与 SMTP 服务器通信。

其他关键字

本节说明了其他关键字。其中包括以下各节：

- 第 354 页的 “通道操作类型”
- 第 354 页的 “Pipe 通道”
- 第 354 页的 “指定邮箱过滤器文件位置”
- 第 355 页的 “垃圾邮件过滤器关键字”
- 第 355 页的 “地址验证之后扩展之前的路由”
- 第 358 页的 “NO-SOLICIT SMTP 扩展支持”
- 第 359 页的 “对错误 RCPT TO: 地址设置限制”

进程通道覆盖

关键字：notificationchannel 和 dispositionchannel

这些关键字将进程通道分别替换为用于初始队列传送状态通知 (DSN) 和邮件处理通知 (MDN) 的位置。如果已命名的通道不存在， Messaging Server 将恢复使用进程通道。

notificationchannel 将进程通道替换为用于初始队列传送状态通知 (DSN) 的位置。如果已命名的通道不存在， Messaging Server 将恢复使用进程通道。

dispositionchannel 将进程通道替换为用于初始队列邮件处理通知 (MDN) 的位置。如果已命名的通道不存在， Messaging Server 将恢复使用进程通道。

通道操作类型

关键字：submit

Messaging Server 支持 RFC 2476 的邮件提交协议。submit 关键字可用于将通道标记为仅用来提交的通道。通常此功能主要在 TCP/IP 通道 （例如专用于提交邮件的特殊端口上运行的 SMTP 服务器）中有用； RFC 2476 创建了 587 端口用于此类邮件提交。

Pipe 通道

关键字：user

user 关键字用于 pipe 通道中，指明通道将在其下运行的用户名称。

请注意， user 参数通常必须为小写，但如果是引用的参数，则保持原来的大小写状态。

指定邮箱过滤器文件位置

关键字：filter、nofilter、channelfilter、nochannelfilter、destinationfilter nodestinationfilter、sourcefilter、nosourcefilter、fileinto 和 nofileinto

filter 关键字可以用来在本地和 ims-ms 通道中指定用于该通道的用户过滤器文件的位置。它使用一个必需的 URL 参数，该参数说明过滤器文件的位置。 nofilter 是默认设置，表示不为通道启用用户邮箱过滤器。

sourcefilter 和 destinationfilter 关键字可用于一般 MTA 通道中，分别指定对外来邮件和外发邮件应用的通道级别的过滤器。这些关键字使用必需的 URL 参数，说明通道过滤器文件的位置。 nosourcefilter 和 nodestinationfilter 是默认设置，表示不为通道的任意方向启用通道邮箱过滤器。

已作废的 channelfilter 和 nochannelfilter 关键字分别是 destinationfilter 和 nodestinationfilter 的同义词。

fileinto 关键字 （当前仅支持用于 ims-ms 和 LMTP 通道）指定应用邮箱过滤器 fileinto 运算符时更改地址的方式。对于 ims-ms 通道，通常的用法为：

```
fileinto $U+$S@$D
```

以上命令指定应该将文件夹名称作为子地址插入原来的地址，用以替换原来存在的任意子地址。

对于 LMTP 通道，通常的用法为：

```
fileinto @$4O:$U+$S@$D
```

其中 $4O 包含 4 和字母 O，而不是零。

垃圾邮件过滤器关键字

关键字：destinationspamfilterXoptin 和 sourcespamfilterXoptin

destinationspamfilterXoptin 指定所有发送到此通道的邮件均通过过滤软件 X （过滤软件 X 由 option.dat 中的 spamfilterX_library 定义）运行。关键字后面跟过滤器参数，可用的参数取决于过滤程序。

sourcespamfilterXoptin 指定所有源自此通道的邮件均通过过滤软件 X （定义过滤软件 X 由 option.dat 中的 spamfilterX_library 定义）运行。关键字后面跟系统范围内的默认参数，可用的参数取决于过滤程序。如果 switchchannel 有效，请将此关键字放置在 switched-to 通道上。

有关如何使用这些关键字的完整的详细信息，请参见第 399 页的 “指定通道级别的过滤”。

地址验证之后扩展之前的路由

关键字：aliasdetourhost

aliasdetourhost 允许进行托管用户的 mailHost 属性值的特定于源通道的替换。尤其是， aliasdetourhost 常用于在将本地 （此系统上托管的）用户的邮件路由到单独的主机以进行某种处理时实现 “绕道而行”。邮件可以在原始主机上进行验证 （邮件的地址是合法本地地址），绕行到处理主机，然后再返回原始主机进行扩展和传送。

aliasdetourhost 允许更好地配置和使用通道及第三方过滤主机的 “中间过滤”排序。除了使用备用转换通道外，通常还使用 aliasdetourhost。 aliasdetourhost 用于影响本地 （系统上托管的）用户的路由选择，而备用转换通道用于影响远程收件人的路由选择。由。

aliasdetourhost 的参数是主机或域名，或者是主机 / 域指定。（请注意，重写规则可以处理主机名、 IP 实际地址和通道标记，这些均被默认为主机名。）如果在源通道上指定关键字，此关键字将导致储存在 LDAP 中的地址别名扩展在邮件主机信息检查点之前停止 （处理转换标记信息之后）。邮件将在该点被发送到 aliasdetourhost 值，并在别名扩展之前、地址验证之后成功地完成地址处理。

以下示例说明了可以在何处使用 aliasdetourhost 来避免各种与转换通道过滤相关的问题：假定使用前端 MTA 和后端邮件存储设置系统。用户将其传送选项设置为 forward 和 mailbox。MTA 将备用转换通道用于反病毒 / 垃圾邮件系统。邮件到达此用户时， MTA 别名将扩展并生成两个收件人 （一个本地收件人，一个远程收件人）。远程收件人的副本将直接被发送。另一方面，本地收件人的副本将进入转换通道进行扫描，然后返回。然后，将再次应用别名扩展生成远程收件人的第二个副本，本地收件人的副本将正常传送。得到的结果：两个副本发送到远程收件人，一个副本发送到本地收件人。

将不把备用转换通道用于本地托管用户 （但对于其他收件人，可能仍将使用备用转换通道），使用 aliasdetourhost 的通道可以执行以下操作：

- 接受邮件。
- 将邮件路由到外部垃圾邮件 / 病毒过滤器
- 为地址扩展和传送重新接受邮件。

示例 1：

假定从 MTA 的独立主机上运行第三方扫描程序。以下示例允许使用用户条目转发而不必创建虚假复制，并在接受邮件之前保留执行收件人地址验证的功能。

1. 创建新通道 tcp_scanner。

   在该通道上放置 daemon 关键字，以指向过滤系统。将 enqueue_removeroute 也添加到此通道。在 imta.cnf 中， tcp_scanner 通道与此通道类似：

   ```
   tcp_scanner smtp mx single_sys subdirs 20 noreverse maxjobs 7 pool
   SMTP_POOL daemon my_a-v_filter.siroe.com enqueue_removeroute
   tcp_scanner-daemon
   ```

2. 在要扫描的所有外来源 tcp 通道 （可能包括 tcp_local, tcp_submit、tcp_intranet 和 tcp_auth）上，将 aliasDetourHost tcp_scanner-daemon 添加到 tcp_local。以下显示了一个 tcp_local 和 tcp_submit 的示例。

   ```
   ! tcp_local
   tcp_local smtp mx single_sys remotehost inner switchchannel
   identnonenumeric subdirs 20 maxjobs 7 pool SMTP_POOL maytlsserver
   maysaslserver saslswitchchannel tcp_auth missingrecipientpolicy 0
   aliasdetourhost tcp_scanner-daemon
   tcp-daemon

   ! tcp_submit
   tcp_submit submit smtp mx single_sys mustsaslserver maytlsserver
   missingrecipientpolicy 4 aliasdetourhost tcp_scanner-daemon
   tcp_submit-daemon
   ```

请注意， aliasdetourhost (tcp_scanner-daemon) 的参数是新通道 tcp_scanner 的正式主机名。

3. 通过 tcp_scanner 通道，创建重写规则以接收扫描系统返回的邮件。

```
[1.2.3.4] $E$R$U[1.2.3.4]@tcp_scanner-daemon
```

其中， 1.2.3.4 是扫描程序系统的 IP 地址。

如果没有此重写规则，邮件将通过其他 tcp* 源通道之一进入，并且因为这些源通道均有 aliasdetourhost，所以将再次扫描邮件。将出现一个回路。

4. 重新编译配置并重新启动分发程序。

```
#imsimta cnbuild
#imsimta restart dispatcher
```

示例 2：

假定第三方扫描程序在与 MTA 相同的主机上运行，但是在不同的端口上进行侦听。假定在端口 10024 上接受邮件，并在端口 10025 上传回邮件。

1. 创建新通道 tcp_scanner。

```
! tcp_scanner
tcp_scanner smtp nomx single_sys identnonenumeric subdirs 20 maxjobs 7 pool
SCAN_POOL daemon 127.0.0.1 port 10024 enqueue_removeroute
tcp_scanner-daemon
```

2. 在要扫描的所有外来源 tcp 通道 （可能包括 tcp_local、 tcp_submit 和 tcp_intranet 等）上，将 aliasDetourHost tcp_scanner-daemon 添加到 tcp_local。以下显示了一个 tcp_local 和 tcp_submit 的示例。

```
! tcp_local
tcp_local smtp mx single_sys remotehost inner switchchannel
identnonenumeric subdirs 20 maxjobs 7 pool SMTP_POOL maytlsserver
maysaslserver saslswitchchannel tcp_auth missingrecipientpolicy 0
aliasdetourhost tcp_scanner-daemon
tcp-daemon

! tcp_submit
tcp_submit submit smtp mx single_sys mustsaslserver maytlsserver
missingrecipientpolicy 4 aliasdetourhost tcp_scanner-daemon
tcp_submit-daemon
```

3. 添加到 mappings 文件以通过 tcp_scanner 通道重新路由外发邮件。

```
CONVERSIONS

in-chan=tcp_scanner;out-chan=*;CONVERT              No
in-chan=tcp_*;out-chan=tcp_local;CONVERT      Yes,Channel=tcp_scanner
```

4. 在 job_controller.cnf 中的 SMTP_POOL 下，添加并发扫描的数量限制。

   尽管也应为扫描软件设置限制，但最好保持相同的设置，以便在扫描程序不接受邮件时 Messaging Server 不会尝试将邮件发送到扫描程序。

   ```
   !
   [POOL=SCAN_POOL]
   job_limit=2
   !
   ```

5. 将新服务添加到 dispatcher.cnf 以接受特殊端口上扫描程序返回的邮件，并使其源于 tcp_scan 以便不对其进行再次扫描

   ```
   !
   [SERVICE=SMTP_SCANNING]
   INTERFACE_ADDRESS=127.0.0.1
   PORT=10025
   IMAGE=IMTA_BIN:tcp_smtp_server
   LOGFILE=IMTA_LOG:tcp_smtp_server.log
   STACKSIZE=2048000
   PARAMETER=CHANNEL=tcp_scanner
   !
   ```

6. 重新编译配置并重新启动分发程序。

   ```
   # imsimta cnbuild
   # imsimta restart job_controller
   # imsimta restart dispatcher
   ```

NO-SOLICIT SMTP 扩展支持

关键字：sourcenosolicit 和 destinationnosolicit

Internet-Draft draft-malamud-no-soliciting-07.txt 中所述的 NO-SOLICIT SMTP 扩展已经在 Messaging Server 中作为建议的标准实施。以下通道关键字可以用来控制此功能：

sourcenosolicit 指定一个以逗号分隔的列表，此列表包括将在此通道提交的邮件中阻塞的请求字段值。值的列表将显示在 NO-SOLICIT EHLO 响应中。可以在这些值中使用全局样式通配符，但是，包含通配符的值将不会在 EHLO 通告中显示。

destinationnosolicit 指定一个以逗号分隔的列表，此列表包括不会被此通道中排队的邮件接受的请求字段值。

对错误 RCPT TO: 地址设置限制

关键字：deferralrejectlimit

对单个会话期间允许的错误 RCPT TO：地址的数量设置限制。在拒绝指定数量的 To：地址后，所有后续收件人（无论正确还是错误）都将被拒绝，并显示 4xx 错误。提供与 ALLOW_REJECTIONS_BEFORE_DEFERRAL SMTP 通道关键字相同的功能，但是以通道为基础。

第 13 章

使用预定义通道

首次安装 Messaging Server 时，有几个通道已经被定义 （请参见表 13-1）。本章介绍如何使用 MTA 中预定义的通道定义。

如果您还未阅读过第 10 章 “关于 MTA 服务和配置”，则应该在阅读本章前先阅读该章。有关在 imta.cnf 文件中配置重写规则的信息，请参见第 11 章 “配置重写规则”。

本章包含以下各节：

- 第 362 页的 “使用 Pipe 通道将邮件传送给程序”
- 第 363 页的 “配置本地 (/var/mail) 通道”
- 第 364 页的 “使用 Hold 通道临时保留邮件”
- 第 365 页的 “转换通道”
- 第 383 页的 “字符集转换和邮件重新格式化”

第 298 页的 “配置通道默认值”对 defaults 通道进行了介绍。

表 13-1 预定义的通道

通道	定义
defaults	用于指定各种通道的默认关键字。请参见第 298 页的 “配置通道默认值”。
l	仅适用于 UNIX。用于进行路由决策和使用 UNIX 邮件工具提交邮件。
ims-ms	向本地存储传送邮件。
native	仅适用于 UNIX。向 /var/mail 传送邮件。（请注意， Messaging Server 不支持对 /var/mail 的访问。用户必须使用 UNIX 工具访问 /var/mail 存储中的邮件。）
pipe	用于通过站点提供的程序或脚本执行传送。 pipe 通道执行的命令由管理员通过 imsimta 程序接口控制。

表 13-1 预定义的通道

通道	定义
reprocess process	这两个通道用于延迟邮件处理和脱机邮件处理。 reprocess 通道作为源通道或目标通道，通常不可见； process 通道与其他 MTA 通道一样是可见的。
defragment	提供了重新组合 MIME 片段邮件的方法。
conversion	对流经 MTA 的邮件按主体部分执行转换。
bitbucket	用于需要被废弃的邮件。
inactive/deleted	用于处理已在目录中被标记为 “无效 / 已删除”的用户的邮件。通常退回邮件并向邮件发件人返回自定义的退回消息。
hold	用于保留用户的邮件。例如，当用户从一个邮件服务器迁移到另一个邮件服务器时。
sms	向 SMS 网关提供对单向电子邮件的支持。
tcp_local tcp_intranet tcp_auth tcp_submit tcp_tas	实现基于 TCP/IP 的 SMTP。多线程的 TCP SMTP 通道包含一个多线程的 SMTP 服务器，该服务器在分发程序的控制下运行。外发 SMTP 邮件由通道程序 tcp_smtp_client 处理，并根据需要在作业控制器的控制下运行。 tcp_local 接收来自远程 SMTP 主机的外来邮件。根据是否使用智能主机 / 防火墙配置，将外发邮件直接发送到远程 SMTP 主机，或者将外发邮件发送到智能主机 / 防火墙系统。 tcp_intranet 在内部网中接收和发送邮件。 tcp_auth 用作 tcp_local 的切换通道；经过验证的用户将切换到 tcp_auth 通道，以避免中继阻止限制。 tcp_submit 在保留的提交端口 587 （请参见 RFC 2476）上接收邮件提交（通常来自用户代理）。 tcp_tas 是各站点用来进行统一邮件传送的特殊通道。

使用 Pipe 通道将邮件传送给程序

用户可能希望将外来邮件传递给程序而不是邮箱。例如，用户可能希望将其外来邮件发送到邮件分类程序。 pipe 通道使用站点提供的基于用户的程序执行邮件传送。

为了便于程序传送，必须首先通过 pipe 通道将程序注册为能够调用的程序。可以使用 imsimta program 实用程序完成此操作。该实用程序为每个通过 pipe 通道注册为能够调用的程序赋予唯一的名称。然后最终用户可以将方法名称指定为其 mailprogramdeliveryinfo LDAP 属性的值。

例如，要将 UNIX 命令 myprocmail 添加为用户可以调用的程序，应该首先使用 imsimta program 实用程序注册该命令，如以下示例所示。此示例注册了称作 myprocmail 的程序，该程序执行带有参数 -d *username* 的 procmail 程序，并以用户身份执行：

```
imsimta program -a -m myprocmail -p procmail -g "-d %s" -e user
```

请确保可执行程序存在于 programs 目录 *msg_svr_base*/data/site-programs 中。还要确保将执行权限设置为 “其他”。

要使用户能够访问程序，用户的 LDAP 条目必须包含以下属性和值：

```
maildeliveryoption: program
mailprogramdeliveryinfo: myprocmail
```

有关 imsimta program 实用程序的详细信息，请参见 Messaging Server Reference Manual。

其他传送程序必须符合以下出口代码和命令行参数限制：

出口代码限制。由 pipe 通道调用的传送程序必须返回有意义的错误代码，以便通道了解是使邮件出队、传送邮件供日后处理还是返回邮件。

如果子进程使用出口代码 0 (EX_OK) 退出，则认为邮件已成功传送，并将其从 MTA 队列中删除。如果使用出口代码 71、 74、 75 或 79 （EX_OSERR、 EX_IOERR、 EX_TEMPFAIL 或 EX_DB）退出，则认为出现临时错误，邮件的传送将被延迟。如果返回其他任何出口代码，邮件将被作为无法传送的邮件返回其创始者。系统标题文件 sysexits.h 中对这些出口代码进行了定义。

命令行参数。传送程序可以具有任意数量的固定参数和变量参数 %s ；对于由用户执行的程序，变量参数 %s 代表用户名，对于由邮寄主管 ("inetmail") 执行的程序，变量参数 %s 代表用户名 + 域。例如，以下命令行使用 procmail 程序传送收件人的邮件。

```
/usr/lib/procmail -d %s
```

配置本地 (/var/mail) 通道

选项文件可用于控制本地通道的各种特性。此本地通道选项文件必须存储在 MTA 配置目录中并且命名为 native_option （例如 *msg_svr_base*/config/native_option）。

选项文件由若干行组成。每一行包含一个选项的设置。选项设置具有以下格式：

option=value

value 可以是字符串或整数，这取决于选项的要求。

表 13-2 本地通道选项

选项	说明
FORCE_CONTENT_LENGTH （0 或 1；仅适用于 UNIX）	如果 FORCE_CONTENT_LENGTH=1，则 MTA 向传送到本机通道的邮件添加 Content-length: 标题行，并且当 "From" 位于行的开头时，使通道不使用 ">From" 语法。这使本地 UNIX 邮件可以与 Sun 较新的邮箱工具兼容，但与其他 UNIX 邮件工具存在潜在的不兼容性。
FORWARD_FORMAT （字符串）	指定用户的 .forward 文件的位置。字符串 %u 表示它将被替换到每个用户 ID 中。字符串 %h 表示它将被替换到每个用户的主目录中。默认行为 （如果未明确指定此选项）相当于： FORWARD_FORMAT=%h/.forward
REPEAT_COUNT （整数） SLEEP_TIME （整数）	当 MTA 试图传送新邮件时，如果用户的新邮件文件被其他进程锁定，这些选项将提供一种方法，用来控制本地通道程序尝试重试的次数和频率。如果在指定的重试次数之后仍不能打开文件，邮件将保留在本地队列中，下次运行本地通道时将再次尝试传送新邮件。 REPEAT_COUNT 选项控制通道程序在放弃之前尝试打开邮件文件的次数。REPEAT_COUNT 默认值为 30 （尝试 30 次）。 SLEEP_TIME 选项控制通道程序在两次尝试之间等待的秒数。SLEEP_TIME 默认值为 2 （两次重试之间等待 2 秒）。
SHELL_TIMEOUT （整数）	控制通道等待用户的 shell 命令在 .forward 中完成的时间长度 （以秒为单位）。出现这种超时后，邮件将被返回原始发件人，并返回类似 “等待用户的 shell 命令 *command* 完成超时” 的错误消息。默认值为 600 （10 分钟）。
SHELL_TMPDIR （目录专用）	控制向 shell 命令进行传送时本地通道创建临时文件的位置。默认情况下，这种临时文件是在用户的主目录中创建的。使用此选项，管理员可以选择在其他 （单个）目录中创建临时文件。例如： SHELL_TMPDIR=/tmp

使用 Hold 通道临时保留邮件

hold 通道用于保留暂时无法接收新邮件的收件人的邮件。邮件被保留可能是由于正在更改用户名，或者由于正在将用户的邮箱从一个邮件主机或域移动到另一个邮件主机或域。可能还有其他原因要临时保留邮件。

要保留邮件时，将把邮件定位到 *msg_svr_base*/queue/hold 目录中的 hold 通道，这时使用的机制与将邮件定位到 reprocess 通道时所使用的机制相同。使用这种方法，将不更改信封 To: 地址。邮件将作为 *ZZxxx*.HELD 文件写入到 *msg-server*/queue/hold 目录中的 hold 通道队列。这可以防止作业控制器看到这些邮件，从而 “保留” 这些

邮件。使用 imsimta qm dir -held 命令可以查看 .HELD 文件列表。使用 imsimta qm release 命令可以选择和释放这些邮件。释放邮件时，将其名称更改为 ZZ*xxx*.00，并通知作业控制器。然后，与 hold 通道关联的主程序 reprocess.exe 将处理这些邮件。因此，将使用正常的重写机制处理邮件 （以及 To: 地址）。

有关 imsimta qm 命令的详细信息，请参见 *Sun Java System Messaging Server Administration Reference* 。

转换通道

转换通道使您可以对流经 MTA 的指定邮件执行任意的主体部分处理。（请注意，主体部分不同于邮件，邮件可以包含多个主体部分，例如附件中的主体部分。此外，主体部分是由 MIME 标题指定和描述的。）该处理可以由站点提供的任何程序或命令过程进行，并可以进行诸如文本或图像的格式转换、病毒扫描、语言转换等操作。可以选择 MTA 通信的各种邮件类型用于转换，并且可以为每种类型的邮件主体部分指定特定的进程和程序。

使用本章的前提是了解通道的概念 （请参见第 175 页的 “通道”）。有关使用转换通道进行病毒扫描的补充信息，请参阅 Messaging Server 文档 Web 站点 http://docs.sun.com/db/coll/S1_MsgTechNotes 底部的 Messaging Server 技术说明。

转换通道的实现由以下部分组成：A) 选择邮件通信用于处理， B) 指定处理不同邮件的方式。将对这些过程作进一步详细介绍。

注 MTA 配置文件 (imta.cnf) 中将自动创建默认的转换通道。此通道可以原样使用，无需修改。

本节包含以下几部分：

- 第 366 页的 “MIME 概述”
- 第 367 页的 “选择用于转换处理的通信”
- 第 368 页的 “控制转换处理”
- 第 377 页的 “使用转换通道输出退回、删除或保留邮件”
- 第 378 页的 “转换通道示例”

MIME 概述

转换通道大量使用 MIME （通用 Internet 邮件扩展服务）标题行。您需要了解邮件结构和 MIME 标题字段。有关 MIME 的完整信息，请参阅 RFC 1806、 RFC 2045-2049 和 RFC 2183。为方便起见，本文对 MIME 做了简要概述。

邮件结构

简单邮件由标题和主体组成。标题位于邮件的顶部并包含特定的控制信息 （例如日期、主题、发件人和收件人）。主体是标题后面第一个空行之后的所有内容。MIME 指定了构建更复杂的邮件的方法，邮件可以包含多个主体部分，甚至主体部分中还可以嵌套主体部分。这样的邮件称作多部分邮件，如前文中所述，转换通道对邮件按主体部分进行处理。

MIME 标题

MIME 规范为主体部分定义了一系列标题行。其中包括 `MIME-Version`、`Content-type`、 `Content-Transfer-Encoding`、 `Content-ID` 和 `Content-disposition`。转换通道最经常使用的是 `Content-type` 和 `Content-disposition` 标题。以下显示了某些 MIME 标题行的示例：

```
Content-type: APPLICATION/wordperfect5.1;name=Poem.wpc
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename=Poem.wpc
Content-description: "Project documentation Draft1 wordperfect format"
```

注 MIME 标题行不同于通用的非 MIME 标题行 （例如 `To:`、 `Subject:` 和 `From:`）。就转换通道而言， MIME 标题行基本上以字符串 `Content-` 开头。

`Content-type` 标题

MIME `Content-Type` 标题说明主体部分的内容。以下显示了 `Content-Type` 标题的格式 （带有示例）：

`Content-type:` *type/subtype; parameter1=value; parameter2=value...*

type 说明主体部分内容的类型。类型包括 `Text`、 `Multipart`、 `Message`、 `Application`、 `Image`、 `Audio` 和 `Video`。

subtype 进一步说明内容类型。每个 Content-type 都有自己的一组子类型。例如：text/plain、 application/octet-stream 和 image/jpeg。 MIME 邮件的内容子类型是由 IANA （Internet 编号授权机构）指定和列出的。在以下站点可以查看该列表：http://www.isi.edu/in-notes/iana/assignments/media-types/media-types

parameter 特定于各个 Content-type/subtype 对。例如，以下显示了 charset 和 name 参数：

```
Content-type: text/plain; charset=us-ascii
Content-type: application/msword; name=temp.doc
```

charset 参数为文本邮件指定字符集。name 参数提供将数据写入文件时建议使用的文件名。

注 Content-Type 值、 subtypes 和参数名称都不区分大小写。

Content-disposition 标题

MIME Content-disposition 标题提供主体部分的显示信息。通常将其添加到附件中，指定是显示附件的主体部分 (inline) 还是显示将被复制的文件名 (attachment)。Content-disposition 标题具有以下格式：

Content-disposition: *disposition_type; parameter1=value;parameter2=value...*

disposition_type 通常为 inline （显示主体部分）或 attachment （显示为要保存的文件）。Attachment 通常具有参数 filename，该参数带有一个值，指定被保存文件的建议文件名。

有关 Content-disposition 标题的详细信息，请参见 RFC2183。

选择用于转换处理的通信

与其他 MTA 通道不同，转换通道通常不是在地址或 MTA 重写规则中指定的。相反，邮件是使用 CONVERSIONS 映射表 （由 imta_tailor 文件中的参数 IMTA_MAPPING_FILE 指定）发送到转换通道的。该表的条目具有以下格式：

IN-CHAN=*source-channel*;OUT-CHAN=*destination-channel*;CONVERT *Yes/No*

MTA 处理每个邮件时将探测 CONVERSIONS 映射表 （如果存在）。如果 *source-channel* 是邮件所来自的通道， *destination-channel* 是邮件将要进入的通道，则执行 CONVERT 之后的操作 （Yes 意味着 MTA 将邮件从其 *destination-channel* 转移到转换通道；如果未发现匹配，邮件将被排入常规目标通道）。

注 user@conversion.*localhostname* 格式或 user@conversion 格式的地址将通过转换通道进行路由，而不考虑 CONVERSIONS 映射表。

以下示例将所有非内部邮件 （来自 Internet 或发送到 Internet 的邮件）路由到转换通道。

```
CONVERSIONS

   IN-CHAN=tcp_local;OUT-CHAN=*;CONVERT   Yes
   IN-CHAN=*;OUT-CHAN=tcp_local;CONVERT     Yes
```

第一行指定将处理来自 tcp_local 通道的邮件。第二行指定也将处理进入 tcp_local 通道的邮件。 tcp_local 通道处理进入和来自 Internet 的所有邮件。由于默认设置是不经过转换通道，因此其他任何邮件将不经过转换通道。

请注意，这是一个非常基本的表，对于具有更多自定义配置的站点 （例如，使用多个外发到 Internet 的 tcp_* 通道的站点，或使用多个从 Internet 进入的 tcp_* 通道的站点）可能不够用。

控制转换处理

当邮件被发送到转换通道时，将按主体部分对其进行处理。处理是由 MTA conversions 文件控制的，该文件由 imta_tailor 文件中的 IMTA_CONVERSION_FILE 选项指定 （默认指定：*msg_svr_base*/conversions）。 conversions 文件由一些以行分隔的条目组成，这些条目控制将被处理的主体部分的类型和处理的方式。

每个条目由一个或多个行组成，行中包含一个或多个 name=*value* 参数子句。参数子句中的值符合 MIME 约定。除最后一行外，每一行必须以分号 (;) 结尾。此文件中的一个物理行最多可包含 252 个字符。您可以使用反斜杠 (\) 继续字符将一个逻辑行分为多个物理行。将通过不以分号结束的行、一个或多个空行或者两者的结合来终止条目。

以下是转换文件条目的简单示例：

代码示例 13-1 conversions 文件条目

```
out-chan=ims-ms; in-type=application; in-subtype=wordperfect5.1;
  out-type=application; out-subtype=msword; out-mode=block;
  command="/usr/bin/convert -in=wordp -out=msword 'INPUT_FILE' \ 'OUTPUT_FILE'"
```

out-chan=ims-ms; in-type=application; in-subtype=wordperfect5.1 子句限定主体部分。也就是说，这些子句指定被转换部分的类型。将读取每个部分的标题并提取其 Content-Type: 标题和其他标题的信息。然后将从头到尾按顺序扫描转换文件中的条目；将检查存在的所有 in-* 参数和 OUT-CHAN 参数 （如果存在）。如果上述所有参数都与被处理的主体部分的相应信息相匹配，将执行由 command= 或 delete= 子句指定的转换，并设置 out-* 参数。

如果未出现匹配，则将该部分与下一个 conversions 文件条目进行匹配。对所有主体部分进行扫描和处理 （假定有合格的匹配）后，邮件将被发送到下一个通道。如果没有匹配，则不进行处理，邮件将被发送到下一个通道。

out-chan=ims-ms 指定仅转换被发送到 ims-ms 通道的邮件部分。 in-type=application 和 in-subtype=wordperfect5.1 指定邮件部分的 MIME Content-type 标题必须为 application/wordperfect5.1。

可以使用其他 in-* 参数对邮件部分作进一步限定。（请参见表 13-6。）上述条目将对具有以下 MIME 标题行的邮件部分触发转换操作：

```
Content-type: APPLICATION/wordperfect5.1;name=Draft1.wpc
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename=Draft1.wpc
Content-description: "Project documentation Draft1 wordperfect format"
```

在代码示例 13-1 中的三个转换文件限定参数之后，接下来的两个参数（out-type=application 和 out-subtype=msword）指定替换 MIME 标题行，这些标题行将被附加到 “已处理” 的主体部分。 out-type=application 和 out-subtype=msword 指定外发邮件的 MIME Content-type/subtype 为 application/msword。

请注意，由于 in-type 和 out-type 参数相同，因此 out-type=application 是不必要的，因为转换通道默认为外发主体部分原始的 MIME 标签。可以使用其他输出参数指定外发主体部分的其他 MIME 标签。

out-mode=block （代码示例 13-1）指定站点提供的程序将返回的文件类型。也就是说，它指定存储文件的方式，以及在返回的文件中重新读取转换通道的方式。例如， html 文件以文本模式存储，而 .exe 程序文件或 zip 文件以块 / 二进制模式存储。模式用于说明被读取文件的特定存储格式。

代码示例 13-1 中最后一个参数

```
command="/usr/bin/convert -in=wordp -out=msword 'INPUT_FILE' 'OUTPUT_FILE'"
```

指定将对主体部分进行的操作。

command= 参数指定将对主体部分执行的程序。/usr/bin/convert 是假设的命令名称；-in=wordp 和 -out=msword 是假设的命令行参数，指定输入文本和输出文本的格式；INPUT_FILE 和 OUTPUT_FILE 是转换通道环境参数 （请参见第 371 页的 “使用 转换通道环境变量”），指定包含原始主体部分的文件以及程序将存储被转换主体部分的文件。

注 现在，当常规转换条目请求包含外部邮件标题的文件时，信封创始者和收件人信息将分别作为 x-envelope-from 字段和 x-envelope-to 字段提供。

用 DELETE=1 替换 command 参数即可删除邮件部分，而不对主体部分执行命令。

注 只要修改了 conversions 文件，就必须重新编译配置 （请参见 Sun Java System Messaging Server Administration Reference 中的 imsimta refresh 命令）。

转换通道信息流程

信息的流程如下：包含主体部分的邮件进入转换通道。转换通道分析邮件，并逐一处理各部分。然后转换通道对主体部分进行限定，即通过将主体部分的 MIME 标题行与**限定参数**进行比较来确定是否对其进行处理。如果主体部分合格，则开始转换处理。如果要将 MIME 或主体部分信息传递到转换脚本，该信息将存储在由**信息传递参数**指定的环境变量 （表 13-3）中。

这时，将对主体部分进行由**操作参数**指定的操作。通常，该操作为删除主体部分或将其传递给脚本中包含的程序。脚本将处理主体部分，然后将其重新发送给转换通道，以重新组合成处理后的邮件。脚本还可以使用转换通道**输出选项**将信息发送给转换通道。这些信息可能是要添加到输出主体部分的新的 MIME 标题行、要返回给邮件发件人的错误文本或者指示 MTA 启动某些操作 （例如退回、删除或保留邮件）的特殊指令。

最后，转换通道按照**输出参数**的指定对输出主体部分的标题行进行替换。

使用 转换通道环境变量

对邮件主体部分进行操作时，在通道和站点提供的程序之间来回传递 MIME 标题行信息 （或整个主体部分）通常是很有用的。例如，程序可能需要 Content-type 和 Content-disposition 标题行信息以及邮件主体部分。通常，站点提供的程序的主要输入是从文件读取的邮件主体部分。对主体部分进行处理后，程序需要将其写入一个文件，转换通道可以从该文件中进行读取。这种类型的信息传递是通过使用转换通道环境变量进行的。

可以使用 parameter-symbol-* 参数在 conversions 文件中创建环境变量，或通过使用一组预定义的转换通道环境变量 （请参见表 13-4 第 375 页）进行创建。

以下 conversions 文件条目和外来标题显示了如何使用环境变量将 MIME 信息传递给站点提供的程序。

conversions 文件条目：

```
in-channel=*; in-type=application; in-subtype=*;
  parameter-symbol-0=NAME; parameter-copy-0=*;
  dparameter-symbol-0=FILENAME; dparameter-copy-0=*;
  message-header-file=2; original-header-file=1;
  override-header-file=1; override-option-file=1;
  command="/bin/viro-scan500.sh 'INPUT_FILE' 'OUTPUT_FILE'"
```

外来标题：

```
Content-type: APPLICATION/msword; name=Draft1.doc
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename=Draft1.doc
Content-description: "Project documentation Draft1 msword format"
```

in-channel=*; in-type=application; in-subtype=* 指定对来自 application 类型的所有输入通道的邮件主体部分进行处理。

parameter-symbol-0=NAME 指定将第一个 Content-type 参数值 （此示例中为 Draft1.doc）存储在称作 NAME 的环境变量中。

parameter-copy-0=* 指定将输入主体部分的所有 Content-type 参数复制到输出主体部分。

dparameter-symbol-0=FILENAME 指定将第一个 Content-disposition 参数值 （此示例中为 Draft1.doc）存储在称作 FILENAME 的环境变量中。

dparameter-copy-0=* 指定将输入主体部分的所有 Content-disposition 参数复制到输出主体部分。

message-header-file=2 指定将邮件的原始标题作为一个整体 （最外层邮件标题）写入到由环境变量 MESSAGE_HEADERS 指定的文件中。

original-header-file=1 指定将封闭的 MESSAGE/RFC822 部分的原始标题写入到由环境变量 ORIGINAL_HEADERS 指定的文件中。

override-header-file=1 指定从环境变量 OUTPUT_HEADERS 指定的文件中读取 MIME 标题，这将覆盖封闭的 MIME 部分中原始的 MIME 标题行。 $OUTPUT_HEADERS 是运行转换时创建的应急的临时文件。站点提供的程序将使用此文件存储转换过程中更改的 MIME 标题行。然后，当转换通道重新组合主体部分时，将从此文件中读取 MIME 标题行。请注意，只能对 MIME 标题行进行修改。其他通用的非 MIME 标题行不能通过转换通道进行更改。

override-option-file=1 指定转换通道从 OUTPUT_OPTIONS 环境变量命名的文件中读取 *转换通道* **选项**。请参见第 374 页的 “使用转换通道输出选项”。

command="msg_svr_base/bin/viro-scan500.sh" 指定将对邮件主体部分执行的命令。

表 13-3 转换通道环境变量

环境变量	说明
ATTACHMENT_NUMBER	用于当前部件的附件号。它与 ATTACHMENT-NUMBER 转换匹配参数的格式相同。
CONVERSION_TAG	当前活动转换标记的列表。此列表与 TAG 转换匹配参数相对应。
INPUT_CHANNEL	将邮件排队送到转换通道的通道。此通道与 IN-CHANNEL 转换匹配参数相对应。
INPUT_ENCODING	最初存在于主体部分中的编码。
INPUT_FILE	包含原始主体部分的文件的名称。站点提供的程序应读取此文件。
INPUT_HEADERS	包含主体部分原始标题行的文件的名称。站点提供的程序应读取此文件。
INPUT_TYPE	输入邮件部分的 MIME Content-type。
INPUT_SUBTYPE	输入邮件部分的 MIME 内容子类型。
INPUT_DESCRIPTION	输入邮件部分的 MIME content-description。
INPUT_DISPOSITION	输入邮件部分的 MIME content-disposition。
MESSAGE_HEADERS	文件名称，此文件包含封闭的邮件 （不只是主体部分）的原始最外层标题，或者包含该部分最直接的封闭 MESSAGE/RFC822 部分的标题。站点提供的程序应读取此文件。
OUTPUT_CHANNEL	邮件被发送到的通道。此通道与 OUT-CHANNEL 转换匹配参数相对应。

表 13-3 转换通道环境变量 （续）

环境变量	说明
OUTPUT_FILE	文件名称，站点提供的程序应在此文件中存储其输出。站点提供的程序应创建并编写此文件。
OUTPUT_HEADERS	文件名称，站点提供的程序应在此文件中存储封闭部分的 MIME 标题行。站点提供的程序应创建并编写此文件。请注意，文件应包含实际 MIME 标题行 （而不是 option=value 行），后跟一个空行作为其最后一行。另请注意，只能对 MIME 标题行进行修改。其他通用的非 MIME 标题行不能通过转换通道进行更改。
OUTPUT_OPTIONS	文件名称，站点提供的程序应从此文件中读取转换通道选项。请参见第 374 页的“使用转换通道输出选项”。
PART_NUMBER	当前部件的部件号。它与 PART-NUMBER 转换匹配参数的格式相同。
PART_SIZE	要处理的部件的大小 （字节）。

邮件转换标记

邮件转换标记是与特定收件人或发件人相关联的特殊标记。传送邮件时，该标记对于可能将其用于进行特殊处理的转换通道程序是可见的。转换标记储存在 LDAP 目录中。

可以按以下方式来使用邮件转换标记：管理员可以使用值为 harmonica 的邮件转换标记来设置选定的用户。然后，管理员将设置一个转换通道，在处理邮件时，该通道将检测是否存在该标记和 harmonica 值。如果存在，程序将执行某个任意函数。

可以基于用户或域设置邮件转换标记。域级别的收件人 LDAP 属性为 MailDomainConversionTag （可以使用 MTA 选项 LDAP_DOMAIN_ATTR_CONVERSION_TAG 进行修改）。用户级别的收件人 LDAP 属性为 MailConversionTag （可以使用 MTA 选项 LDAP_CONVERSION_TAG 进行修改）。两种属性均可具有多个值，每个值指定一个不同的标记。与给定收件人相关联的标记集是可以积累的，即：将在域级别设置的标记与在用户级别设置的标记相结合。

基于发件人的转换标记可以使用 MTA 选项 LDAP_SOURCE_CONVERSION_TAG 和

LDAP_DOMAIN_ATTR_SOURCE_CONVERSION_TAG 进行设置，这些选项将为与这些源地址相

关联的转换标记分别指定用户和域级别的 LDAP 属性。这些选项都没有默认属性。

使用转换通道输出选项

转换通道输出选项 （表 13-4）是动态变量，用于将信息和特殊指令从转换脚本传递到转换通道。例如，在主体部分处理期间，脚本可能要发送一个特殊指令，要求转换通道退回邮件，并向返回的邮件添加错误文本，说明邮件中带有病毒。

输出选项是通过在所需的转换条目中设置 OVERRIDE-OPTION-FILE=1 启动的。然后，脚本将根据需要设置输出选项并将其存储在环境变量文件 OUTPUT_OPTIONS 中。脚本完成对主体部分的处理后，转换通道将从 OUTPUT_OPTIONS 文件中读取选项。

OUTPUT_OPTION 变量是转换通道从中读取选项的文件的名称。通常，它被用作传递信息的应急临时文件。以下示例显示了一个脚本，该脚本使用输出选项向邮件中带有病毒的发件人返回错误消息。

```
/usr/local/bin/viro_screen2k $INPUT_FILE   # run the virus screener

if [ $? -eq 1 ]; then
   echo "OUTPUT_DIAGNOSTIC='Virus found and deleted.'"> $OUTPUT_OPTIONS
   echo "STATUS=178029946" >> $OUTPUT_OPTIONS
else
   cp $INPUT_FILE $OUTPUT_FILE # Message part is OK
fi
```

在此示例中，系统诊断消息和状态代码被添加到由 $OUTPUT_OPTIONS 定义的文件中。如果读取 $OUTPUT_OPTIONS 临时文件，您会看到类似于以下的内容：

```
OUTPUT_DIAGNOSTIC="Virus found and deleted."
STATUS=178029946
```

OUTPUT_DIAGNOSTIC='Virus found and deletedí 行告诉转换通道将文本 Virus found and deleted 添加到邮件中。

178029946 是基于 pmdf_err.h 文件的 PMDF__FORCERETURN 状态，该文件位于 *msg_svr_base*/include/deprecated/pmdf_err.h 中。此状态代码指示转换通道将邮件返回发件人。（有关使用特殊指令的详细信息，请参见第 377 页的 “使用转换通道输出退回、删除或保留邮件”。）

以下显示了输出选项的完整列表。

表 13-4 转换通道输出选项

选项	说明
OUTPUT_TYPE	输出邮件部分的 MIME 内容类型。
OUTPUT_SUBTYPE	输出邮件部分的 MIME 内容子类型。
OUTPUT_DESCRIPTION	输出邮件部分的 MIME 内容说明。
OUTPUT_DIAGNOSTIC	转换通道强制退回邮件时，作为发送给发件人的邮件的一部分的文本。
OUTPUT_DISPOSITION	输出邮件部分的 MIME content-disposition。
OUTPUT_ENCODING	在输出邮件部分中使用的 MIME 内容传送编码。
OUTPUT_MODE	转换通道编写输出邮件部分所用的 MIME Mode，因此也是收件人读取输出邮件部分使用的模式。
STATUS	转换器的退出状态。这通常是一个特殊指令，启动由转换通道进行的某些操作。在 *msg_svr_base*/include/deprecated/pmdf_err.h 中可以查看指令的完整列表。

封闭 MESSAGE/RFC822 部分中的标题

对邮件部分执行转换时，转换通道可以访问封闭 MESSAGE/RFC822 部分中的标题，或者访问邮件标题 （如果没有封闭 MESSAGE/RFC822 部分）。标题中的信息对于站点提供的程序可能会很有用。

如果选择了带有 ORIGINAL-HEADER-FILE=1 的条目，则封闭 MESSAGE/RFC822 部分的所有原始标题行都将被写入由 ORIGINAL_HEADERS 环境变量所表示的文件。如果 OVERRIDE-HEADER-FILE=1，则转换通道将读取由 ORIGINAL_HEADERS 环境变量所表示的文件的内容，并将其用作该封闭部分中的标题。

通过转换条目调用映射表

可以将 out-parameter-* 值存储在任意命名的映射表中并对其进行检索。某些客户机使用一个普通名称 （例如 att.dat）发送所有附件，不管附件是 postscript、msword、text 还是其他类型，上述功能对于重命名客户机发送的附件很有用。这是重新标记邮件部分，以便其他客户机 （例如 Outlook）能够通过读取扩展名来打开邮件部分的普通方法。

从映射表检索参数值的语法如下：

'mapping-table-name:mapping-input[*$Y, $N*]'

$Y 将返回一个参数值。如果未找到匹配，或者匹配返回 $N，将忽略转换文件条目中的此参数，或将其看作空字符串。缺少匹配或返回 $N 不会导致转换条目本身被中止。

请仔细阅读以下映射表：

```
X-ATT-NAMES

   postscript       temp.PS$Y
   wordperfect5.1   temp.WPC$Y
   msword           temp.DOC$Y
```

用于上述映射表的以下转换条目将导致在附件中使用特定文件名称替换普通文件名称：

```
out-chan=tcp_local; in-type=application; in-subtype=*;
   in-parameter-name-0=name; in-parameter-value-0=*;
   out-type=application; out-subtype='INPUT-SUBTYPE';
   out-parameter-name-0=name;
   out-parameter-value-0="'X-ATT-NAMES:\\'INPUT_SUBTYPE\\''";
   command="cp  'INPUT_FILE'  'OUTPUT_FILE'"
```

在以上示例中， out-chan=tcp_local; in-type=application; in-subtype=* 指定被处理的邮件必须来自 content-type 标题为 application/* （* 指定任何子类型都可以）的 tcp_local 通道。

in-parameter-name-0=name; in-parameter-value-0=* 进一步指定邮件必须具有参数类型 name=* （同样， * 指定任何参数值都可以。）

out-type=application; 指定处理后邮件的 MIME Content-type 参数为 application。

out-subtype= 扦 NPUT-SUBTYPEí; 指定处理后主体部分的 MIME subtype 参数为 INPUT-SUBTYPE 环境变量，它是输入 subtype 的原始值。因此，如果要将

Content-type: application/xxxx; name=foo.doc

更改为

Content-type: application/msword; name=foo.doc

您需要使用

```
out-type=application; out-subtype=msword
```

out-parameter-name-0=name; 指定输出主体部分的第一个 MIME Content-type 参数的类型为 name=。

out-parameter-value-0= 扰 -ATT-NAMES:\\ 扦 NPUT_SUBTYPE\\ 拨 ; 指定使用第一个 MIME subtype 参数值，并在映射表 X-ATT-NAMES 中搜索 subtype 匹配。如果找到匹配， name 参数将接收 X-ATT-NAMES 映射表中指定的新值。因此，如果参数类型为 msword， name 参数将为 temp.DOC。

使用转换通道输出退回、删除或保留邮件

本节介绍如何使用转换通道选项退回、删除或保留邮件。基本过程如下：

1. 在相应的 conversions 文件条目中设置 OVERRIDE-OPTION-FILE=1。这将告诉转换通道从 OUTPUT_OPTIONS 文件中读取输出选项。
2. 使用转换脚本来确定需要对特定邮件主体部分进行的操作。
3. 在脚本中，通过在 OUTPUT_OPTIONS 文件中写入 STATUS=*directive_code* 选项来指定用于该操作的特殊指令。

在 *msg_svr_base*/include/deprecated/pmdf_err.h 中可以查看特殊指令的完整列表。转换通道常用的指令如下：

表 13-5 转换通道常用的特殊指令

名称	十六进制值	十进制值
PMDF__FORCEHOLD	0x0A9C86AA	178030250
PMDF__FORCERETURN	0x0A9C857A	178029946
PMDF__FORCEDELETE	0x0A9C8662	178030178

我们将使用示例来说明这些指令的功能。

退回邮件

要使用转换通道退回邮件，请在相应的 conversions 文件条目中设置 OVERRIDE-OPTION-FILE=1，并将以下行添加到转换脚本中：

```
echo "STATUS=178029946" >> $OUTPUT_OPTIONS
```

如果希望将简短的文本字符串添加到退回的邮件中，请将以下行添加到转换脚本中：

```
echo OUTPUT_DIAGNOSTIC=text-string >> $OUTPUT_OPTIONS
```

其中 text string 大致为："The message sent from your machine contained a virus which has been removed.Be careful about executing email attachments."

有条件地删除邮件部分

根据邮件部分所包含的内容有条件地删除邮件部分可能会很有用。可以使用输出选项进行此操作。与之相反， DELETE=1 转换参数子句将无条件删除邮件部分。

要使用输出选项删除邮件部分，请在相应的 conversions 文件条目中设置 OVERRIDE-OPTION-FILE=1，并将以下行添加到转换脚本中：

```
echo "STATUS=178030178" >> $OUTPUT_OPTIONS
```

保留邮件

根据邮件包含的内容有条件地保留邮件可能会很有用。要使用输出选项删除邮件部分，请在相应的 conversions 文件条目中设置 OVERRIDE-OPTION-FILE=1，并将以下行添加到转换脚本中：

```
echo "STATUS=178030250" >> $OUTPUT_OPTIONS
```

这将请求转换通道将邮件保留为转换通道队列中的 .HELD 文件。

转换通道示例

以下示例中所示的 CONVERSIONS 映射和一组转换规则使 GIF、JPEG 和 BITMAP 文件被发送到假设的通道 tcp_docuprint 中，并被自动转换为 PostScript。其中几个转换使用假设的 /usr/bin/ps-converter.sh 进行该转换。还包含一个将 WordPerfect 5.1 文件转换为 Microsoft Word 文件的附加规则。

```
CONVERSIONS

      IN-CHAN=*;OUT-CHAN=tcp_docuprint;CONVERT    Yes
```

```
out-chan=ims-ms; in-type=application; in-subtype=wordperfect5.1;
  out-type=application; out-subtype=msword; out-mode=block;
  command="/bin/doc-convert -in=wp -out=msw   'INPUT_FILE'  'OUTPUT_FILE'"

out-chan=tcp_docuprint; in-type=image; in-subtype=gif;
  out-type=application; out-subtype=postscript; out-mode=text;
  command="/bin/ps-convert -in=gif -out=ps   'INPUT_FILE'  'OUTPUT_FILE'"

out-chan=tcp_docuprint; in-type=image; in-subtype=jpeg;
  out-type=application; out-subtype=postscript; out-mode=text;
  command="/bin/ps-convert -in=jpeg -out=ps   'INPUT_FILE'  'OUTPUT_FILE'"

out-chan=tcp_docuprint; in-type=image; in-subtype=bitmap;
  out-type=application; out-subtype=postscript; out-mode=text;
  command="/bin/ps-convert -in=bmp -out=ps   'INPUT_FILE'  'OUTPUT_FILE'"
```

自动检测 Arabic 字符集

为自动检测 Arabic 字符集，新增了 *auto_ef* 程序。

您可以从转换通道调用 auto_ef 程序来自动检测并标记 Arabic 字符集中多数未标记或未正确标记的文本邮件。这些未标记或未正确标记的邮件通常是从 Yahoo 或 Hotmail 以 Arabic 语言发送的。

如果没有正确标记字符集，许多邮件客户机就不能正确显示邮件。

如果邮件包含 MIME 内容类型标题，则 auto_ef 程序检测并处理仅具有文本 / 纯文本内容类型的邮件。如果邮件不是以 MIME 内容类型标题标记的，则 auto_ef 无条件地增加文本 / 纯文本内容类型。

要激活或启用此程序，必须：

1. 编辑 *msg_svr_base*/config 目录下的映射文件来启用您所选择的源通道和目标通道的转换通道。要为所有从 Internet 到本地用户的邮件启用转换通道，请在映射文件中增加如下部分：

   ```
   CONVERSIONS

       IN-CHAN=tcp*;OUT-CHAN=ims-ms;CONVERT    YES
   ```

   请注意，IN 和 OUT 通道取决于您的配置。如果您在中继 MTA 上部署，则必须修改通道以适合您的配置。例如，

   ```
   IN-CHAN=tcp*;OUT-CHAN=tcp*;CONVERT YES
   ```

   或者，您可以将所有通道打开，方法如下：

   ```
   IN-CHAN=*;OUT-CHAN=*;CONVERT YES
   ```

2. 在 *msg_svr_base*/config 目录下创建转换文件，该文件归 Messaging Server 用户所有并可由该用户读取，其内容如下：

   ```
   !
   in-channel=*; out-channel=*;
     in-type=text; in-subtype=*;
     parameter-copy-0=*; dparameter-copy-0=*;
     original-header-file=1; override-header-file=1;
     command="msg_svr_base/lib/arabicdetect.sh"
   !
   ```

3. 使用如下命令编译 MTA 配置：

   msg_svr_base/sbin/imsimta cnbuild

4. 使用下面的命令重新启动：

   msg_svr_base/sbin/imsimta restart

表 13-6 转换参数

参数	说明
限定参数 （指定邮件被转换之前必须匹配的参数。）	
OUT-CHAN, OUT-CHANNEL	执行转换所需匹配的输出通道 （允许使用通配符）。仅当邮件被发送到指定的通道时，才执行此条目指定的转换。
IN-CHAN, IN-CHANNEL	执行转换所需匹配的输入通道 （允许使用通配符）。仅当邮件来自指定的通道时，才执行此条目指定的转换。

表 13-6 转换参数 （续）

参数	说明
IN-TYPE	执行转换所需匹配的输入 MIME 类型 （允许使用通配符）。仅当此字段与主体部分的 MIME 类型匹配时，才执行指定的转换。
IN-SUBTYPE	执行转换所需匹配的输入 MIME 子类型 （允许使用通配符）。仅当此字段与主体部分的 MIME 子类型匹配时，才执行此条目指定的转换。
IN-PARAMETER-NAME-*n*	执行转换所需匹配的输入 MIME Content-Type 参数名称； *n* = 0、 1、 2.... 此参数可以与 IN-PARAMETER-VALUE-*n* 配合使用，以通过所包含的名称和值明确标识参数。
IN-PARAMETER-VALUE-*n*	执行转换所需匹配的相应 IN-PARAMETER-NAME 的输入 MIME Content-Type 参数值。仅当此字段与主体部分的 Content-Type 参数列表中的相应参数匹配时，才执行此条目指定的转换。允许使用通配符。
IN-PARAMETER-DEFAULT-*n*	未提供参数时，输入 MIME Content-Type 参数的默认值。主体部分中未指定此类参数时，该值被用作 IN-PARAMETER-VALUE-*n* 测试的默认值。
IN-DISPOSITION	执行转换所需匹配的输入 MIME Content-Disposition。
IN-DPARAMETER-NAME-*n*	执行转换所需匹配的输入 MIME Content-Disposition 参数名称； *n* = 0、 1、 2.... 此参数可以与 IN-DPARAMETER-VALUE-*n* 配合使用，以通过所包含的名称和值明确标识参数。
IN-DPARAMETER-VALUE-*n*	执行转换所需匹配的相应 IN-DPARAMETER-NAME 的输入 MIME Content-Disposition 参数值。仅当此字段与主体部分的 Content-Disposition: 参数列表中的相应参数匹配时，才执行此条目指定的转换。允许使用通配符。
IN-DPARAMETER-DEFAULT-*n*	未提供参数时，输入 MIME Content-Disposition 参数的默认值。主体部分中未指定此类参数时，该值被用作 IN-DPARAMETER-VALUE-*n* 测试的默认值。
IN-DESCRIPTION	执行转换所需匹配的输入 MIME Content-Description。
IN-SUBJECT	来自封闭 MESSAGE/RFC822 部分的 Subject。
TAG	输入标记，如邮件列表 CONVERSION_TAG 参数所设置。
输出参数 （指定主体部分的转换后输出设置。）	
OUT-TYPE	输出 MIME 类型 （如果与输入类型不同）。
OUT-SUBTYPE	输出 MIME 子类型 （如果与输入子类型不同）。
OUT-PARAMETER-NAME-*n*	输出 MIME Content-Type 参数名称； *n* = 0、 1、 2...
OUT-PARAMETER-VALUE-*n*	输出与 OUT-PARAMETER-NAME-*n* 相对应的 MIME Content-Type 参数值。
PARAMETER-COPY-*n*	要从输入主体部分的 Content-Type 参数列表复制到输出主体部分的 Content-Type: 参数列表的 Content-Type 参数列表； *n*=0、1、2... 使用要复制的 MIME 参数的名称，这与 IN-PARAMETER-NAME-*n* 子句相匹配。
OUT-DISPOSITION	输出 MIME Content-Disposition （如果与输入 MIME Content-Disposition 不同）。
OUT-DPARAMETER-NAME-*n*	输出 MIME Content-Disposition 参数名称； *n*=0、 1、 2...

表 13-6 转换参数 （续）

参数	说明
OUT-DPARAMETER-VALUE-*n*	输出与 OUT-DPARAMETER-NAME-*n* 相对应的 MIME Content-Disposition 参数值。
DPARAMETER-COPY-*n*	要从输入主体部分的 Content-Disposition：参数列表复制到输出主体部分的 Content-Disposition：参数列表的 Content-Disposition：参数列表；*n* = 0、1、2... 将要复制的 MIME 参数的名称当作参数，这与 IN-PARAMETER-NAME-*n* 子句相匹配。可以在该参数中使用通配符。特别是，参数 * 的意思是复制所有原始 Content-Disposition：参数。
OUT-DESCRIPTION	输出 MIME Content-Description （如果与输入 MIME Content-Description 不同）。
OUT-MODE	读取和存储被转换文件所使用的模式。应该为 BLOCK （二进制并可执行）或 TEXT。
OUT-ENCODING	重新组合邮件时要对被转换文件应用的编码。
操作参数 （指定要对邮件部分进行的操作。）	
COMMAND	执行转换所需执行的命令。执行转换所需执行的命令。此参数是必需的；如果未指定命令，将忽略条目。请使用 /（而不是 \）来指定路径。示例：command="D:/tmp/mybat.bat"
DELETE	0 或 1。如果设置该标志，将删除邮件部分。（如果被删除的是邮件中唯一的部分，将使用一个空文本部分进行替换。）
RELABEL	RELABEL=1 将把 MIME 标签重新标记为输出参数指定的任意内容。 Relabel=0 不进行任何操作。通常在标记错误的部分中进行重新标记 （例如：从 Content-type：application/octet-stream 到 Content-type：application/msword），以便用户可以 “双击” 打开一个部分，而无需将该部分保存到文件中，然后再用程序打开。
SERVICE-COMMAND	SERVICE-COMMAND=command 将执行站点提供的程序，该程序将在整个 MIME 邮件 （MIME 标题和内容主体部分）中操作。此外，与其他 CHARSET-CONVERSION 操作或转换通道操作不同， service-command 需要自己进行 MIME 分解、解码、重新编码和重新组合。请注意，此标志将使条目在转换通道处理期间被忽略；相反，将在字符集转换处理期间执行 SERVICE-COMMAND 条目。请使用 /（而不是 \）来指定路径。示例：command="D:/tmp/mybat.bat"
信息传递参数 （用于在通道和站点提供的程序之间传递信息。）	
DPARAMETER-SYMBOL-*n*	将在其中存储 Content-disposition 参数值 （如果存在）的环境变量；*n* = 0、 1、 2... 在执行站点提供的程序之前，将从 Content-disposition：参数列表中按顺序提取每个 DPARAMETER-SYMBOL-*n* （n=0 是第一个参数， n=2 是第二个参数，等等），并将其置于指定的环境变量中。
PARAMETER-SYMBOL-*n*	将在其中存储 Content-Type 参数值 （如果存在）的环境变量；*n* = 0、 1、 2... 在执行站点提供的程序之前，将从 Content-Type：参数列表中按顺序提取每个 PARAMETER-SYMBOL-*n* （n=0 是第一个参数， n=2 是第二个参数，等等），并将其置于名称相同的环境变量中。将 MIME 参数要转换为的变量的名称作为参数，这与 IN-PARAMETER-NAME-*n* 子句相匹配。

表 13-6 转换参数 （续）

参数	说明
MESSAGE-HEADER-FILE	将邮件的全部或部分原始标题写入由环境变量 MESSAGE_HEADERS 指定的文件，或者不写入邮件的原始标题。如果设置为 1，则将直接的封闭主体部分的原始标题写入由环境变量 MESSAGE_HEADERS 指定的文件。如果设置为 2，则将邮件的原始标题作为一个整体 （最外层的邮件标题）写入该文件。
ORIGINAL-HEADER-FILE	0 或 1。如果设置为 1，则将封闭的 MESSAGE/RFC822 部分 （不只是主体部分）的原始标题写入由环境变量 ORIGINAL_HEADERS 表示的文件。
OVERRIDE-HEADER-FILE	0 或 1。如果设置为 1，转换通道将从环境变量 OUTPUT_HEADERS 中读取 MIME 标题行，这将覆盖封闭的 MIME 部分中的原始标题行。
OVERRIDE-OPTION-FILE	如果 OVERRIDE-OPTION-FILE=1，转换通道将从 OUTPUT_OPTIONS 环境变量中读取选项。
PART-NUMBER	以点分隔的整数：*a. b. c*...MIME 主体部分的编号。

字符集转换和邮件重新格式化

本节介绍由 MTA 在内部执行的字符集转换、格式化转换和标记转换。请注意，本节中的某些示例使用了已过时或已作废的技术 （例如 DEC VMS 或 d 通道）。虽然这些技术已过时或已作废，但这不会使这些示例成为特定于 DEC 或 d 通道的示例。这些示例对于说明转换技术的工作原理仍然有效。我们将在以后的版本中更新这些示例。

字符集转换表是 Messaging Server 中一个非常基本的映射表。此表的名称为 CHARSET-CONVERSION。它用于指定所应进行的通道之间字符集转换的类型以及邮件重新格式化的类型。

在很多系统中，无需进行字符集转换或邮件重新格式化，因此无需使用此表。但是在某些情况下必须进行字符转换。例如，运行日文 OpenVMS 的站点可能就需要在 DEC Kanji 与在 Internet 上普遍使用的 ISO-2022 Kanji 之间进行转换。另外，大量使用多个国家的文字时也可能需要使用转换，因为在这种情况下， DEC 多国字符集 (DEC-MCS) 和指定用于 MIME 的 ISO-8859-1 字符集之间的微小差异都可能会导致出现问题，因而可能需要在二者之间进行实际转换。

CHARSET-CONVERSION 映射表还可以用于更改邮件的格式。它提供了将多个非 MIME 格式转换为 MIME 的功能。也可以对 MIME 编码和结构进行更改。当邮件被转发到仅支持 MIME 或 MIME 的某些子集的系统时，将使用这些选项。最后，在少数情况下，提供了从 MIME 到非 MIME 格式的转换。

MTA 将使用两种不同的方法探测 CHARSET-CONVERSION 映射表。第一次探测用于确定 MTA 是否应该对邮件重新格式化，如果是，应该使用哪些格式化选项。（如果未指定重新格式化， MTA 将不再进行检查以确定特定的字符集转换。）第一次探测的输入字符串具有以下通用格式：

IN-CHAN=*in-channel*;OUT-CHAN=*out-channel*;CONVERT

其中 *in-channel* 是源通道的名称 （邮件来自的通道）， *out-channel* 是目标通道的名称 （邮件将进入的通道）。如果出现匹配，所产生的字符串应该是用逗号分隔的关键字列表。表 13-7 列出了这些关键字。

表 13-7 CHARSET-CONVERSION 映射表关键字

关键字	说明
Always	强制转换，即使邮件将在进入 *out-channel* 之前先通过转换通道。
Appledouble	将其他 MacMIME 格式转换为 Appledouble 格式。
Applesingle	将其他 MacMIME 格式转换为 Applesingle 格式。
BASE64	将 MIME 编码转换为 BASE64。此关键字仅应用于已经编码的邮件部分。使用内容传送编码 7BIT 或 8bit 的邮件不需要任何特殊编码，因此该 BASE64 选项对这些邮件无效。
Binhex	将其他 MacMIME 格式 （或包含 Macintosh 类型和 Mac 生成器信息的部分）转换为 Binhex 格式。
Block	仅从 MacMIME 格式部分提取数据分叉。
Bottom	将所有 message/rfc822 主体部分 （转发的邮件）“转变”为邮件内容部分和标题部分。
Delete	将所有 message/rfc822 主体部分 （转发的邮件）“转变”为邮件内容部分，删除转发的标题。
Level	从邮件中删除冗余的多部分级别。
Macbinary	将其他 MacMIME 格式 （或包含 Macintosh 类型和 Macintosh 生成器信息的部分）转换为 Macbinary 格式。
No	禁用转换。
QUOTED-PRINTABLE	将 MIME 编码转换为 QUOTED-PRINTABLE。
Record,Text	按每行 80 个字符对文本 / 纯文本部分进行自动换行。
Record,Text= n	按每行 n 个字符对文本 / 纯文本部分进行自动换行。
RFC1154	将邮件转换为 RFC 1154 格式。
Top	将所有 message/rfc822 主体部分 （转发的邮件）“转变”为标题部分和邮件内容部分。

表 13-7 CHARSET-CONVERSION 映射表关键字

关键字	说明
UUENCODE	将 MIME 编码转换为 X-UUENCODE。
Yes	启用转换。

字符集转换

如果 MTA 探测并发现要对邮件重新格式化，它将接下去检查邮件的每个部分。如果找到任意文本部分，其字符集参数将被用于生成第二次探测。仅当 MTA 已经检查并发现可能需要转换时，才执行第二次探测。第二次探测中的输入字符串外观如下：

IN-CHAN=*in-channel*;OUT-CHAN=*out-channel*;IN-CHARSET=*in-char-set*

in-channel 和 *out-channel* 如上所述， *in-char-set* 是与前面提到的特定部分相关联的字符集的名称。如果第二次探测未出现匹配，将不执行字符集转换 （尽管可能会根据第一次探测中匹配的关键字执行邮件的重新格式化 [例如，对 MIME 结构的更改]）。如果出现匹配，将生成以下格式的字符串：

OUT-CHARSET=*out-char-set*

其中 *out-char-set* 指定 in-char-set 应转换成的字符集的名称。请注意，这两个字符集都必须在字符集定义表 charsets.txt （位于 MTA 表格目录中）中有所定义。如果该文件中未对字符集进行正确定义，将不进行转换。这通常不成问题，因为该文件定义了几百个字符集；目前使用的大多数字符集在该文件中都有定义。有关 charsets.txt 文件的详细信息，请参见 imsimta chbuild （UNIX 和 NT）实用程序的说明。

如果满足所有条件， MTA 接下去将建立字符集映射并进行转换。将使用邮件部分转换成的字符集的名称对已转换的邮件部分进行重新标记。

字符集转换映射已扩展为可以提供以下几种附加功能：

- 可以在映射条目的输出模板中指定 IN-CHARSET 选项。如果指定此选项，则将覆盖编码词中指定的字符集。
- 可以指定接受整数 0 或 1 的 RELABEL-ONLY 选项。如果此选项的值为 1，则 OUT-CHARSET 仅替换 IN-CHARSET，而不会进行重新标记。
- 如果使用 IN-CHARSET 选项将输入字符集设置为 *，则将依据此字符集来确定合适的标签。

示例：在 ISO-8859-1 和 UTF-8 之间相互转换

假定在本地使用 ISO-8859-1，但需要将此字符集转换为 UTF-8 才能在 Internet 上使用。而且，假定通过 tcp_local 和 tcp_internal 和 ims-ms 与 Internet 相连接，内部邮件源自这些通道并通过其进行传送。以下显示的 CHARSET-CONVERSION 表是以上述假定为前提进行的转换。

```
CHARSET-CONVERSION

  IN-CHAN=tcp_internal;OUT-CHAN=tcp_local;CONVERT                 Yes
  IN-CHAN=tcp_local;OUT-CHAN=tcp_internal;CONVERT                 Yes
  IN-CHAN=tcp_local;OUT-CHAN=ims-ms;CONVERT                       Yes
  IN-CHAN=*;OUT-CHAN=*;CONVERT                                    No
  IN-CHAN=tcp_internal;OUT-CHAN=tcp_local;IN-CHARSET=ISO-8859-1  OUT-CHARSET=UTF-8
  IN-CHAN=tcp_local;OUT-CHAN=tcp_internal;IN-CHARSET=UTF-8       OUT-CHARSET=ISO-8859-1
  IN-CHAN=tcp_local;OUT-CHAN=ims-ms;IN-CHARSET=UTF-8           OUT-CHARSET=ISO-8859-1
```

示例：在 EUC-JP 和 ISO-2022-JP 之间相互转换

下面显示的 CHARSET-CONVERSION 表指定了在本地使用的 EUC-JP 和基于 JP 代码的 ISO 2022 之间进行转换。

```
CHARSET-CONVERSION

  IN-CHAN=ims-ms;OUT-CHAN=ims-ms;CONVERT                        No
  IN-CHAN=tcp_internal;OUT-CHAN=ims-ms;CONVERT                  No
  IN-CHAN=tcp_internal;OUT-CHAN=tcp_internal;CONVERT            No
  IN-CHAN=tcp_internal;OUT-CHAN=*;CONVERT                       Yes
  IN-CHAN=*;OUT-CHAN=ims-ms;CONVERT                             Yes
  IN-CHAN=*;OUT-CHAN=tcp_internal;CONVERT                       Yes
  IN-CHAN=tcp_internal;OUT-CHAN=*;IN-CHARSET=EUC-JP             OUT-CHARSET=ISO-2022-JP
  IN-CHAN=*;OUT-CHAN=ims-ms;IN-CHARSET=ISO-2022-JP              OUT-CHARSET=EUC-JP
  IN-CHAN=*;OUT-CHAN=tcp_internal;IN-CHARSET=ISO-2022-JP      OUT-CHARSET=EUC-JP
```

邮件的重新格式化

如上所述，CHARSET-CONVERSION 映射表也用于影响 MIME 和几个专用邮件格式之间的附件转换。

以下各节给出了可以使用 CHARSET-CONVERSION 映射表影响的其他类型的邮件重新格式化的示例。

非 MIME 二进制附件转换

如果为处理邮件所涉及的所有通道启用了 CHARSET-CONVERSION，则特定的非标准（非 MIME）格式的邮件 （例如，特定的专用格式的邮件或来自 Microsoft Mail [MSMAIL] SMTP 网关的邮件）将被自动转换成 MIME 格式。如果您有 tcp_local 通道，它通常是来自 Microsoft Mail SMTP 网关的邮件的外来通道，以下命令将启用传送到本地用户的邮件的转换：

```
CHARSET-CONVERSION

   IN-CHAN=tcp_local;OUT-CHAN=ims-ms;CONVERT          Yes
```

您可能还希望为其他本地邮件系统添加通道条目。例如， tcp_internal 通道条目：

```
CHARSET-CONVERSION

    IN-CHAN=tcp_local;OUT-CHAN=l;CONVERT                 Yes
    IN-CHAN=tcp_local;OUT-CHAN=tcp_internal;CONVERT        Yes
```

或者，如果要对传送到每个通道的邮件进行转换，您只需指定 OUT-CHAN=*，而不是 OUT-CHAN=ims-ms。但是这将增加邮件处理的开销，因为这时要对进入 tcp_local 通道的所有邮件进行仔细检查，而不只是检查发送到特定通道的邮件。

更重要的是，这种不加选择的转换会使系统对于只是通过系统的邮件 （未必属于您自己的站点）的转换变得迟疑不决或可能不进行转换；而在这种情况下，系统应该只起传输作用，除了邮件信封和相关的传输信息，不必对其他信息进行更改。

要将 MIME 转换为 Microsoft Mail SMTP 网关可以理解的格式，请将 MTA 配置中的某个单独通道 （例如 tcp_msmail）用于 Microsoft Mail SMTP 网关，然后将以下内容放入 mappings. 文件中：

```
CHARSET-CONVERSION

   IN-CHAN=*;OUT-CHAN=tcp_msmail;CONVERT         RFC1154
```

重新标记 MIME 标题

某些用户代理或网关可能会发出 MIME 标题只包含很少信息的邮件，但是使用这些信息足以构建更精确的 MIME 标题。尽管最佳解决方案是正确配置这些用户代理或网关，但是如果它们不在您的控制范围之内，您可以要求 MTA 尝试重新构建更有用的 MIME 标题。

如果 CHARSET-CONVERSION 映射表的第一次探测产生了 Yes 或 Always 关键字，则 MTA 将检查 conversions 文件是否存在。如果 conversions 文件存在， MTA 将在其中查找带有 RELABEL=1 的条目，如果找到这样的条目，MTA 将执行该条目中指定的任意 MIME 重新标记操作。有关 conversions 文件条目的信息，请参见第 368 页的 “控制转换处理”。

例如，如下所示的 CHARSET-CONVERSION 表：

```
CHARSET-CONVERSION

   IN-CHAN=tcp_local;OUT-CHAN=tcp_internal;CONVERT            Yes
```

与 MTA 转换文件条目

```
out-chan=ims-ms; in-type=application; in-subtype=octet-stream;
  in-parameter-name-0=name; in-parameter-value-0=*.ps;
  out-type=application; out-subtype=postscript;
     parameter-copy-0=*; relabel=1

out-chan=ims-ms; in-type=application; in-subtype=octet-stream;
  in-parameter-name-0=name; in-parameter-value-0=*.msw;
  out-type=application; out-subtype=msword;
     parameter-copy-0=* relabel=1
```

的组合将使邮件被重新标记：通过 tcp_local 通道到达并被路由到 ims-ms 通道的邮件，如果到达时的原始 MIME 标记为 application/octet-stream，但带有扩展名为 ps 或 msw 的文件名参数，则它们将分别被重新标记为 application/postscript 或 application/msword。（请注意，这种更精确的标记本来应该由原来的用户代理或网关自己执行。）这样的重新标记与 MIME-CONTENT-TYPES-TO-MR 映射表结合使用会特别有用，可用于将生成的 MIME 类型转换回相应的 MRTYPE 标记 （这类标记需要进行精确的 MIME 标记才能理想地运行）；如果所有内容类型都只被标记为 application/octet-stream，则 MIME-CONTENT-TYPES-TO-MR 映射表最多只能将这些类型无条件地转换为 MRTYPE 一种类型。

通过以上示例组合后， MIME-CONTENT-TYPES-TO-MR 映射表条目包括

```
APPLICATION/POSTSCRIPT          PS
APPLICATION/MSWORD                 MW
```

原来的标记，例如

```
Content-type: application/octet-stream; name=stuff.ps
```

将被重新标记为

```
Content-type: application/postscript
```

然后被转换为 MRTYPE 标记 PS 以使邮件路由器知道需要 PostScript。

有时，按照相反类型的方向进行重新标记，将特定的 MIME 附件标记 “降级”为 application/octet-stream （通用二进制数据标记）也很有用。而且，“降级”特定的 MIME 标记通常与 mime_to_x400 通道 (PMDF-X400) 或 xapi_local 通道 (PMDF-MB400) 上的 convert_octet_stream 通道关键字结合使用，以将所有二进制 MIME 附件强制转换为 X.400 bodypart 14 格式。

例如，如下所示的 CHARSET-CONVERSION 映射表

```
CHARSET-CONVERSION

    IN-CHAN=*;OUT-CHAN=mime_to_x400*;CONVERT       Yes
```

与下面的 PMDF 转换文件条目

```
out-chan=mime_to_x400*; in-type=application; in-subtype=*;
   out-type=application; out-subtype=octet-stream; relabel=1

out-chan=mime_to_x400*; in-type=audio; in-subtype=*;
   out-type=application; out-subtype=octet-stream; relabel=1

out-chan=mime_to_x400*; in-type=image; in-subtype=*;
   out-type=application; out-subtype=octet-stream; relabel=1

out-chan=mime_to_x400*; in-type=video; in-subtype=*;
   out-type=application; out-subtype=octet-stream; relabel=1
```

的组合将把各种特定的 MIME 附件标记降级为进入 mime_to_x400* 通道的所有邮件通用的 application/octet-stream 标记 （从而应用 convert_octet_stream）。

MacMIME 格式转换

Macintosh 文件包括两个部分，即包含 Macintosh 专用信息的资源分叉和包含可在其他平台上使用的数据的数据分叉。这使 Macintosh 文件的传输变得更为复杂，因为传输 Macintosh 文件部分有四种不同的常用格式。其中三种格式 （Applesingle、Binhex 和 Macbinary）由在一个部分中共同编码的 Macintosh 资源分叉和 Macintosh 数据分叉组成。第四种格式 （Appledouble）是多部分的格式，资源分

叉和数据分叉位于不同的部分中。因此在非 Macintosh 平台上， Appledouble 可能是最有用的格式，因为在这种情况下可以忽略资源分叉部分，非 Macintosh 应用程序可以使用数据分叉部分。但是专门向 Macintoshe 进行发送时，其他格式可能会非常有用。

MTA 可以在这些不同的 Macintosh 格式之间进行转换。CHARSET-CONVERSION 关键字 Appledouble、 Applesingle、 Binhex 或 Macbinary 告诉 MTA 将其他 MacMIME 结构部分分别转换为 multipart/appledouble、 application/applefile、 application/mac-binhex40 或 application/macbinary MIME 结构。此外， Binhex 或 Macbinary 关键字还可以请求对非 MacMIME 格式部分进行指定的格式转换，如果该部分的 MIME Content-type: 标题中包含 X-MAC-TYPE 和 X-MAC-CREATOR 参数。CHARSET-CONVERSION 关键字 Block 告诉 MTA 仅从 MacMIME 格式部分中提取数据分叉，放弃资源分叉 （由于这样做会丢失信息，因此通常最好使用 Appledouble）。

例如，下面的 CHARSET-CONVERSION 表将通知 MTA 在传送到 VMS MAIL 邮箱或 GroupWise 邮局时转换为 Appledouble 格式，在传送到邮件路由器通道时转换为 Macbinary 格式：

```
CHARSET-CONVERSION

   IN-CHAN=*;OUT-CHAN=l;CONVERT            Appledouble
   IN-CHAN=*;OUT-CHAN=wpo_local;CONVERT    Appledouble
   IN-CHAN=*;OUT-CHAN=tcp_internal;CONVERT    Macbinary
```

转换成 Appledouble 格式仅应用于已经是 MacMIME 格式之一的部分。转换成 Macbinary 格式仅应用于已经是 MacMIME 格式之一的部分，或 MIME Content-type: 标题上包含 X-MAC-TYPE 和 X-MAC-CREATOR 参数的非 MacMIME 部分。

转换到 Appledouble 或 Block 格式时，可以使用 MAC-TO-MIME-CONTENT-TYPES 映射表指明要放到 Appledouble 部分或 Block 部分的数据分叉中的特定 MIME 标签，这取决于原始 Macintosh 文件中的 Macintosh 生成器和 Macintosh 类型信息。此表的探测形式为 *format*|*type*|*creator*|*filename*。其中 format 为 SINGLE、 BINHEX 或 MACBINARY 之一， type 和 creator 分别为十六进制的 Macintosh 类型和 Macintosh 生成器信息， filename 为文件名。

例如，要在向 ims-ms 通道进行发送时转换成 Appledouble，并在转换时将特定的 MIME 标签用于从 MACBINARY 或 BINHEX 部分转换而来的所有 MS Word 或 PostScript 文档，则正确的表可以是：

```
CHARSET-CONVERSION

  IN-CHAN=*;OUT-CHAN=ims-ms;CONVERT     Appledouble

MAC-TO-MIME-CONTENT-TYPES

!PostScript
    MACBINARY|45505346|76677264|*     APPLICATION/POSTSCRIPT$Y
    BINHEX|45505346|76677264|*        APPLICATION/POSTSCRIPT$Y
!Microsoft Word
    MACBINARY|5744424E|4D535744|*     APPLICATION/MSWORD$Y
    BINHEX|5744424E|4D535744|*        APPLICATION/MSWORD$Y
```

请注意，要执行指定的标记，必须在映射条目的模板 （右侧）中设置 $Y 标志。在 MTA 表格目录的 mac_mappings.sample 文件中可以查看其他类型附件的范例条目。

如果要将非 MacMIME 格式部分转换为 Binhex 或 Macbinary 格式，则需要提供这些部分的 X-MAC-TYPE 和 X-MAC-CREATOR MIME Content-type：参数值。请注意，可以使用 MIME 重新标记功能将这些参数强制放入邮件部分 （否则邮件部分中将没有这些参数）。

服务转换

可以将 MTA 的转换服务功能与站点提供的程序一起使用来处理邮件，以生成新格式的邮件。上述类型的 CHARSET-CONVERSION 操作和 conversion 通道操作都是在单个 MIME 邮件部分的内容中进行，转换服务与它们不同，它是在整个 MIME 邮件部分（MIME 标题和内容）以及整个 MIME 邮件中操作。此外，与其他 CHARSET-CONVERSION 操作或转换通道操作不同，转换服务需要自己进行 MIME 分解、解码、重新编码和重新组合。

与其他 CHARSET-CONVERSION 操作一样，转换服务通过 CHARSET-CONVERSION 映射表启用。如果 CHARSET-CONVESION 映射表的第一个探测产生了 Yes 或 Always 关键字，则 MTA 将检查 MTA conversions 文件是否存在。如果 conversions 文件存在， MTA 将在其中查找指定 SERVICE-COMMAND 的条目，如果找到这样的条目，则执行该条目。conversions 文件条目应具有以下格式：

```
in-chan=channel-pattern;
  in-type=type-pattern; in-subtype=subtype-pattern;
  service-command=command
```

command 字符串是最重要的。它是执行服务转换时应该执行的命令 （例如调用文档转换器）。命令必须处理一个输入文件，其中包含要服务的邮件文本，并生成一个输出文件，其中包含新邮件文本。在 UNIX 中，如果操作成功，命令必须使用“0”退出，否则使用非零值退出。

例如，如下所示的 CHARSET-CONVERSION 表

```
CHARSET-CONVERSION

IN-CHAN=bsout_*;OUT-CHAN=*;CONVERT     Yes
```

与以下 UNIX 上的 MTA conversions 文件条目

```
in-chan=bsout_*; in-type=*; in-subtype=*;
service-command="/pmdf/bin/compress.sh compress $INPUT_FILE $OUTPUT_FILE"
```

的组合将使来自 BSOUT 通道的所有邮件都被压缩。

环境变量用于传递输入文件名称、输出文件名称以及包含邮件信封收件人地址列表的文件的名称。这些环境变量的名称如下：

- INPUT_FILE - 要处理的输入文件的名称
- OUTPUT_FILE - 要生成的输出文件的名称
- INFO_FILE - 包含信封收件人地址的文件的名称

通过使用标准命令行替换可以将这三个环境变量的值替换到命令行中：即在变量名称前加 UNIX 美元字符。例如，如果 INPUT_FILE 和 OUTPUT_FILE 的值为 a.in 和 a.out，然后在 UNIX 上进行了如下声明：

```
in-chan=bsout_*; in-type=*; in-subtype=*;
    service-command="/pmdf/bin/convert.sh $INPUT_FILE $OUTPUT_FILE"
```

系统将执行以下命令

```
/pmdf/bin/convert.sh a.in a.out
```

第 14 章

将垃圾邮件和病毒过滤程序集成至 Messaging Server

本章介绍如何使用 Messaging Server 来集成和配置垃圾邮件和病毒过滤软件。本章介绍的垃圾邮件 / 病毒过滤技术比转换通道 （请参见第 365 页的 “转换通道”）所提供的技术更加强大。 Messaging Server 支持 Symantec Brightmail AntiSpam、SpamAssassin、和支持 Internet Content Adaptation Protocol (ICAP, RFC 3507)（特别是 Symantec AntiVirus Scan Engine）的反垃圾邮件 / 反病毒程序。

注 本章中有关**反垃圾邮件**或**垃圾邮件过滤**功能的信息也适用于**反病毒**或**病毒过滤**功能 （如果有）。某些产品可以提供这两种功能 (Brightmail)，而其他产品可能仅提供垃圾邮件过滤功能 (SpamAssassin) 或仅提供病毒过滤功能 (Symantec AntiVirus Scan Engine)。另请注意，通常在配置参数中使用 `spam`。

本章分为以下几节：

- 第 394 页的 “将垃圾邮件过滤程序集成至 Messaging Server—操作原理”
- 第 394 页的 “部署和配置第三方垃圾邮件过滤程序”
- 第 405 页的 “使用 Symantec Brightmail Anti-Spam”
- 第 409 页的 “使用 SpamAssassin”
- 第 422 页的 “使用 Symantec Anti-Virus Scanning Engine (SAVSE)”
- 第 428 页的 “支持 Sieve 扩展”

将垃圾邮件过滤程序集成至 Messaging Server—操作原理

从 Messaging Server 的角度来看，反垃圾邮件解决方案的实现机制大多相同：

1. Messaging Server 将邮件的副本发送至垃圾邮件过滤软件。
2. 垃圾邮件过滤软件分析邮件并返回结论说明是否为垃圾邮件。某些程序，如 SpamAssassin 可能还返回**垃圾邮件分数**，该分数是对邮件可能为垃圾邮件的数字评定。
3. Messaging Server 辨认结论并在邮件上进行 Sieve 操作 （请参见第 401 页的“指定要对垃圾邮件执行的操作”）。

垃圾邮件过滤程序通过协议与 MTA 进行交互。协议可能是标准 （在 Symantec AntiVirus Scan Engine 等基于 ICAP 的程序中）、专用 （在 Brightmail 中）或仅仅非标准 （在 SpamAssassin 中）。每个协议都要求软件使用 MTA 挂钩至界面。Brightmail 和 SpamAssassin 是最早的两个可以与 Messaging Server 集成的垃圾邮件过滤程序。 MTA 现在支持使用 ICAP 的程序。

部署和配置第三方垃圾邮件过滤程序

在 Messaging Server 上部署第三方过滤软件需要五个操作：

- **确定要部署哪些垃圾邮件过滤程序，以及要在其上部署这些程序的服务器的数量。** Messaging Server 允许您使用最多四种不同的垃圾邮件 / 病毒程序来过滤外来邮件。这些程序可以在单独的系统上、单一系统部署中与 Messaging Server 相同的系统上或两层部署中与 MTA 相同的系统上运行。所需的服务器数量取决于邮件负荷、硬件性能以及其他因素。有关确定您站点上的硬件要求的指导，请参阅垃圾邮件过滤软件文档或咨询代表。
- **安装和配置垃圾邮件过滤软件**。有关此信息，请参阅垃圾邮件过滤软件文档或咨询代表。
- **装入和配置过滤客户机库**。此操作包括在 MTA `option.dat` 文件中指定客户机库和配置文件，以及在过滤软件的配置文件中设置所需选项。第 395 页的“装入和配置垃圾邮件过滤软件客户机库”。
- **指定要被过滤的邮件**。邮件可以由用户、域或通道进行过滤。第 396 页的“指定要过滤的邮件”。
- **指定如何处理垃圾邮件**。垃圾邮件可以被放弃、归档到文件夹或在主题行上被标记为垃圾邮件，等等。第 401 页的“指定要对垃圾邮件执行的操作”。

注 由于以前版本的 Messaging Server 仅支持 Brightmail 过滤技术，因此关键字和选项具有如 `sourcebrightmail` 或 `Brightmail_config_file` 这样的名称。这些关键字和选项的名称已更改为更加通用的名称，例如 `sourcespamfilter` 或 `spamfilter_config_file`。为了兼容，保留了以前的 Brightmail 名称。

装入和配置垃圾邮件过滤软件客户机库

每个垃圾邮件过滤程序都应为 Messaging Server 提供客户机库文件和配置文件。装入和配置客户机库包括以下两个操作：

- 在 `options.dat` 文件中指定垃圾邮件过滤软件库的路径 (`spamfilterX_library`) 和配置文件 (`spamfilterX_config_file`)。除了这些选项，还有很多其他选项用于指定垃圾邮件过滤 LDAP 属性，以及要在垃圾邮件上使用的 Sieve 操作。
- 在垃圾邮件过滤软件配置文件中指定所需的选项。每个垃圾邮件过滤程序都有不同的配置文件和配置选项。垃圾邮件过滤软件一节以及过滤软件文档中介绍了这些内容。请参见第 405 页的 “使用 Symantec Brightmail Anti-Spam” 或第 409 页的 “使用 SpamAssassin”，以及第 422 页的 “使用 Symantec Anti-Virus Scanning Engine (SAVSE)”。

指定垃圾邮件过滤软件库的路径

Messaging Server 可以为邮件调用最多四种不同的过滤系统。例如，您可以通过 Symantec AntiVirus Scan Engine 和 SpamAssassin 运行邮件。每个过滤软件都是由 1 到 4 之间的一个数字进行标识的。这些数字将显示为各种垃圾邮件过滤选项、LDAP 属性和通道关键字的一部分， *X* 用作过滤标识号。例如，`sourcespamfilterX`*`X`*`optin` 或 `spamfilterX_config_file`。如果关键字或选项名称中遗漏了标识号，则将默认为 1。

以下 `option.dat` 设置用于指定 Messaging Server 通过 Symantec AntiVirus Scan Engine 和 SpamAssassin 来过滤邮件：

```
spamfilter1_library=Symantec_Library_File
spamfilter1_config_file=Symantec_Config_File
spamfilter2_library=SpamAssassin_Library_File
spamfilter2_config_file=SpamAssassin_Config_File
```

使用其他选项或关键字配置系统时，请使用该选项或关键字末尾的相应号码。例如，sourcespamfilter2optin 将参阅 SpamAssassin。sourcespamfilter1optin 将参阅 Symantec AntiVirus Scan Engine。没有必要按顺序使用编号。例如，如果要暂时禁用 Symantec AntiVirus Scan Engine，则可以只注释掉 spamfilter1_library 配置文件。

指定要过滤的邮件

一旦安装了垃圾邮件过滤软件并准备使用 Messaging Server 运行时，您需要指定要过滤的邮件。 Messaging Server 可以由用户、域或通道进行配置，以过滤邮件。以下每节介绍了一种方案：

- 第 396 页的 “指定用户级别的过滤”
- 第 398 页的 “指定域级别的过滤”
- 第 399 页的 “指定通道级别的过滤”

注 表达式 *optin* 意味着用户、域或通道被选择来接收邮件过滤。

指定用户级别的过滤

可能需要为每个用户指定过滤。例如，如果将垃圾邮件过滤或病毒过滤作为高级服务提供给 ISP 用户，则可以指定能接收和不能接收该服务的用户。用户过滤的一般步骤如下所示：

1. 指定激活垃圾邮件过滤软件的用户 LDAP 属性。

   在 option.dat 中设置 LDAP_OPTIN*X* 选项。示例：

   ```
   LDAP_OPTIN1=SymantecAV
   LDAP_OPTIN2=SpamAssassin
   ```

2. 在接收垃圾邮件过滤的用户条目中设置过滤属性。

   过滤属性的值为多个值并取决于服务器。使用步骤 1 所示的示例，条目为：

   ```
   SymantecAV:virus
   SpamAssassin:spam
   ```

   对于像 Brightmail 这种既可以过滤病毒又可以过滤垃圾邮件的程序，有效值为 spam 和 virus。用作多值属性时，每个值均需要一个单独的属性条目。例如，如果 Brightmail 的过滤属性被设置为 Brightmail，则条目为：

   ```
   Brightmail:spam
   Brightmail:virus
   ```

用户级别的过滤示例

本示例假定使用的是 Brightmail。还假定在 `option.dat` 文件中将 `LDAP_OPTIN1` 设置为 `Brightmail`。用户 Otis Fanning 在其用户条目中将 `Brightmail` 属性设置为 `spam` 和 `virus`。 Brightmail 将对他的邮件进行垃圾邮件和病毒过滤。代码示例 14-1 显示了 Otis Fanning 的 Brightmail 用户条目。

代码示例 14-1 Brightmail 的示例 LDAP 用户条目

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
pabURI: ldap://ldap.siroe.com:389/ou=fanning,ou=people,o=sesta.com,o=isp,o=pab
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota:  -1
mailMsgQuota:  100
Brightmail: virus
Brightmail: spam
```

如果使用的是 Symantec AntiVirus Scan Engine 和 SpamAssassin，则条目将类似于如下所示：

```
SymantecAV: virus
SpamAssassin: spam
```

有关更多示例和详细信息，请参见 " 使用 Symantec Brightmail Anti-Spam"、" 使用 SpamAssassin" 或 " 使用 Symantec Anti-Virus Scanning Engine (SAVSE)"。

指定域级别的过滤

您可以指定接收过滤的域。此功能的示例是：是否将反垃圾邮件或反病毒过滤作为高级服务提供给 ISP 域用户。指定域过滤的一般步骤如下所示：

1. 指定激活过滤软件的域 LDAP 属性。

   在 option.dat 中设置 LDAP_DOMAIN_ATTR_OPTIN*X* 选项。示例：

   ```
   LDAP_DOMAIN_ATTR_OPTIN1=SymantecAV
   LDAP_DOMAIN_ATTR_OPTIN2=SpamAssassin
   ```

2. 在接收垃圾邮件过滤的域条目中设置过滤属性。

   过滤属性的值为多个值并取决于服务器。使用步骤 1 所示的示例，条目将如下所示：

   ```
   SymantecAV: virus
   SpamAssassin: spam
   ```

   对于象 Brightmail 这种既可以过滤病毒又可以过滤垃圾邮件的程序，有效值为 spam 和 virus。用作多值属性时，每个值均需要一个单独的属性值条目。例如，如果 LDAP_DOMAIN_ATTR_OPTIN1 被设置为 Brightmail，则条目为：

   ```
   Brightmail: spam
   Brightmail: virus
   ```

域级别过滤示例

本示例假定使用的是 Brightmail。还假定在 option.dat 文件中将 LDAP_DOMAIN_ATTR_OPTIN1 设置为 Brightmail。对于 Sun LDAP Schema 1，在 DC 树的域条目 sesta.com 中将 Brightmail 属性设置为 spam 和 virus。对于 Sun LDAP Schema 2，也将域条目中的 Brightmail 设置为可以接收垃圾邮件过滤。

Brightmail 将对所有发送到 sesta.com 的邮件进行垃圾邮件和病毒过滤。代码示例 14-2 显示了域条目。

代码示例 14-2 Brightmail 的示例 LDAP 域条目

```
dn: dc=sesta,dc=com,o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
objectClass: nsManagedDomain
objectClass: icsCalendarDomain
description: DC node for sesta.com hosted domain
dc: sesta
inetDomainBaseDN: o=sesta.com,o=isp
inetDomainStatus: active
mailDomainStatus: active
mailDomainAllowedServiceAccess: +imap, pop3, http:*
```

代码示例 14-2 Brightmail 的示例 LDAP 域条目

```
mailRoutingHosts: manatee.siroe.com
preferredMailHost: manatee.siroe.com
mailDomainDiskQuota:  100000000
mailDomainMsgQuota:  -1
mailClientAttachmentQuota:  5
Brightmail: spam
Brightmail: virus
```

如果使用的是 Symantec AntiVirus Scan Engine 和 SpamAssassin，则条目将类似于如下所示：

```
SymantecAV: virus
SpamAssassin: spam
```

有关更多示例和详细信息，请参见 " 使用 Symantec Brightmail Anti-Spam"、" 使用 SpamAssassin" 或 " 使用 Symantec Anti-Virus Scanning Engine (SAVSE)"。

指定通道级别的过滤

按照源通道或目标通道的过滤为垃圾邮件过滤提供了更高的灵活性和粒度。例如，您可能希望按以下方式进行过滤：

- 只有从特定的 MTA 中继发送到后端邮件存储的邮件
- 所有来自特定 MTA 的外来邮件。
- 所有来自特定 MTA 的外发邮件。
- 所有来自特定 MTA 的外来邮件和外发邮件。

Messaging Server 使您可以按照源通道或目标通道指定过滤。表 14-1 中所述的通道关键字是实现过滤的机制。以下示例说明如何设置通道级别的过滤。

1. 在向后端邮件存储主机发送邮件的所有外来 SMTP 服务器的 `imta.cnf` 文件中添加重写规则。示例：

   ```
   msg_store1.siroe.com    $U@msg_store1.siroe.com
   ```

2. 使用 `destinationspamfilterXoptin` 关键字添加与该重写规则对应的通道。示例：

   ```
   tcp_msg_store1 smtp subdirs 20 backoff "pt5m" "pt10" "pt30" "pt1h" \
   "pt2h" "pt4h" maxjobs 1 pool IMS_POOL fileinto $U+$S@$D \
   destinationspamfilterloptin spam
   msg_store1.siroe.com
   ```

表 14-1 垃圾邮件过滤器的 MTA 通道关键字

通道关键字	说明
destinationspamfilter*X*optin	指定发送到该通道的所有邮件均由反垃圾邮件软件 *X* 进行过滤，即使那些服务未由用户或域使用 LDAP_OPTIN LDAP 属性进行指定。（过滤软件 X 由 option.dat 中的 spamfilter*X*_library 定义。）过滤器参数取决于过滤程序，并且跟在关键字后面。例如，Brightmail 的参数通常为 spam、virus 或 spam,virus。SpamAssassin 的参数为 spam。 在本示例中，将对发送到邮件存储中的所有邮件进行垃圾邮件扫描： ims-ms destinationspamfilter1optin spam,virus. . .
sourcespamfilter*X*optin	指定所有源自此通道的邮件将由反垃圾邮件软件 *X* 进行过滤，即使那些服务未由用户或域使用 LDAP_OPTIN LDAP 属性进行指定。此关键字后面跟系统范围内的默认参数，可用的参数取决于过滤程序。例如，对于 Brightmail，参数为 spam、virus 或 spam,virus。对于 SpamAssassin，参数为 spam。如果 switchchannel 有效，请将此关键字放置在 switched-to 通道上。

通道级别过滤示例

这些示例假定过滤程序由数字 1 指定。

示例 1。对所有从 MTA 中继发送到称为 msg_store1.siroe.com 的后端邮件存储的邮件进行垃圾邮件和病毒过滤。

1. 在向后端邮件存储主机发送邮件的 imta.cnf 文件中添加重写规则。示例：

   ```
   msg_store1.siroe.com   $U@msg_store1.siroe.com
   ```

2. 使用 destinationspamfilter*X*optin 关键字添加与该重写规则对应的通道。示例：

   ```
   tcp_msg_store1 smtp subdirs 20 backoff "pt5m" "pt10" "pt30" "pt1h" \
   "pt2h" "pt4h" maxjobs 1 pool IMS_POOL fileinto $U+$S@$D \
   destinationspamfilter1optin spam,virus
   msg_store1.siroe.com
   ```

示例 2。对所有通过 MTA 的外来邮件进行垃圾邮件过滤 （通常情况下，所有外来邮件都通过 tcp_local 通道）：

```
tcp_local smtp mx single_sys remotehost inner switchchannel \
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \
maytlsserver maysaslserver saslswitchchannel tcp_auth \
sourcespamfilter1optin spam
tcp-daemon
```

示例 3。过滤所有通过 MTA 的外发到 Internet 的邮件：（通常情况下，所有外发到 Internet 的邮件都通过 tcp_local 通道）。

```
tcp_local smtp mx single_sys remotehost inner switchchannel \
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \
maytlsserver maysaslserver saslswitchchannel tcp_auth \
destinationspamfilterloptin spam
tcp-daemon
```

示例 4。过滤所有通过 MTA 的外来和外发邮件：

```
tcp_local smtp mx single_sys remotehost inner switchchannel \
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \
maytlsserver maysaslserver saslswitchchannel tcp_auth \
sourcespamfilterloptin spam destinationspamfilterloptin spam
tcp-daemon
```

示例 5。过滤所有发送到两层系统中本地邮件存储的邮件，不使用基于用户的选定：

```
ims-ms smtp mx single_sys remotehost inner switchchannel \
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \
maytlsserver maysaslserver saslswitchchannel tcp_auth \
destinationspamfilterloptin spam
tcp-daemon
```

示例 6。对所有外来和外发邮件进行垃圾邮件和病毒过滤 （假定软件可以进行垃圾邮件过滤，也可以进行病毒过滤）：

```
tcp_local smtp mx single_sys remotehost inner switchchannel \
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \
maytlsserver maysaslserver saslswitchchannel tcp_auth \
destinationspamfilterloptin spam,virus sourcespamfilterloptin \
spam,virus
tcp-daemon
```

指定要对垃圾邮件执行的操作

垃圾邮件过滤程序分析邮件并向 Messaging Server 返回结论说明是否为垃圾邮件。然后 Messaging Server 将对邮件采取操作。使用 Sieve 邮件过滤语言指定操作。可能的操作包括放弃邮件、将邮件归档到文件夹、添加标题、向主题行添加标记，等等。也可以使用具有 if-then-else 语句的复杂 Sieve 脚本。

注 有关完整的 Sieve 语法，请参见 Sieve 规范 3028。另请参见 http://www.cyrusoft.com/sieve/

使用表 14-2 中所述的 MTA 垃圾邮件过滤器选项 (option.dat) 来指定 Sieve 脚本。主垃圾邮件过滤器操作选项包括 SpamfilterX_null_action （指定 Sieve 规则在返回的垃圾邮件结论为空值时执行）和 SpamfilterX_string_action （指定 Sieve 规则在返回的垃圾邮件结论为字符串时执行）。

垃圾邮件过滤程序通常向 MTA 返回一个字符串或一个空值以表示邮件为垃圾邮件。某些程序还会返回垃圾邮件分数——该分数是对邮件可能为垃圾邮件的数字评定。此分数可用于整个操作的一部分。以下示例显示了如何指定对已过滤的邮件的操作。每个示例均假定过滤程序由数字 1 指定。

示例 1：将结论为空值的垃圾邮件归档到文件 SPAM_CAN 中。

```
spamfilter1_null_action=data:,require "fileinto"; fileinto "SPAM_CAN";
```

也可以对返回的结论为字符串的垃圾邮件执行相同的操作：

```
spamfilter1_string_action=data:,require "fileinto"; fileinto "SPAM_CAN";
```

示例 2：将带有返回的结论字符串的垃圾邮件归档到以返回的结论字符串 （即 $U 所执行的操作）命名的文件。也就是说，如果返回的结论字符串为 spam，则邮件将存储在名为 spam 的文件中。

```
spamfilter1_null_action=data:,require "fileinto"; fileinto "$U";
```

示例 3：放弃结论为字符串值的垃圾邮件。

```
spamfilter1_string_action=data:,discard
```

也可以对返回的结论为空值的垃圾邮件执行相同的操作：

```
spamfilter1_null_action=data:,require "fileinto"; fileinto "SPAM_CAN";
```

示例 4。此行将向结论为字符串的确定为垃圾邮件的每个邮件添加标题 Spam-test :FAIL:

```
spamfilter1_string_action=data:,require ["addheader"];addheader "Spam-test:FAIL";
```

示例 5。此行将向返回字符串的垃圾邮件的主题行添加字符串 [PROBABLE SPAM]。

```
spamfilter1_string_action=data:,addtag "[PROBABLE SPAM]";
```

示例 6。此选项行假定返回的结论为字符串值，并且如果标题包含 resent-from 和 User-1，则将垃圾邮件归档到邮箱 testspam 中。如果邮件没有此标题，则该选项行将邮件归档到 spam 中。

```
spamfilter1_string_action=data:,require "fileinto";\
  if header :contains ["resent-from"] ["User-1"] {\
  fileinto "testspam";\
  } else {\
  fileinto "spam";};
```

因为可以使用大多数垃圾邮件过滤器软件对结论字符串进行配置，所以您可以根据返回的字符串来指定不同的操作。可以使用匹配的 spamfilter*X*_verdict_*n* 和 spamfilter*X*_action_*n* 选项对来完成此操作。

示例 7。这些匹配的选项对将放弃返回的结论字符串为 remove 的垃圾邮件。

```
spamfilter1_verdict_0=remove
spamfilter1_action_0=data:,discard
```

有关如何指定垃圾邮件结论字符串的说明，请参阅特定的垃圾邮件过滤软件各节。

表 14-2 MTA 垃圾邮件过滤器选项 (option.dat)

用于 Spam Assassin 的 MTA 选项	说明
SpamfilterX_config_file	指定过滤软件 X 配置文件的完整文件路径和名称。 默认值：无
SpamfilterX_library	指定过滤软件 X 共享库的完整文件路径和名称。 默认值：无
SpamfilterX_optional	用于控制是将过滤库 X 报告的某些失败视为临时进程失败还是忽略这些失败。默认值 0 指定垃圾邮件过滤问题将导致临时进程失败。如果将此值更改为 1，则在某些 （可能不是全部）过滤库失败的情况下，系统将跳过垃圾邮件过滤进程。特别是，如果系统阻塞，库代码中没有返回值，则 MTA 的某些部分也可能会阻塞。也可以将此值设置为 -2 和 2。分别与 0 和 1 相同，只是在垃圾邮件过滤器插件报告问题时，这样设置会导致发送系统日志消息。 默认值：0
LDAP_optinX	指定基于用户激活过滤软件 X 所使用的 LDAP 属性名称。这应该是 inetMailUser 对象类中的属性。 属性本身可以具有多个值并区分大小写。对于 SpamAssassin，该属性值应为小写的 spam。 默认值：无

表 14-2 MTA 垃圾邮件过滤器选项 (option.dat)

用于 Spam Assassin 的 MTA 选项	说明
LDAP_domain_attr_optin*X*	指定基于域激活过滤软件 X 所使用的 LDAP 属性名称。它适用于目标域。它与 LDAP_optin 类似，但是应该位于对象类 mailDomain 中。 默认值：无
Spamfilter*X*_null_optin	指定一个字符串，如果发现该字符串为 LDAP_optin*X* 或 LDAP_domain_attr_optin*X* 定义的属性的值，将导致 MTA 如该属性不存在那样运行。也就是说，该字符串禁用了此条目的过滤。有关用法的详细信息，请参见第 396 页的 “指定要过滤的邮件”。 默认值：空字符串。默认情况下，系统将忽略空选定属性。（这是自 iPlanet Messaging Server 5.2 以来的更改，在 iPlanet Messaging Server 5.2 中，空选定属性使用空选定列表触发过滤。可以通过将 spamfilter*X*_null_optin 设置为实际中始终不会出现的字符串来恢复 5.2 版的这种行为。）
Spamfilter*X*_null_action	定义 Sieve 规则，指定当过滤软件 X 返回空值结论时如何处理邮件。使用文件 URL 可以从外部存储 Sieve 表达式。例如：file:///var/opt/SUNWmsgsr/config/null_action.sieve。此外，请勿使用 Sieve 拒收操作拒绝垃圾邮件，因为这样做会向无辜的团体 （其地址曾被用于发送垃圾邮件）发送未传送通知。 默认值：data:,discard;
Spamfilter*X*_string_action	定义 Sieve 规则，指定当结论为字符串时如何处理邮件。使用文件 URL 可以从外部存储 Sieve 表达式。例如：file:///var/opt/SUNWmsgsr/config/null_action.sieve。此外，请勿使用 Sieve reject 操作拒绝垃圾邮件，因为这样做会向无辜的团体 （其服务器曾被用于发送垃圾邮件）发送未传送通知。 默认值：data:,require "fileinto"; fileinto "$U; 其中 $U 是 verdict 返回的字符串。
spamfilter*X*_verdict_*n*	spamfilter*X*_verdict_*n* 和 spamfilter*X*_action_*n* 是匹配的选项对，其中，*n* 是 0 到 9 之间的数字。这些选项使您可以为任意结论字符串指定 Sieve 过滤器。分别将 spamfilter*X*_verdict_*n* 和 spamfilter*X*_action_*n* 设置为结论字符串和 Sieve 过滤器，从而可以实现此操作。其中，*n* 是 0 到 9 之间的整数。例如，通过指定以下选项，某个站点可以使 "reject" 结论导致 sieve 拒收操作： spamfilter1_verdict_*0*=reject spamfilter1_action_*0*=data:,require "reject"; reject "Rejected by spam filter"; 所有 spamfilter*X*_verdict_*n* 选项的默认值和对应的操作选项的默认值均为空字符串。 默认值：无
spamfilter*X*_action_*n*	请参见 spamfilter*X*_verdict_*n*。默认值：无
spamfilter*X*_final	某些过滤库可以执行基于收件人地址的一组操作。 spamfilter*X*_final 可以指定传递到过滤库的收件人地址的类别。设为 0 的值将使用中间地址；设为 1 将发送最终格式的收件人地址。 默认值：0

表 14-2 MTA 垃圾邮件过滤器选项 (option.dat)

用于 Spam Assassin 的 MTA 选项	说明
optin_user_carryover	转发是对垃圾邮件过滤进程的挑战。设想一个用户条目，该条目指定了 forward 传送选项，并且指定了其他用户的转发地址。此外，用户条目还设置选定了某种特定类别的过滤。那么，是否应将过滤应用到已转发的邮件呢？一方面，一个特定用户的正确过滤选择对于另外一个用户来说不一定是正确的选择。另一方面，取消过滤操作可能被视为违反了站点的安全策略。 没有一个在所有情况下均正确的答案。因此，转发邮件时，OPTIN_USER_CARRYOVER 将控制如何将垃圾邮件过滤选定列表从一个用户或别名条目传送到另外一个用户或别名条目。该选项是按位编码的值。不同的位值具有的含义如下： 位 0 （值 1）。每个 LDAP 用户条目无条件地覆盖所有先前活动的用户 / 域选定。 位 1 （值 2）。如果用户的域具有选定属性，则该属性将覆盖所有先前处于活动状态的用户 / 域 / 别名选定。 位 2 （值 4）。如果用户具有选定属性，则该属性将覆盖所有先前处于活动状态的用户 / 域 / 别名选定。 位 3 （值 8）。由 [optin] 非位置参数指定的选定将覆盖所有先前处于活动状态的用户 / 域 / 别名选定。 默认值：0 （如果一个用户具有可以转发到另一个用户的传送选项，则选定将累积起来。此默认值确保了转发时站点安全策略的有效性；其他设置可能不具有此种功能。）

使用 Symantec Brightmail Anti-Spam

Brightmail 解决方案由 Brightmail 服务器和下载到电子邮件服务器的实时反垃圾邮件和反病毒规则更新组成。

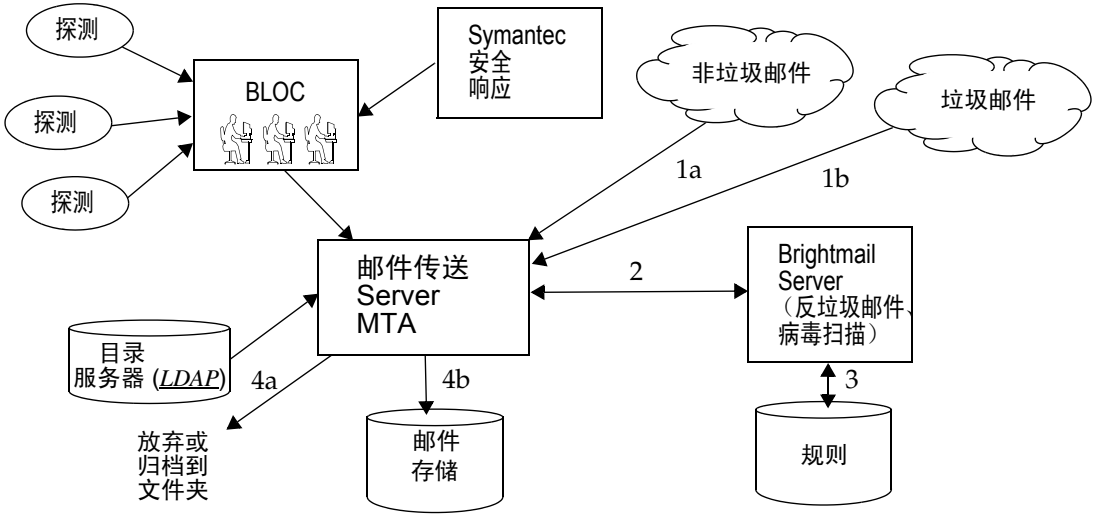
Brightmail 的工作方式

Brightmail 服务器部署在用户站点上。 Brightmail 在 Internet 周围设置了电子邮件探测，用于检测新的垃圾邮件。 Brightmail 技术人员创建了实时阻止此垃圾邮件的自定义规则。还要实时地将这些规则下载到 Brightmail 服务器。 Brightmail 数据库保持更新， Brightmail 服务器将为指定用户或域运行此数据库电子邮件过滤器。

Brightmail 的体系结构

图 14-1 说明了 Brightmail 的体系结构。

图 14-1 Brightmail 和 Messaging Server 体系结构



当 Brightmail 支援和运作中心 (BLOC) 从电子邮件探测接收到垃圾邮件时，操作员将立即创建相应的垃圾邮件过滤规则，该规则将被下载到 Brightmail 用户计算机上。同样， Brightmail 也将发送 Symantec 安全响应实时病毒规则。用户的 Brightmail 服务器将使用这些规则捕捉垃圾邮件和病毒。

MTA 使用 Brightmail SDK 与 Brightmail 服务器通信。 MTA 根据 Brightmail 返回的响应分发邮件。 MTA 收到邮件 (1a) 或 (1b) 后，将把邮件发送到 Brightmail 服务器 (2)。Brightmail 服务器使用其规则和数据来确定邮件是否为垃圾邮件或病毒 (3)，并向 MTA 返回结论。根据该结论，MTA 将 (4a) 放弃邮件或将邮件作为文件保存到文件夹，或 (4b) 将其正常传送到目的地。

由于 Brightmail SDK 是第三方软件，因此我们未将其包含在安装工具包中。必须从 Brightmail Inc. 获得 Brightmail SDK 和服务器软件。 MTA 的配置设置可以判断是否装入 Brightmail SDK 以及装入的位置，以启用 Brightmail 集成。

装入 SDK 后， Brightmail 邮件处理将由若干因素和粒度级别来确定 （Brightmail 用于指定有效处理的术语为**选定**）。这由以下条件指定：

- 是否已经为 Brightmail 启用源通道或目标通道 (`imta.cnf`)
- 是否具有用于选定服务的默认通道 (`imta.cnf`)
- 是否具有基于每个域的选定 (LDAP)
- 是否具有基于每个用户的选定 (LDAP)

对于任何特定的邮件收件人，上述选定项和默认项是相互组合的，即如果已经指定用于垃圾邮件和病毒的默认通道，则无需使用基于每个用户的选定。也就是说，如果系统管理员决定为所有人进行垃圾邮件和病毒的过滤，则无需向用户显示用于垃圾邮件或病毒的选定功能。无法选择退出处理，也就是说，如果用户已经通过系统选项或域选项选定某项服务，则不能说不需要该服务。这还意味着，如果您选定了服务，并且您已经将邮件转发给另一个地址，则该地址将在以您的名义执行完过滤后获得该邮件。

仅提供两种服务，即病毒检测或垃圾邮件检测。 Brightmail 还提供 “内容过滤”服务，但此功能是使用 Sieve 提供的，因此让 Brightmail 进行 Sieve 过滤不具有增值效果。

确定邮件带有病毒后，可以将 Brightmail 服务器配置为清除病毒并将干净的邮件重新提交回 MTA。（由于丢失有关重新提交的干净邮件中的原邮件信息会造成某些不良的负面影响，因此我们建议您不要将 Brightmail 配置为将干净的邮件重新提交回 MTA。）当邮件为垃圾邮件时，从 Brightmail 返回的结论和 Brightmail 中的配置使 MTA 能够确定如何处理该邮件。可以放弃该邮件、归档到文件夹、在主题行上将其标记为垃圾邮件或病毒、传递给 Sieve 规则、正常传送到 INBOX 中，等等。

Brightmail 服务器可以与 MTA 位于同一系统中，也可以位于单独的系统中。事实上，您可以让多个 Brightmail 服务器服务于一个或多个 MTA。 Brightmail SDK 使用 Brightmail 配置文件来确定要使用的 Brightmail 服务器。

Brightmail 要求和性能注意事项

- Brightmail 服务器必须在 Solaris 操作系统中运行。
- 如果 Brightmail 进行垃圾邮件检查和病毒检查两种功能，则 MTA 邮件吞吐量可能会降低 50%。要保持 MTA 吞吐量，可能需要为每个 MTA 配置两个 Brightmail 服务器。
- 尽管 SpamAssassin 可以基于用户执行不同类型的过滤，但是它无法同时对同一邮件应用两组不同的过滤条件。因此， SpamAssassin 仅允许系统范围内的过滤。不可以使用各个用户定制的过滤。

部署 Brightmail

执行以下步骤部署 Brightmail。

- **安装并配置 Brightmail**。请参阅 Brightmail 软件文档或咨询代表，以获得有关安装和配置的信息。第 408 页的 “Brightmail 配置选项”中显示了选定的 Brightmail 配置选项，但最完整并且最新的信息是在 Brightmail 文档中。

- **装入和配置 Brightmail 客户机库**。此操作包括向 MTA 中指定 Brightmail 客户机库 `libbmiclient.so` 和配置文件 `config`。请参见第 395 页的 “装入和配置垃圾邮件过滤软件客户机库”。
- **指定进行垃圾邮件过滤的邮件**。用户、域或通道均可以过滤邮件。请参见第 396 页的 “指定要过滤的邮件”。
- **指定在垃圾邮件上进行的操作**。可以放弃垃圾邮件、将垃圾邮件归档到文件夹或在主题行上将其标记为垃圾邮件，等等。请参见第 401 页的 “指定要对垃圾邮件执行的操作”。
- **根据需要设置其他的 MTA 过滤器配置参数**。请参见第 403 页的 “MTA 垃圾邮件过滤器选项 (option.dat)”。

Brightmail 配置选项

表 14-3 显示了选定的 Brightmail 配置文件选项。可以从 Brightmail 获得 Brightmail 配置文件选项的最完整的列表。选项和值不区分大小写。

表 14-3 选定的 Brightmail 配置文件选项

Brightmail 选项	说明
`blSWPrecedence`	给定的邮件可以有多个结论。此选项指定优先级顺序。因此，如果将此选项指定为 `virus-spam`（结论由连字符 [-] 隔开），则首先对邮件进行病毒处理，然后进行垃圾邮件处理。这是将 Brightmail 和 Sun Java System Messaging Server 结合使用时的推荐设置。
`blSWClientDestinationDefault`	指定如何传送正常邮件 （也就是说，不是垃圾邮件也不是病毒，因此没有结论）。通常您希望正常传送此邮件，因此应指定 `inbox` 作为值。无默认值。
`blSWLocalDomain`	此属性指定被当作本地域的域。此属性可以有多个行，指定多个被当作本地域的域。本地域和外地域用于指定对结论的两种不同处理方法。 请参见以下的 `blSWClientDestinationLocal` 和 `blSWClientDestinationForeign`。例如，您可以指定 `blSWLocalDomain=siroe.com`

表 14-3 选定的 Brightmail 配置文件选项

Brightmail 选项	说明
blSWClientDestinationLocal	此选项指定用于本地域的结论和操作对。通常此选项有两个行，一行用于垃圾邮件，一行用于病毒。值的格式为 verdict|action，例如， blSWClientDestinationLocal=spam|spambox blSWClientDestinationLocal=virus| Brightmail 对 “空”操作 （即 “|”右侧没有值）的默认解释是放弃邮件。因此如果以上示例具有结论 virus，将放弃邮件。如果结论为 spam，以上示例将把邮件作为文件保存到名为 spambox 的文件夹。如果邮件不是垃圾邮件或病毒，则结论不匹配，将根据上述 blSWClientDestinationDefault 设置中的设置正常传送邮件。 使用单独的 Brightmail 服务器或 MTA 服务器时，可以通过使用 Brightmail_verdict_n/Brightmail_action_n/Brightmail_null_action/Brightmail_string_action MTA 选项自定义每个 MTA 进行的操作，以覆盖 Brightmail 服务器返回的操作和结论。在此示例中，可以使用 MTA 中不同的 Brightmail_null_action 来覆盖病毒操作 （放弃病毒邮件），或使用 Brightmail_verdict_0=spambox 和 Brightmail_action_0=data:,require "fileinto";fileinto "Junk"; 将邮件作为文件保存到名为 Junk 而不是 spambox 的文件夹中。
blSWClientDesintationForeign	格式和解释与上述 blSWClientDestinationLocal 相同，但应用于非本地域中的用户。
blSWUseClientOptin	与 Sun Java System Messaging Server 结合使用时，请始终将此选项设置为 TRUE。
blswcServerAddress	格式为 ip:port[,ip:port,...]，用于指定一个或多个 Brightmail 服务器的 IP 地址和端口号

使用 SpamAssassin

本节包含以下小节：

- 第 410 页的 “SpamAssassin 概述”
- 第 410 页的 “SpamAssassin/Messaging Server 操作原理”
- 第 411 页的 “SpamAssassin 要求和使用注意事项”
- 第 412 页的 “部署 SpamAssassin”
- 第 412 页的 “SpamAssassin 配置示例”
- 第 418 页的 “测试 SpamAssassin”
- 第 420 页的 “SpamAssassin 选项”

SpamAssassin 概述

Messaging Server 支持使用 SpamAssassin，一种用于识别垃圾邮件的邮件过滤器免费软件。SpamAssassin 由一个使用 Perl 编写的库和一组可用于将 SpamAssassin 集成到邮件传送系统的应用程序和实用程序组成。

SpamAssassin 通过对邮件标题和主体信息执行一系列测试，从而为每个邮件计算一个分数。测试成功，则返回结论真 （垃圾邮件）；测试失败，则返回结论假 （非垃圾邮件）。该分数为实数，可能为正，也可能为负。分数超过了指定阈值 （通常为 5.0）的邮件被认为是垃圾邮件。 SpamAssassin 结果字符串的示例是：

```
True ; 18.3 / 5.0
```

`True` 表示邮件为垃圾邮件。 `18.3` 为 SpamAssassin 分数。 `5.0` 是阈值。

SpamAssassin 的可配置程度很高。可以随时添加或删除测试，也可以调整现有测试的分数。这都是通过各种配置文件进行的。在 SpamAssassin Web 站点中可以找到有关 SpamAssassin 的详细信息。

调用 Brightmail 垃圾邮件和病毒扫描库的同一机制也可以用于连接到 SpamAssassin `spamd` 服务器。 Messaging Server 中提供的模块的名称为 `libspamass.so`。

SpamAssassin/Messaging Server 操作原理

`spamd` 是 SpamAssassin 的守护程序版本，可以从 MTA 中调用。 `spamd` 侦听套接字上的请求并产生子程序以测试邮件。子程序在处理邮件并返回结果后结束。从理论上讲，分叉应当是有效率的进程，因为代码本身可以在子进程间实现共享。

没有使用 SpamAssassin 安装中的客户机部分 `spamc`。相反，客户机部分的功能是通过名为 `libspamass.so` 的共享库 （Messaging Server 的一部分）来实现的。加载 `libspamass.so` 的方法与加载 Brightmail SDK 的方法相同。

从 MTA 的角度来看，几乎可以在用于垃圾邮件过滤的 SpamAssassin 和 Brightmail 之间进行透明切换。但是并非完全透明，因为这两种程序的功能不同。例如，Brightmail 还可以进行病毒过滤，但是 SpamAssassin 仅用于垃圾邮件过滤。两种软件包返回的结果 （或**结论**）也不同。 SpamAssassin 可以提供分数，而 Brightmail 仅可以提供结论名称，因此这两种软件的配置也有一些差别。

使用与 MTA 集成的 SpamAssassin 时， SpamAssassin 仅返回分数和结论。邮件本身不会被修改。也就是说，必须由 Sieve 脚本来设置诸如添加标题和修改主题行这样的选项。此外， `mode` 选项使您可以指定表示结论的返回字符串。此字符串选项为空字符串、默认字符串、SpamAssassin 结果字符串或 `verdict` 字符串。有关详细信息，请参见第 420 页的表 14-4 。

SpamAssassin 要求和使用注意事项

- SpamAssassin 为免费软件。可以在 http://www.spamassassin.org 上找到该软件和文档。
- 可以调整和配置 SpamAssassin 以使其提供非常准确的垃圾邮件检测。对 SpamAssassin 的调整取决于您和 SpamAssassin 社区。 Messaging Server 不会提供或增强 SpamAssassin 的功能。
- 虽然没有具体的数字，但是 SpamAssassin 似乎比 Brightmail 更多地降低了吞吐量。
- 可以为用户、域或通道启用与 MTA 集成的 SpamAssassin。
- 可以将 SpamAssassin 配置为使用其他联机数据库，例如， Vipul 的 Razor 或分布式校验和信息交换站 (DCC)。
- 虽然 Messaging Server 没有提供安全套接字层 (SSL) 版本的 `libspamass.so`，但是可以建立 SpamAssassin 以使用 openSSL。
- 需要 Perl 5.6 或更高版本。

在哪里运行 SpamAssassin？

SpamAssassin 可以在其自己的单独系统上、单一系统部署中与 Messaging Server 相同的系统上或两层部署中与 MTA 相同的系统上运行。如果在 MTA 和邮件存储之间使用本地邮件传输协议 (LMTP)，则必须从 MTA 中调用过滤。不能从邮件存储中调用过滤。如果在 MTA 和邮件存储之间使用 SMTP，则既可以从 MTA 也可以从邮件存储中调用过滤，并且 SpamAssassin 可以在上述系统或单独的第三方系统中运行。

如果要使用运行了 SpamAssassin 的多个服务器，则必须在这些服务器的前面使用负载平衡器。配置 MTA，使其仅有一个 SpamAssassin 服务器地址。

部署 SpamAssassin

执行以下步骤部署 SpamAssassin。

- **安装并配置 SpamAssassin**。请参阅 SpamAssassin 软件文档，以获得有关安装和配置的信息。另请参见第 420 页的 “SpamAssassin 选项”。
- **装入和配置 SpamAssassin 客户机库**。此操作包括向 MTA 中指定客户机库 `libspamass.so` 和配置文件 （必须创建此文件）。请参见第 395 页的 “装入和配置垃圾邮件过滤软件客户机库”。
- **指定进行垃圾邮件过滤的邮件**。用户、域或通道均可以过滤邮件。请参见第 396 页的 “指定要过滤的邮件”。
- **指定在垃圾邮件上进行的操作**。可以放弃垃圾邮件、将垃圾邮件归档到文件夹或在主题行上将其标记为垃圾邮件，等等。请参见第 401 页的 “指定要对垃圾邮件执行的操作”。
- **根据需要设置其他过滤器配置参数**。请参见第 403 页的 “MTA 垃圾邮件过滤器选项 (option.dat)”。

SpamAssassin 配置示例

本节介绍了一些通用的 SpamAssassin 配置示例：

- 第 413 页的 “将垃圾邮件归档到单独的文件夹”
- 第 414 页的 “向垃圾邮件添加包含 SpamAssassin 分数的标题”
- 第 416 页的 “向主题行添加 SpamAssassin 结果字符串”

注 这些示例使用了许多选项和关键字。有关详细信息，请参见第 400 页的 “垃圾邮件过滤器的 MTA 通道关键字”和第 403 页的 “MTA 垃圾邮件过滤器选项 (option.dat)”。

将垃圾邮件归档到单独的文件夹

本示例将测试传入到本地邮件存储的邮件并将垃圾邮件归档到名为 spam 的文件夹中。可以按照任何顺序来执行前三个步骤。

1. 创建 SpamAssassin 配置文件。

   步骤 2 中指定了此文件的名称和位置。spamassassin.opt 是一个很好的文件名。本文件包含以下各行：

```
host=127.0.0.1
port=2000
mode=0
verdict=spam
debug=1
```

   host 和 port 分别指定运行了 spamd 的系统的名称和 spamd 侦听外来请求的端口。 mode=0 指定如果系统认为邮件为垃圾邮件，则返回一个由 verdict 指定的字符串。 debug=1 就在 SpamAssassin 库中启用调试。有关 SpamAssassin 配置参数的说明，请参见第 420 页的表 14-4 。

2. 向 option.dat 文件添加以下各行：

```
! for Spamassassin
spamfilter1_config_file1=/opt/SUNWmsgsr/config/spamassassin.opt
spamfilter1_library1=/opt/SUNWmsgsr/lib/libspamass.so
spamfilter1_optional=1
spamfilter1_string_action=data:,require "fileinto"; fileinto "$U;
```

   spamfilter1_config_files 指定 SpamAssassin 配置文件。

   spamfilter1_library 指定了 SpamAssassin 共享库。

   spamfilter1_optional=1 指定 spamd 失败时， MTA 继续运行。

   spamfilter1_string_action 指定对垃圾邮件采取 Sieve 操作。

   在本示例中，因为默认值已为 data:,require "fileinto"; fileinto "$U;，所以无需 spamfilter1_string_action。该行指定将垃圾邮件发送到某个文件夹。文件夹的名称是 SpamAssassin 返回的垃圾邮件结论值。spamassassin.opt 中的 verdict 选项指定了 SpamAssassin 返回的值。（请参见步骤 1。）在此示例中，文件夹名称为 spam。

3. 指定要过滤的邮件。

   要过滤传入到本地邮件存储的所有邮件，请通过在 ims-ms 通道中添加 destinationspamfilter*X*optin spam 关键字来更改 imta.cnf 文件。

```
!
! ims-ms
ims-ms defragment subdirs 20 notices 1 7 14 21 28 backoff "pt5m" "pt10m"
"pt30m" "pt1h"  "pt2h" "pt4h" maxjobs 4 pool IMS_POOL fileinto
$U+$S@$D destinationspamfilter1optin spam
ims-ms-daemon
```

4. 重新编译配置并重新启动服务器。只需要重新启动 MTA。无需执行 stop-msg。

```
# imsimta cnbuild
# imsimta restart
```

5. 启动 spamd 守护程序。通常使用以下格式的命令执行此操作：

   ```
   spamd -d
   ```

   spamd 默认为只接受来自本地系统的连接。如果是在不同的系统中运行 SpamAssassin 和 Messaging Server，则需要以下语法：

   spamd -d -i *listen_ip_address* -A *allowed_hosts*

   其中 *listen_ip_address* 是要侦听的地址， *allowed_hosts* 是可以连接到此 spamd 实例的授权的主机或网络 （使用 IP 地址）的列表。

注 0.0.0.0 可以与 -i *listen_ip_address* 结合使用以使 spamd 侦听所有地址。最好侦听所有地址，原因是 spamfilter*X*_verdict_*n* 可以避免在更改系统的 IP 地址时必须更改命令脚本。

向垃圾邮件添加包含 SpamAssassin 分数的标题

此示例将标题 Spam-test:*result string* 添加到已被 SpamAssassin 确定为垃圾邮件的邮件。以下为标题示例：

```
Spam-test:True ; 7.3 / 5.0
```

其中， Spam-test: 是文字，其后的内容为结果字符串。 True 表示邮件为垃圾邮件（false 表示邮件不是垃圾邮件）。 7.3 是 SpamAssassin 分数。 5.0 是阈值。该结果对于设置 Sieve 过滤器非常有用，该过滤器可以对高于某一分数或介于某分数之间的邮件进行归档或放弃。

此外，将 USE_CHECK 设置为 0 会将结论字符串与匹配的 SpamAssassin 测试列表一同返回。请参见第 420 页的表 14-4 中的 USE_CHECK。

1. 指定要过滤的邮件。第 413 页的 “将垃圾邮件归档到单独的文件夹”中的步骤 3 说明了此操作。

2. 创建 SpamAssassin 配置文件。

   使用 spamfilter_configX_file 指定此文件的名称和位置 （见下一步）。其中包含以下几行：

```
host=127.0.0.1
port=2000
mode=1
field=
debug=1
```

   host 和 port 指定运行了 spamd 的系统的名称和 spamd 侦听外来请求的端口。mode=1 指定如果系统发现邮件为垃圾邮件，则返回 SpamAssassin 结果字符串。field= 为 SpamAssassin 结果字符串指定了字符串前缀。在此示例中，由于我们要在 Sieve 脚本中指定字符串前缀，所以无需前缀。 debug=1 用于将在 SpamAssassin 库中启用调试。

3. 向 option.dat 文件添加以下各行：

```
!for Spamassassin
spamfilte1r_config_file=/opt/SUNWmsgsr/config/spamassassin.opt
spamfilter1_library=/opt/SUNWmsgsr/lib/libspamass.so
spamfilter1_optional=1
spamfilter1_string_action=data:,require ["addheader"];addheader "Spam-test:$U";
```

   如前面示例所述，前三个选项指定了 SpamAssassin 配置文件、共享库以及共享库失败时 MTA 继续运行。下面一行：

   spamfilter1_string_action=data:,require ["addheader"];addheader "Spam-test:$U";

   指定了要向垃圾邮件添加的标题。标题带有文字前缀 Spam-text:，后跟 SpamAssassin 返回的字符串。因为已在步骤 2 中指定了 mode=1，所以将返回 SpamAssassin 结果字符串。例如：True; 7.3/5.0

4. 重新编译配置，重新启动服务器并启动 spamd 守护程序。

   请参见第 413 页的 “将垃圾邮件归档到单独的文件夹”。

向主题行添加 SpamAssassin 结果字符串

通过向主题行添加 SpamAssassin 结果字符串，用户可以确定是否要阅读带有 SpamAssassin 分数的邮件。例如：

```
Subject:[SPAM True ; 99.3 / 5.0] Free Money At Home with Prescription Xanirex!
```

请注意，如果将 USE_CHECK 设置为 0，则可以将结论字符串与匹配的 SpamAssassin 测试列表一同返回 （请参见第 420 页的表 14-4 中的 USE_CHECK）。因为此列表可能会非常长，所以最好将 USE_CHECK 设置为 1。

1. 指定要过滤的邮件。请参见第 413 页的 “将垃圾邮件归档到单独的文件夹”中的步骤 3。

2. 创建 SpamAssassin 配置文件。

   第 413 页的 “将垃圾邮件归档到单独的文件夹”中介绍了此步骤。 mode=1 指定如果系统发现邮件为垃圾邮件，则返回 SpamAssassin 结果字符串。

```
host=127.0.0.1
port=2000
mode=1
debug=1
```

   host 和 port 指定运行了 spamd 的系统的名称和 spamd 侦听外来请求的端口。 mode=1 指定如果邮件为垃圾邮件，则返回 SpamAssassin 结果字符串。 debug=1 将在 SpamAssassin 库中启用调试。

3. 向 option.dat 文件添加以下各行：

```
!for Spamassassin
spamfilter1_config_file=/opt/SUNWmsgsr/config/spamassassin.opt
spamfilter1_library=/opt/SUNWmsgsr/lib/libspamass.so
spamfilter1_optional=1
spamfilter1_string_action=data:,addtag "[SPAM detected:$U]";
```

   如前面示例所述，前三个选项指定了 SpamAssassin 配置文件、共享库以及共享库失败时 MTA 继续运行。下面一行

   ```
   spamfilter1_string_action=data:,addtag "[SPAM detected $U]";
   ```

指定了要向 Subject: 行添加标记。此标记的文字前缀为 SPAM detected，后跟 field 字符串 （默认值为：Spam-Test），再后跟由 SpamAssassin 返回的 "[*result string*]"。因为已在步骤 2 中指定了 mode=1，所以将返回 SpamAssassin 结果字符串。因此，主题行将类似以下内容：

```
Subject: [SPAM detected Spam-Test: True ; 11.3 / 5.0] Make Money!
```

也可以同时使用 addheader 和 addtag。

```
spamfilter1_string_action=data:,require ["addheader"];addtag "[SPAM
detected $U]";addheader "Spamscore: $U";
```

以获得如下邮件：

```
Subject: [SPAM detected Spam-Test: True ; 12.3 / 5.0] Vigaro Now!
Spamscore: Spam-Test: True ; 12.3 / 5.0
```

设置 spamassassin.opt 中的 field= 可以删除 Spam-Test 的默认值。将返回以下较干净的邮件：

```
Subject: [SPAM True ; 91.3 / 5.0] Vigaro Now!
Spamscore: True ; 91.3 / 5.0
```

4. 重新编译配置，重新启动服务器并启动 spamd 守护程序。

请参见第 413 页的 “将垃圾邮件归档到单独的文件夹”。

测试 SpamAssassin

要测试 SpamAssassin，请首先在 spamassassion.opt 文件中设置 debug=1。您不必在 imta.cnf 中启用特定于通道的 master_debug 或 slave_debug。然后，将测试邮件发送给测试用户。 *msg_svr_base*/data/tcp_local_slave.log* 文件应当具有类似于以下内容的行：

```
15:15:45.44: SpamAssassin callout debugging enabled; config
/opt/SUNWmsgsr/config/spamassassin.opt
     15:15:45.44: IP address 127.0.0.1 specified
     15:15:45.44: Port 2000 selected
     15:15:45.44: Mode 0 selected
     15:15:45.44: Field "Spam-Test: " selected
     15:15:45.44: Verdict "spam" selected
     15:15:45.44: Using CHECK rather than SYMBOLS
     15:15:45.44: Initializing SpamAssassin message context
     ...
     15:15:51.42: Creating socket to connect to SpamAssassin
     15:15:51.42: Binding SpamAssassin socket
     15:15:51.42: Connecting to SpamAssassin
     15:15:51.42: Sending SpamAssassin announcement
     15:15:51.42: Sending SpamAssassin the message
     15:15:51.42: Performing SpamAssassin half close
     15:15:51.42: Reading SpamAssassin status
     15:15:51.67: Status line: SPAMD/1.1 0 EX_OK
     15:15:51.67: Reading SpamAssassin result
     15:15:51.67: Result line: Spam: False ; 1.3 / 5.0
     15:15:51.67: Verdict line: Spam-Test: False ; 1.3 / 5.0
     15:15:51.67: Closing connection to SpamAssassin
     15:15:51.73: Freeing SpamAssassin message context
```

如果日志文件没有包含与以上内容类似的行，或者未运行 spamd，则将最后的句点 (.) 发送到 SMTP 服务器后， SMTP 对话框中将返回以下错误消息：

```
452 4.4.5 Error writing message temporaries - Temporary scan failure:End
message status = -1
```

此外，如果在 option.dat 中设置了 spamfilter1_optional=1 （强烈推荐），则将接受邮件而不会过滤邮件。就好像没有启用垃圾邮件过滤一样，并且 tcp_local_slave.log* 中将显示以下内容：

```
15:35:15.69: Creating socket to connect to SpamAssassin
15:35:15.69: Binding SpamAssassin socket
15:35:15.69: Connecting to SpamAssassin
15:35:15.69: Error connecting socket: Connection refused
15:35:15.72: Freeing SpamAssassin message context
```

在 SMTP 服务器接收到整个邮件之后 （也即，最后的 “.” 发送到 SMTP 服务器之后），在 SMTP 服务器向发件人确认它已收到邮件之前，系统将调用 SpamAssassin。

另一项测试是使用诸如 Mail-SpamAssassin-2.60 目录中的 sample-spam.txt 来发送范例垃圾邮件。此邮件中包含以下特殊的文本字符串：

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

对应的 tcp_local_slave.log* 包含了类似下面的内容：

```
16:00:08.15: Creating socket to connect to SpamAssassin
16:00:08.15: Binding SpamAssassin socket
16:00:08.15: Connecting to SpamAssassin
16:00:08.15: Sending SpamAssassin announcement
16:00:08.15: Sending SpamAssassin the message
16:00:08.15: Performing SpamAssassin half close
16:00:08.15: Reading SpamAssassin status
16:00:08.43: Status line: SPAMD/1.1 0 EX_OK
16:00:08.43: Reading SpamAssassin result
16:00:08.43: Result line: Spam: True ; 1002.9 / 5.0
16:00:08.43: Verdict line: Spam-Test: True ; 1002.9 / 5.0
16:00:08.43: Closing connection to SpamAssassin
16:00:08.43: Mode 0 verdict of spam
16:00:08.43: Mode 0 verdict of spam
16:00:08.47: Freeing SpamAssassin message context
```

mail.log_current 文件中的对应条目如下所示。请注意目标地址的 +spam 部分，该部分表示将邮件归档到名为 spam 的文件夹中。

```
15-Dec-2003 15:32:17.44 tcp_intranet ims-ms E 1 morchia@siroe.com rfc822;morchia
morchia+spam@ims-ms-daemon
15-Dec-2003 15:32:18.53 ims-ms D 1 morchia@siroe.com rfc822;morchia
morchia+spam@ims-ms-daemon
```

SpamAssassin 选项

本节包含了 SpamAssassin 选项表。

表 14-4 SpamAssassin 选项 (spamassassin.opt)

选项	说明	默认值
调试	指定是否在 libspamass.so 中启用调试。对 spamd 本身的调试是由调用 spamd 的命令行控制的。设置为 0 或 1。	0
field	指定 SpamAssasin 结果的字符串前缀。 SpamAssassin 结果类似于如下所示： Spam-Test: False ; 0.0 / 5.0 Spam-Test: True ; 27.7 / 5.0 field 选项提供更改结果中 Spam-Test 部分的方法。请注意，如果指定了空 field 值，“:”将被删除。 如果将 USE_CHECK 设置为 0，则结果字符串将类似于以下字符串： Spam-test: False ; 0.3 / 4.5 ; HTML_MESSAGE,NO_REAL_NAME Spam-test: True ; 8.8 / 4.5 ; NIGERIAN_BODY, NO_REAL_NAME,PLING_PLING,RCVD_IN_SBL,SUBJ_ALL_CAPS	“Spam-test”
host	运行 spamd 的系统的名称。	localhost

表 14-4 SpamAssassin 选项 (spamassassin.opt)

选项	说明	默认值
mode	控制 SpamAssassin 过滤器结果向结论信息的转换，即在处理邮件后指定被返回的结论信息。可以使用以下四种模式。有关详细解释，请参见第 422 页的“SpamAssassin mode 选项”。 0 — 如果邮件是垃圾邮件，则返回**结论字符串**（由 verdict 选项指定）。使用 MTA 选项 spamfilter*X*_string_action 来指定返回 verdict 字符串时要执行的操作。如果 verdict 选项 （定义如下）为空或未指定，并且邮件是垃圾邮件，则返回**空结论**。使用 MTA 选项 spamfilter*X*_null_action 来指定返回空结论时要执行的操作。 如果不是垃圾邮件，则返回 *SpamAssassin* **默认的结果字符串**。（默认结论始终意味着不采取任何操作并照常传送。） 1 — 如果发现邮件为垃圾邮件，则返回 SpamAssassin **结果字符串**。如果不是垃圾邮件，则返回 *SpamAssassin* **默认的结果字符串**。（再次说明，默认结论始终意味着不采取任何操作并照常传送。） SpamAssassin 结果字符串与下面字符串类似： `True; 6.5 / 7.3` 2 — 与 mode 1 相同，但是返回 SpamAssassin 结果字符串 （不管邮件是否为垃圾邮件）。从不返回默认结论或空结论，并且从未使用 verdict 选项。 3 — 如果邮件是垃圾邮件，则返回 SpamAssassin 结果字符串；如果不是，则返回由 verdict 选项指定的 verdict 字符串。可以通过使用 spamfilter*X*_verdict_*n* 和 spamfilter*X*_action_*n* 匹配选项对来控制针对 SpamAssassin 结果字符串所采取的操作。可以通过使用 spamfilter*X*_string_action 来控制针对 verdict 字符串所采取的操作。	0
port	指定 spamd 侦听外来请求的端口号。	783
USE_CHECK	1 — spamd CHECK 命令将用于返回 SpamAssassin 分数。 0 — 使用 SYMBOLS 命令，该命令将返回分数和匹配的 SpamAssassin 测试列表。在 2.55 以前的 SpamAssassin 版本中，使用此选项可能会导致系统挂起或其他问题。请参见上述 field。	
SOCKS_HOST	字符串。指定中间 SOCKS 服务器的名称。如果指定了此选项，则间接通过指定的 SOCKS 服务器建立 ICAP 连接。	""
SOCKS_PORT	指定运行中间 SOCKS 服务器的端口。	1080
SOCKS_PASSWORD	指定通过 SOCKS 服务器建立连接所使用的密码 （字符串）。是否需要用户名 / 密码取决于 SOCKS 服务器配置。	""
SOCKS_USERNAME	指定通过 SOCKS 服务器建立连接所使用的用户名 （字符串）。	""
verdict	指定用于 MODE 0 的结论字符串。	""

SpamAssassin mode 选项

处理完邮件后， SpamAssassin 将确定邮件是否为垃圾邮件。 mode 使您可以指定表示结论的返回字符串。此字符串选项为空字符串、默认字符串、SpamAssassin 结果字符串或使用 verdict 选项指定的 verdict 字符串。（请注意，**默认字符串**既不是空字符串、SpamAssassin 结果字符串，也不是由 verdict 指定的字符串，而是其他的不可配置的结果字符串。）下表概述了 mode 操作。

表 14-5 针对 SpamAssassin mode 选项返回的字符串

verdict 设置	是否为垃圾邮件?	mode=0	mode=1	mode=2	mode=3
verdict="" （未设置）	是	空	SpamAssassin 结果	SpamAssassin 结果	SpamAssassin 结果
	否	默认字符串	默认字符串	SpamAssassin 结果	默认字符串
verdict= 字符串	是	verdict 字符串	SpamAssassin 结果	SpamAssassin 结果	SpamAssassin 结果
	否	默认字符串	默认字符串	SpamAssassin 结果	verdict 字符串

第一列表示是否设置了 verdict 选项。第二列表示邮件是否为垃圾邮件。 mode 列表示针对各种 mode 返回的字符串。例如，如果未设置 verdict，并将 mode 设置为 0，且邮件不是垃圾邮件，则返回默认字符串。如果将 verdict 设置为 YO SPAM!，并将 mode 设置为 0，且邮件是垃圾邮件，则返回 YO SPAM! 字符串。

使用 Symantec Anti-Virus Scanning Engine (SAVSE)

本节除了介绍如何部署 SAVSE 之外，还介绍了如何部署其他支持 ICAP 的反垃圾邮件 / 反病毒程序。本节包含以下小节：

- 第 423 页的 “SAVSE 概述”
- 第 423 页的 “SAVSE 要求和使用注意事项”
- 第 424 页的 “部署 SAVSE”

- 第 424 页的 “SAVSE 配置示例”
- 第 426 页的 “SAVSE 选项”

SAVSE 概述

SAVSE 是 TCP/IP 服务器应用程序和通信应用程序编程接口 (API)，它提供了病毒扫描服务。SAVSE 是专门为保护通过网络基础设施设备来服务或存储在网络基础设施设备中的通信而设计的，它将检测并防止包括移动代码和压缩文件格式在内的所有主要文件类型中的病毒、蠕虫和特洛伊木马。有关详细信息，请参阅 Symantec 的 Web 站点。

注 Messaging Server 仅支持 SAVSE 的扫描功能，不支持修复或删除功能。

SAVSE 要求和使用注意事项

SAVSE 是获得 Symantec 的单独许可的产品。

仅支持扫描模式，而不支持 SAVSE 配置中的扫描与修复模式或者扫描与删除模式。

在哪些系统中运行 SAVSE？

SAVSE 或其他支持 ICAP 的服务器可以在其自己的单独系统上、单一系统部署中与 Messaging Server 相同的系统上或两层部署中与 MTA 相同的系统上运行。如果在 MTA 和邮件存储之间使用本地邮件传输协议 (LMTP)，则必须从 MTA 中调用过滤。不能从邮件存储中调用过滤。如果在 MTA 和邮件存储之间使用 SMTP，则既可以从 MTA 也可以从邮件存储中调用过滤，并且 SpamAssassin 可以在上述系统或单独的第三方系统中运行。

如果要使用运行了 SAVSE 的多个服务器，则必须在这些服务器的前面使用负载平衡器。配置 MTA，使其仅有一个 SpamAssassin 服务器地址。

部署 SAVSE

执行以下步骤部署 SAVSE。

- **安装并配置 SAVSE**。请参阅 Symantec 软件文档，以获得有关安装和配置的信息。另请参见第 426 页的 “SAVSE 选项”。
- **装入和配置 SAVSE 客户机库**。此操作包括向 MTA 中指定客户机库 `libicap.so` 和配置文件 （必须创建此文件）。请参见第 395 页的 “装入和配置垃圾邮件过滤软件客户机库”。
- **指定进行病毒过滤的邮件**。用户、域或通道均可以过滤邮件。请参见第 396 页的 “指定要过滤的邮件”。
- **指定在病毒邮件上进行的操作**。可以放弃病毒、将病毒归档到文件夹或在主题行上将其标记为病毒，等等。请参见第 401 页的 “指定要对垃圾邮件执行的操作”。
- **根据需要设置其他过滤器配置参数**。请参见第 403 页的 “MTA 垃圾邮件过滤器选项 (option.dat)”。

SAVSE 配置示例

以下示例将测试传入到本地邮件存储的邮件并放弃附带病毒的邮件。可以按照任何顺序来执行前三个步骤。

1. 创建 SAVSE 配置文件。

   步骤 2 中指定了此文件的名称和位置。此处使用的名称为 `SAVSE.opt`。此文件的示例如下所示：

```
host=127.0.0.1
port=1344
mode=0
verdict=virus
debug=1
```

   `host` 和 `port` 分别指定运行 SAVSE 程序的系统的名称和侦听外来请求的端口（SAVSE 的默认值为 1344）。`mode=0` 指定如果系统认为邮件带有病毒，则返回一个由 `verdict` 指定的字符串 （本示例中该字符串为 `virus`）。`debug=1` 启用调试。有关 ICAP 配置参数的说明，请参见第 426 页的表 14-6 。

2. 创建 option.dat 文件。示例：

```
! for Symantex Anti-virus Scan Engine
spamfilter1_config_file=/opt/SUNWmsgsr/config/SAVSE.opt
spamfilter1_library=/opt/SUNWmsgsr/lib/libicap.so
spamfilter1_optional=1
spamfilter1_string_action=data:,discard
```

spamfilter1_config_files 指定了 SAVSE 配置文件。

spamfilter1_library 指定了 SAVSE 共享库的位置。

spamfilter1_optional=1 指定如果 SAVSE 程序失败时， MTA 将继续运行。

spamfilter1_string_action 指定对垃圾邮件采取 Sieve 操作。该值指定带有病毒的邮件将被放弃。因为这是默认值，所以无需指定，除非要更改该值。

3. 指定要过滤的邮件。

要过滤传入到本地邮件存储的所有邮件，请通过在 ims-ms 通道中添加 destinationspamfilter1optin spam 关键字来更改 imta.cnf 文件：

```
!
! ims-ms
ims-ms defragment subdirs 20 notices 1 7 14 21 28 backoff "pt5m" "pt10m"
"pt30m" "pt1h"  "pt2h" "pt4h" maxjobs 4 pool IMS_POOL fileinto
$U+$S@$D destinationspamfilter1optin virus
ims-ms-daemon
```

4. 重新编译配置并重新启动服务器。只需要重新启动 MTA。无需执行 stop-msg。

```
# imsimta cnbuild
# imsimta restart
```

5. 请确保已启动 SAVSE。

SAVSE 应已自动启动，但是如果没有自动启动，则可使用与下面的命令类似的命令：**/etc/init.d/symcscna start**

其他可能的配置

将 mode 设置为 0 可以与 spamfilterX_null_option 一起使用来进行其他操作 （例如，将被确定为垃圾邮件的邮件归档到特定文件夹）。例如：

```
spamfilter1_null_option=data:,require "fileinto"; fileinto "VIRUS";
```

请注意，大多数情况下最好不要将被感染的邮件归档到一个文件夹中。

将 mode 设置为 1 可用于启动一个操作。例如，可以在拒绝邮件中包含垃圾邮件检查结果，只需将 MTA 中的 mode 设置为 1 并将 spamfilterX_string_action 选项设置如下：

```
spamfilter1_string_action=data:,require "reject"; reject "Message contained
a virus [$U]";
```

如 fileinto，最好不要使用 reject 操作来处理病毒，因为它会将病毒发回给发件人。

还可以通过在 option.dat 文件中添加一行，来将标记添加至垃圾邮件标题。示例：

```
spamfilter1_string_action=data:,addtag "[SPAM detected!]";
```

在只需要进行操作而无需考虑邮件是否已被确认带有病毒的情况下，可以将 mode 设置为 2。随后可以被测试的标题字段的添加是明显的 mode 2 应用程序：

```
spamfilterX_string_action=data:,require ["addheader"];addheader "$U"
```

SAVSE 选项

SAVSE 选项文件是更为普通的 ICAP 选项文件。它的名称和位置由 option.dat 中的 spamfilterX_config_file 进行设置。它由 option=value 格式的行组成。必须设置的选项是 HOST。必须将其设置为运行 ICAP 过滤服务器的系统的名称。必须设置此选项，即使 ICAP 服务器正在本地主机上运行。选项文件如下所示：

表 14-6 ICAP 选项

选项	说明	默认值
调试	从 ICAP 界面模块启用或禁用调试输出。 0 或 1。	0
field	指定 ICAP 结果的前缀。 SAVSE 结果字符串类似于如下所示： Virus-Test: False Virus-Test: True; W32.Mydoom.A@mm.enc 此选项提供了一种更改结果的 Virus-Test: 部分的方法。请注意，如果指定了空 field 值，“:”将被删除。	Virus-test

表 14-6 ICAP 选项

选项	说明	默认值
host	运行 ICAP 过滤服务器的系统的名称	localhost

mode	控制 ICAP 过滤器结果向结论信息的转换，即在处理邮件后指定被返回的字符串信息。可以使用以下四种模式。有关详细解释，请参见第 428 页的 “ICAP mode 选项”
	
	0 — 如果邮件包含病毒，则返回**结论字符串** （由 verdict 选项指定）。使用 MTA 选项 spamfilter*X*_string_action 来指定返回 verdict 字符串时要执行的操作。如果 verdict 选项为空或未指定，则返回**空结论**。如果，使用 MTA 选项 spamfilter*X*_null_action 可以指定返回结论为空并要覆盖放弃邮件的默认操作时要采取的操作。
	
	如果邮件不带有病毒，则返回默认字符串。默认字符串是不可配置的，并且始终意味着不采取任何操作并照常传送。
	
	1 — 如果发现邮件包含病毒，则返回 ICAP **结果字符串**。如果邮件不带有病毒，则返回默认字符串。默认字符串始终意味着不采取任何操作并照常传送。以下是两个 ICAP 结果字符串的示例：
	
	`VIRUS TEST: FALSE`
	`VIRUS-TEST: TRUE; W32.Mydoom.A@mm.enc`
	
	2 — 无条件地返回 ICAP 结果字符串；从不返回默认或空结论，并且从不使用 verdict 选项。此设置可用于只需要进行操作而无需考虑邮件是否已被确定为带有病毒。随后可以被测试的标题字段的添加是明显的 mode 2 应用程序：
	
	`spamfilterX_string_action=data:,require ["addheader"];addheader "$U"`
	
	3 — 如果发现邮件包含病毒，则返回 ICAP 结果字符串；如果未发现病毒，则返回由 verdict 选项指定的 verdict 字符串。此设置用于在发现病毒时进行一种操作；而在未发现病毒时进行另一种操作。您可以通过使用 spamfilter*X*_verdict_*n* 和 spamfilter*X*_action_*n* 匹配选项对来控制针对 ICAP 结果字符串所采取的操作。可以通过使用 spamfilter*X*_string_action 来控制针对 verdict 字符串所采取的操作。
		0

port	指定运行 ICAP 服务器的端口号。	1344
SOCKS_HOST	字符串。指定中间 SOCKS 服务器的名称。如果指定了此选项，则间接通过指定的 SOCKS 服务器建立 ICAP 连接。	""
SOCKS_PORT	整数。指定运行中间 SOCKS 服务器的端口。	1080
SOCKS_PASSWORD	字符串。指定通过 SOCKS 服务器建立连接所使用的密码。是否需要用户名 / 密码取决于 SOCKS 服务器配置。	""
SOCKS_USERNAME	字符串。指定通过 SOCKS 服务器建立连接所使用的用户名。	""
verdict	指定用于 MODE 0 和 3 的结论字符串。	""

ICAP mode 选项

处理完邮件后，与 SASVE 相同，ICAP 反病毒程序将确定邮件是否带有病毒。mode 使您可以指定由 ICAP 程序返回的用来表示结论的字符串。字符串选项为**空字符串**、**默认字符串**、*ICAP* **结果字符串**或 verdict **字符串**（使用 verdict 选项指定）。请注意，**默认字符串**既不是空字符串、ICAP 结果字符串，也不是由 verdict 指定的字符串，而是程序返回的其他不可配置的结果字符串。）下表概述了 mode 操作。

表 14-7 针对 ICAP mode 选项返回的结论字符串

verdict 设置	**是否包含病毒?**	**mode=0**	**mode=1**	**mode=2**	**mode=3**
verdict=""（未设置）	是	空	ICAP 结果	ICAP 结果	ICAP 结果
	否	默认字符串	默认字符串	ICAP 结果	默认字符串
verdict= 字符串	是	verdict 字符串	ICAP 结果	ICAP 结果	ICAP 结果
	否	默认字符串	默认字符串	ICAP 结果	verdict 字符串

第一列表示是否设置了 verdict 选项。第二列表示邮件是否包含病毒。 mode 列表示针对各种 mode 返回的字符串。例如，如果未设置 verdict，并将 mode 设置为 0，且邮件不带有病毒，则 ICAP 程序返回默认字符串。如果将 verdict 设置为 WARNING VIRUS!，并将 mode 设置为 0，且邮件带有病毒，则 ICAP 程序返回字符串 WARNING VIRUS!

支持 Sieve 扩展

除了标准的 Sieve 功能之外， Messaging Server 还提供了许多扩展支持，包括 addheader、 addtag、 spamtest 和 spamadjust。第 414 页的 “向垃圾邮件添加包含 SpamAssassin 分数的标题”和第 416 页的 “向主题行添加 SpamAssassin 结果字符串”中介绍了 addheader 和 addtag，此处介绍了 spamtest 和 spamadjust。

这些扩展操作使管理员可以设置不同的阈值，并可以设置将覆盖 SpamAssassin 结论的空白列表。甚至可以将二者组合以产生不同的阈值，这取决于谁发送了特定邮件。 spamadjust 是非标准操作。 ftp://ftp.isi.edu/in-notes/rfc3685.txt 中介绍了 spamtest。

使用带有 “i;ascii-numeric”比较器的 Sieve [RELATIONAL] 扩展操作， spamtest 可以用于将 SpamAssassin 分数与特定值进行比较。 SpamAssassin 分数通常为实数，但是 spamtest 首先将分数舍入到最接近的整数，从而将强制此分数为介于 0 和 10 之间的整数值。 0 以下的值被强制为 0， 10 以上的值被强制为 10。最后，附加上由 Messaging Server 维护的文本字符串就可以产生 spamtest 测试可以理解的测试字符串。

spamadjust 用于调整当前的垃圾邮件分数。此操作采用了一个字符串参数，该参数已扫描为实数值。此值用于调整当前的垃圾邮件分数。整个字符串也将附加到当前的分数文本字符串。在以下所示的示例中，该字符串为 "undisclosed recipients"。

可以执行多次 spamadjust 操作；每次操作的结果都将添加到当前分数中。再次说明，分数值始终从 0 开始。允许使用已签名的数字值，可以降低当前的分数，也可以增加当前的分数。 spamadjust 没有 require 分句；但是应当列出 spamtest 扩展操作。

例如， spamadjust 的 SpamAssassin MODE 的可能用法设置为 2：

```
spamfilterX_string_action=data:,require ["spamtest"];spamadjust "$U";
```

系统级别的 Sieve 过滤器将检查特定类型的标题，如果找到，则将 SpamAssassin 值增加 5，从而可以修改 SpamAssassin 分数。

```
spamfilter1_string_action=require "spamtest";                                    \
if header :contains ["to", "cc", "bcc", "resent-to", "resent-cc", "resent-bcc"]  \
                    ["<undisclosed recipients>", "undisclosed.recipients"]       \
{spamadjust "+5 undisclosed recipients";}
```

最后，用户级别的 Sieve 脚本可以测试结果值、放弃确定为垃圾邮件的邮件、归档可能为垃圾邮件的邮件，并且使来自本地域地址的邮件可以通过以下语句传递：

```
spamfilter1_string_action=require ["spamtest", "relational",  \
"comparator-i;ascii-numeric", "fileinto"];                    \
if anyof (address :matches "from" ["*@siroe.com",             \
                                   "*@*.siroe.com"])          \
    {keep;}                                                   \
elsif spamtest :value "ge" :comparator "i;ascii-numeric" "8" \
    {discard;}                                                \
elsif spamtest :value "ge" :comparator "i;ascii-numeric" "5" \
    {fileinfo "spam-likely";}                                 \
else                                                          \
   {keep;}
```

第 15 章

LMTP 传送

Sun Java System Messaging Server MTA 可以在使用多层邮件传送服务器部署的情况下使用 LMTP （本地邮件传输协议，在 RFC 2033 中定义）来传送到邮件存储。在这些情况下，您使用外来中继和后端邮件存储时，中继将负责地址扩展和传送方法 （例如自动回复和转发），还负责邮递列表扩展。过去传送到后端存储的操作已经通过 SMTP，这需要后端系统在 LDAP 目录中再次查找收件人地址，从而使用 MTA 的整个方法。为了快速而高效的工作， MTA 可以使用 LMTP （而不是 SMTP）将邮件传送到后端存储。Sun Java System Messaging Server 的 LMTP 服务器不会用作通用 LMTP 服务器，而是用作中继和后端邮件存储之间的专用协议。为了简化讨论，将使用涉及两层部署的示例。

注 按照设计， LMTP 用于多层部署。无法将 LMTP 用于单系统部署。此外， Messaging Server 的已实现的 LMTP 服务没有被设计为与其他 LMTP 服务器或其他 LMTP 客户机结合使用。

本章由以下各节组成：

- 第 432 页的 “LMTP 传送功能”
- 第 433 页的 “不带有 LMTP 的两层部署中的邮件传送处理”
- 第 435 页的 “带有 LMTP 的两层部署中的邮件传送处理”
- 第 436 页的 “LMTP 概述”
- 第 445 页的 “要执行的 LMTP 协议”
- 第 437 页的 “配置 LMTP 传送”

LMTP 传送功能

MTA 的 LMTP 服务器能够更有效地传送到后端邮件存储，因为它具有以下功能：

- 减少后端存储中的负载。

  因为中继是横向可伸缩的，而后端存储不是，所以将尽可能多的处理推向中继是很好的操作。

- 减少 LDAP 服务器上的负载。

  LDAP 基础结构通常是大型邮件传送部署中的一个限制因素。

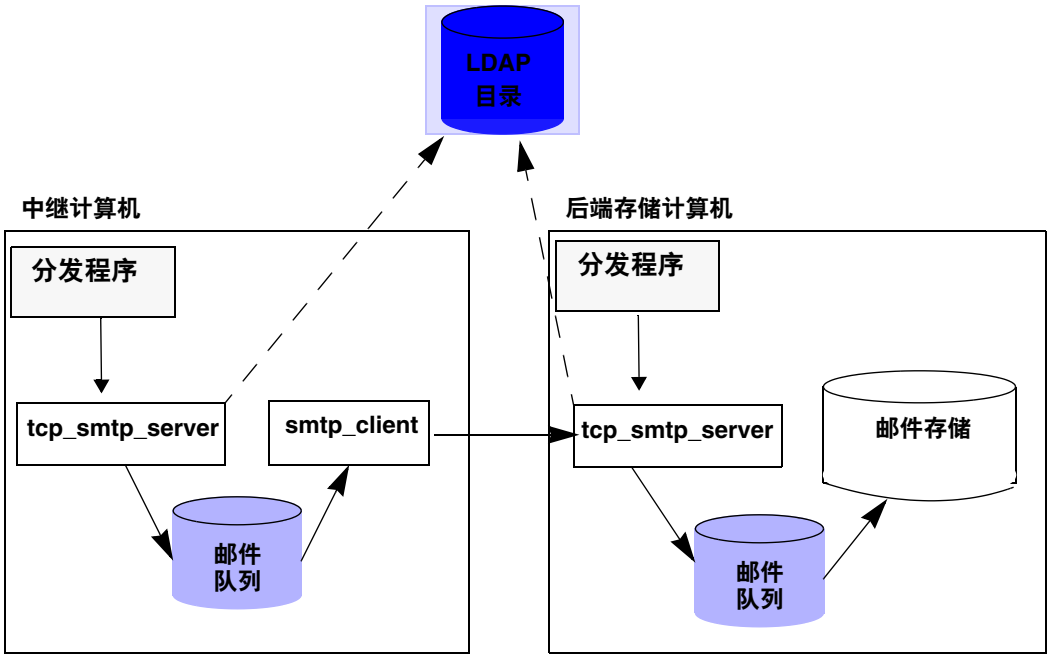
- 减少邮件队列的数目。

  对于邮件传送部署的管理员来说，在中继和后端存储上均存在队列将使查找丢失的邮件更困难。

不带有 LMTP 的两层部署中的邮件传送处理

图 15-1 以图解形式显示了不带有 LMTP 的两层部署方案中邮件处理的以下说明。

图 15-1 不带有 LMTP 的两层部署



不带有 LMTP 的情况下，在存储系统的前面带有中继的两层部署中，外来邮件的处理从 SMTP 端口（由中继计算机上的分发程序选取并传递到 `tcp_smtp_server` 进程）上的连接开始。此进程对外来邮件执行了一系列操作，包括：

- 在目录中查找用户
- 确定用户是否在由此电子邮件部署托管的域内
- 确定用户是否为该域中的有效用户
- 将信封地址重写为 `@mailhost:user@domain`
- 排入邮件以传送到邮件主机

然后 smtp_client 进程从队列中选取邮件消息并将其发送到邮件主机。在邮件主机上，将发生某些非常类似的处理。分发程序将选取 SMTP 端口上的一个连接，并将其传递到 tcp_smtp_server 进程。此进程对邮件执行了一系列操作，包括：

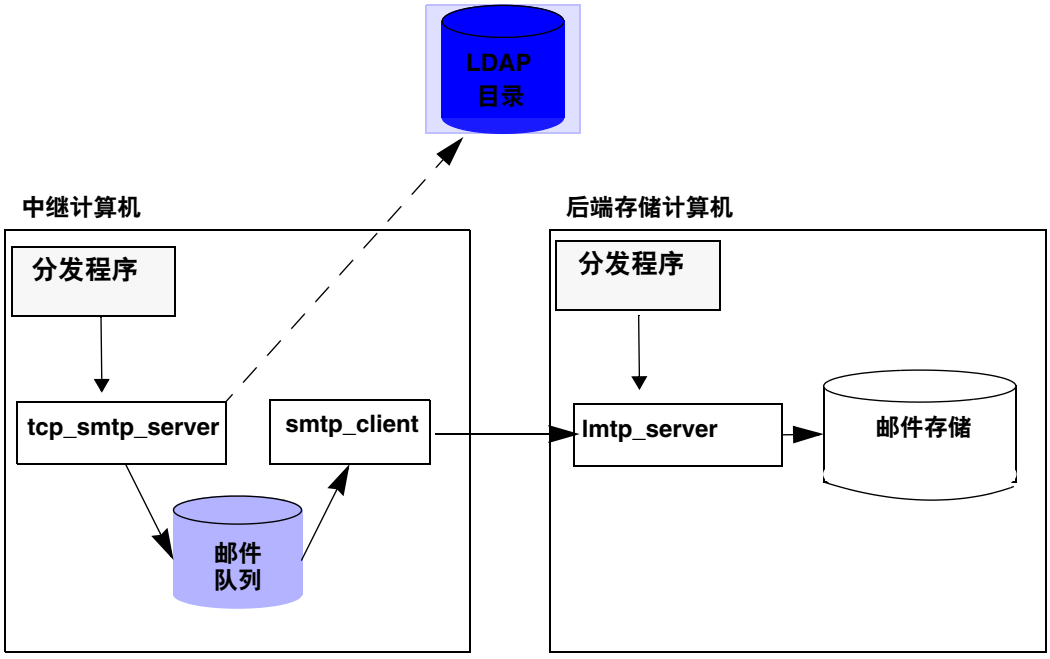
- 在目录中查找用户
- 确定用户是否在由此电子邮件部署托管的域内
- 确定用户是否为该域中的有效用户
- 重写信封地址以将邮件定向到 ims_ms 通道
- 排入邮件以传送到存储

然后 ims_ms 进程选取邮件消息并尝试将其传送到存储。在此方案中，执行了两次排入处理，并且每个 MTA 均执行一次 LDAP 查找。

带有 LMTP 的两层部署中的邮件传送处理

图 15-2 以图解形式显示了带有 LMTP 的两层部署方案中邮件处理的以下说明。

图 15-2 带有 LMTP 的两层部署



LMTP 就位的情况下，分发程序将选取中继计算机的 SMTP 端口上的一个连接，并将其传递到 `tcp_smtp_server` 进程。此进程对外来邮件执行了一系列操作，包括：

- 在目录中查找用户
- 确定用户是否在由此电子邮件部署托管的域内
- 确定用户是否为该域中的有效用户
- 确定托管用户的邮箱的后端邮件存储计算机
- 将地址重写为 `@mailhost:uid@domain.LMTP` 或 `@mailhost:uid@domain.LMTPNATIVE`
- 排入邮件以传送到邮件主机

将格式为 user@domain.LMTP 和 user@domain.LMTPNATIVE 的地址分别通过 tcp_lmtp 通道或 tcp_lmtpnative 通道路由到邮件存储系统。这些通道与使用 LMTP （而不是 SMTP）的后端邮件存储进行通信。在存储计算机上，分发程序将收到一个与 LMTP 端口的连接，并将其传递到 lmtp_server 进程。然后 LMTP 服务器将邮件插入到用户的邮箱或者插入到 UNIX 的本地邮箱。如果邮件传送成功，将在中继计算机上取消该邮件的排队。如果未成功，该邮件将仍旧留在中继计算机上。请注意，邮件存储上的 LMTP 进程不使用任何 MTA 机制以用于处理地址或邮件。

LMTP 概述

通常，后端服务器基本上可以不具备 MTA 本身。必需的 MTA 组件仅包括：

- 分发程序
- libimta
- LMTP 服务器
- imta.cnf 文件
- mappings 文件
- imta.tailor 文件

当分发程序需要 MTA 配置文件时，这些文件可以非常短。分发程序必须在后端服务器上运行，以便其可以启动在该程序下运行的 LMTP 服务器。因为分发程序和 LMTP 服务器使用 libimta 的各种功能，因此也需要将其显示在后端服务器上。

LMTP 服务器不执行任何常规的 MTA 排入或取消排队功能、标题处理或地址转换。中继系统执行邮件和地址内容的所有操作，然后将这些邮件和地址显示给 LMTP 服务器，邮件的格式与要传送到邮件存储的格式完全相同，并且传送地址格式已经是存储所需的格式。通常在邮件被传送到存储时可获取的其它收件人信息 （例如用户的配额）将与作为 LMTP 参数的收件人地址一起显示。如果传送尝试失败，邮件将留在中继系统上的 LMTP 队列中排队。

配置 LMTP 传送

配置 LMTP 传送机制需要在中继计算机和后端存储上均进行配置。在中继上，必须更改 DELIVERY_OPTIONS MTA 选项 （在 option.dat 中），以便将要传送到存储的邮件传递到 LMTP 通道。必须用分发程序 （但不需要作业控制器）配置后端存储。必须配置分发程序以运行 LMTP 服务器。

在典型的多层部署中，用户置备于不同的后端邮件存储计算机中。这些后端计算机中的一台或多台可能未打开 LMTP，因此前端中继需要了解哪些存储计算机可以识别 LMTP。通过使用常规数据库功能明确命名那些配置为接受 LMTP 传送的邮件存储，可以实现此目的。

配置与 LMTP 配合使用的外来 MTA 中继

要配置外来 MTA 中继以使用 LMTP，请执行以下操作：

1. 通过将以下行添加到 option.dat 中激活文本数据库：

   ```
   USE_TEXT_DATABASES=1
   ```

   在此步骤中， MTA 中启用了常规数据库的平面文本文件。请注意如果已经使用常规数据库，可能要跳过此步骤。

2. 创建或修改常规数据库文本文件。

```
# cd /opt/SUNWmsgsr/config/
# vi general.txt

LMTP_CS|msg-store.siroe.com   lmtpcs-daemon
LMTP_CS|name-1-lmtp-store.siroe.com  lmtpcs-daemon
LMTP_CS|name-2-lmtp-store.siroe.com  lmtpcs-daemon
..
..
LMTP_CN|Zmar.Talek@siroe.com  lmtpcn-daemon
..
LMTP_CN|Fred.Bloggs@siroe.com  lmtpcn-daemon

# chown mailsrv general.txt
```

有两类条目，一类用于处理用户特定的、到 lmtpnative 通道的传送，另一类用于处理通过 tcp_lmtpcs 通道传送的存储范围设置。

3. 在 options.dat 文件中创建或修改 DELIVERY_OPTIONS 变量。

必须更改 DELIVERY_OPTIONS 的值。传送选项的当前默认值为：

```
DELIVERY_OPTIONS=\
     *mailbox=$M%$\$2I$_+$2S@ims-ms-daemon,\
     &members=*,\
     *native=$M@native-daemon,\
     *unix=$M@native-daemon,\
     /hold=$L%$D@hold-daemon,\
     &file=+$F@native-daemon,\
     &@members_offline=*,\
     program=$M%$P@pipe-daemon,\
     #forward=**,\
     *^!autoreply=$M+$D@bitbucket
```

将其更改为：

```
DELIVERY_OPTIONS=\
    #*mailbox=@$X:$M$_+$2S%$\$2I@ims-ms-daemon,\
    #&members=*,\
    #*native=@$X:$M,\
    #*unix=@$X:$M,\
    #/hold=$L%$D@hold,\
    #*file=@$X:+$F,\
    #&@members_offline=*,\
    #program=$M%$P@pipe-daemon,\
    #forward=**,\
    #*^!autoreply=$M+$D@bitbucket
```

注意邮箱传送选项的模式中的更改，并请注意，现在自动回复传送选项前已加上字符 #，以在中继计算机上强制进行操作。 $X 替换将插入用户的 mailhost 属性的值。这会生成源路由的地址。

还请注意，为使本机文件、 UNIX 文件和程序传送方法有用， MTA 必须在目标计算机上运行。

4. 将 LMTP 重写规则添加到 imta.cnf 文件的步骤：

```
# cd /opt/SUNWmsgsr/config/
# cp imta.cnf imta.cnf.orig
# vi imta.cnf

!
! pipe
.pipe-daemon $U%$H.pipe-daemon@pipe-daemon
!
! tcp_local
!Rules for top level internet domains
<IMTA_TABLE:internet.rules
!
!Do mapping lookup for internal IP addresses
[] $E$R${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
!
!Do general.txt lookup for lmtp hosts
.domain-name.com $S$U%$H$D@$(LMTP_CN|$U@$H$D)
.domain-name.com $S$U%$H$D@$(LMTP_CS|$H$D)
!
! tcp_intranet
!Do mapping lookup for internal IP addresses
[] $E$R${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
.domain-name.com $U%$H.domain-name.com@tcp_intranet-daemon
```

在此步骤中，一对重写规则将执行常规数据库的标记探测，以查看地址的源路由部分是否与执行 LMTP 传送的任何条目相匹配。在步骤 2 中创建的 general.txt 文件中，具有指定通过适当通道到后端邮件存储的传送的标记条目。这里，重写规则中的 $S 表示仅当地址包含源路由时才回复。如果常规数据库中有匹配的条目，则重写规则成功并且邮件通过 tcp_lmtp*X* 通道 （此通道通过 LMTP 进行传送）被发送到源路由后端主机。

如果没有找到匹配的条目，则重写过程将继续，直到在其他重写规则中找到匹配的条目为止。大多数情况下，如果通过常规数据库探测没有找到匹配的条目，则邮件通过 tcp_intranet 通道 （此通道通过 SMTP 进行传送）被路由。

5. 将新的通道块添加到 imta.cnf

还必须在 imta.cnf 文件的通道定义部分中包含 lmtp 和 lmtpn 通道的通道定义。例如：

```
! tcp_lmtpcs (LMTP client - store)
tcp_lmtpcs defragment lmtp port 225 nomx single_sys subdirs 20 maxjobs 7
pool SMTP_POOL dequeue_removeroute
lmtpcs-daemon
!
! tcp_lmtpcn (LMTP client - native)
tcp_lmtpcn defragment lmtp port 226 nomx single_sys subdirs 20 maxjobs 7
pool SMTP_POOL dequeue_removeroute
!lmtpcn-daemon
```

6. 提交配置更改。

```
# cd /opt/SUNWmsgsr/bin
# ./imsimta refresh

Compiled configuration done

Killing Dispatcher :23021

Dispatcher startup requested

Job Controller shutdown requested

Job Controller startup requested
```

注 请确保在 LMTP 通道中使用 lmtp 通道关键字。但不要在 LMTP 通道中同时使用 smtp 和 lmtp 通道关键字。另请注意，默认情况下，LMTP 通道定义已被注释掉。如果需要 LMTP 工作，必须取消其注释。

如果您既有 Sun Java System Messaging Server 用户组织又有非 Sun Java System Messaging Server 用户组织，则需要能够指明非 Sun Java System Messaging Server 计算机上的用户。这些用户的 delivery 选项不能设置为 mailbox，而必须将他们的 delivery 选项设置为 forward。该转发地址应为源路由格式，并可以为以下任何一种示例 （但不局限于此）：

```
mailForwardingAddress: @nonSJSMSHost.siroe.com:first.last@siroe.com
```

或

```
mailForwardingAddress: @nonSJSMSHost.siroe.com:login@siroe.com
```

或

```
mailForwardingAddress: @nonSJSMSHost.siroe.com:first.last@nonSJSMSHost.siroe.com
```

或

```
mailForwardingAddress: @nonSJSMSHost.siroe.com:login@nonSJSMSHost.siroe.com
```

也即，

```
@nonSJSMSHost.siroe.com:address-which-is-recognized-by-the-nonSJSMSHost
```

配置具有 LMTP 而没有 MTA 的后端存储

如果后端存储要通过 LMTP 接收邮件，则它们不需要 MTA。这意味着它们没有作业控制器，并且没有与 MTA 相关联的任何地址重写机制。但是，它们确实仍需要分发程序和简单的 MTA 配置。特别是需要 dispatcher.cnf 文件和 mappings 文件，这两个文件将构成 MTA 配置的唯一重要部分。

dispatcher.cnf 文件必须包含以下内容：

```
! rfc 2033 LMTP server - store
!
[SERVICE=LMTPSS]
PORT=225
IMAGE=IMTA_BIN:tcp_lmtp_server
LOGFILE=IMTA_LOG:tcp_lmtpss_server.log
PARAMETER=CHANNEL=tcp_lmtpss
STACKSIZE=2048000
!Uncomment the following line and set INTERFACE_ADDRESS to an
appropriate
! host IP (dotted quad) if the dispatcher needs to listen on a
specific
! interface (e.g. in a HA environment).
!INTERFACE_ADDRESS=
!
! rfc 2033 LMTP server - native
!
[SERVICE=LMTPSN]
PORT=226
IMAGE=IMTA_BIN:tcp_lmtpn_server
LOGFILE=IMTA_LOG:tcp_lmtpsn_server.log
PARAMETER=CHANNEL=tcp_lmtpsn
STACKSIZE=2048000
!Uncomment the following line and set INTERFACE_ADDRESS to an
appropriate
! host IP (dotted quad) if the dispatcher needs to listen on a
specific
! interface (e.g. in a HA environment).
!INTERFACE_ADDRESS=
```

请注意，默认情况下， dispatcher.cnf 文件中的 LMTP 服务被注释掉。您必须取消其注释才能使 LMTP 工作。

还可以设置 MAX_CONNS、 MAX_PROCS、 MAX_LIFE_CONNS 和 MAX_LIFE_TIME 的常规分发程序选项，但是需要针对您的硬件相应地进行设置。

PORT_ACCESS 映射很重要。后端服务器的 LMTP 实现旨在用作 Sun Java System Messaging Server 中继和后端存储之间的专用协议。您必须使用 PORT_ACCESS 映射以确保只有此类中继可以连接到这些服务。您的映射文件应类似于此：

```
PORT_ACCESS

  TCP|*|225|1.2.3.4|* $Y
  TCP|*|226|1.2.3.4|* $Y
  TCP|*|225|1.2.3.5|* $Y
  TCP|*|226|1.2.3.5|* $Y
  TCP|*|*|*|*   $N500$ Do$ not$ connect$ to$ this$ machine
```

您应该用连接到后端存储的网络中的中继 IP 地址替换在此处的 PORT_ACCESS 映射表中指定的样例 IP 地址。

必须有一个 imta.cnf 文件，但是它只用于使配置完成。最小的 imta.cnf 文件由以下通道定义组成：

```
! tcp_lmtpss (LMTP server - store)
tcp_lmtpss lmtp
tcp_lmtpss-daemon

!
! tcp_lmtpsn (LMTP server - native)
tcp_lmtpsn lmtp
tcp_lmtpsn-daemon
```

请注意，默认情况下， LMTP 通道定义被注释掉。如果需要 LMTP 工作，必须取消其注释。

配置中继以通过 LMTP 将邮件发送到带有邮件存储和完整 MTA 的后端系统

存在这样的情况，您可能希望后端存储具有 MTA 的全部功能，但是仍旧具有使用 LMTP 的装入保存功能。例如，您可能需要在后端存储上的程序传送。在这种情况下，中继应按照上述第 437 页的 “配置与 LMTP 配合使用的外来 MTA 中继”中的说明进行配置。

在具有完整 MTA 的后端邮件存储系统中配置 LMTP

从后端存储邮件传送系统的配置到使用 LMTP 直接传送到存储的配置的唯一更改是需要将以下行添加到 dispatcher.cnf 文件的最后：

```
! rfc 2033 LMTP server - store
!
[SERVICE=LMTPSS]
PORT=225
IMAGE=IMTA_BIN:tcp_lmtp_server
LOGFILE=IMTA_LOG:tcp_lmtpss_server.log
PARAMETER=CHANNEL=tcp_lmtpss
STACKSIZE=2048000
!Uncomment the following line and set INTERFACE_ADDRESS to an appropriate
! host IP (dotted quad) if the dispatcher needs to listen on a specific
! interface (e.g. in a HA environment).
!INTERFACE_ADDRESS=
!
! rfc 2033 LMTP server - native
!
[SERVICE=LMTPSN]
PORT=226
IMAGE=IMTA_BIN:tcp_lmtpn_server
LOGFILE=IMTA_LOG:tcp_lmtpsn_server.log
PARAMETER=CHANNEL=tcp_lmtpsn
STACKSIZE=2048000
!Uncomment the following line and set INTERFACE_ADDRESS to an appropriate
! host IP (dotted quad) if the dispatcher needs to listen on a specific
! interface (e.g. in a HA environment).
!INTERFACE_ADDRESS=
!
```

请注意，默认情况下， dispatcher.cnf 文件中的 LMTP 服务被注释掉。您必须取消其注释才能使 LMTP 工作。此外， LMTP 端口号仅为示例，您可以任意选择。

这与以上所述的用于仅为 LMTP 配置后端存储时的整个 dispatcher.cnf 文件相同。映射文件还需要 PORT_ACCESS 映射，这已在有关仅具有 LMTP 的后端存储的内容中进行了说明。

要执行的 LMTP 协议

本节提供了 LMTP 对话样例，并带有在该对话中看到的解释。中继上的 LMTP 客户机使用标准的 LMTP 协议与后端存储上的 LMTP 服务器联系。但是，该协议以特定方式使用。例如：

```
---> LHLO
<--- 250 OK
```

对 LHLO 邮件没有采取任何操作。回复始终是 250 OK。

```
---> MAIL FROM:address size=messageSizeInBytes
<--- 250 OK
```

对创始人地址没有进行任何检查或转换。 size= 参数给出了要传送的邮件的大小（以字节为单位）。此邮件的大小与协议中显示的大小完全相同。邮件的大小可以不必完全相同，但是实际邮件的大小不能超过此大小。 LMTP 服务器将按此大小分配内存缓冲区以接收邮件。

```
---> RCPT TO:uid+folder@domain xquota=size,number xdflg=xxx
<--- 250 OK
```

在收到收件人地址时不对其进行任何检查，但是将生成一个收件人列表以便以后使用。请注意，对于主域中的 uids，地址的 @domain 部分将被忽略，并且 +folder 部分是可选的。这与 MTA 中的邮件存储通道所使用的地址格式相同。

xquota= 参数给出了用户的邮件配额，它包括邮件的最大总大小和最大数目。 MTA 提供了在对用户执行 LDAP 查找以进行地址转换时检索到的信息。此信息用于使邮件存储中的配额信息与目录保持同步。获取配额信息不会导致其他性能受到打击。

xdflg= 参数指定了一个数字，该数字可以解释为位字段。这些位将控制传送邮件的方式。例如，值为 2 （如果设置）的位将保证邮件的传送，即使用户超出配额。（请注意， xdflg 是内部参数并且其中的位如有更改或添加，恕不另行通知。我们不支持其他客户机使用我方服务器的此扩展名，也不支持将我方客户机与某些其他服务器和此参数结合使用。）

此交互式操作可能重复许多次，每个收件人一次。

```
--->DATA
---> <the message text>
--->.
```

然后 LMTP 客户机发送整个邮件 （充满点的），类似于 SMTP 执行的操作。邮件完成，一行带有一个点 (.)。如果超过邮件大小，则 LMTP 服务器将发送：

```
<--- 500 message too big
```

并结束连接。

假设正确接收了邮件，则 LMTP 服务器将向 LMTP 客户机发送回每个收件人 （在 RCPT TO: 行中给定的）的状态。例如，如果成功传送了邮件，则响应为：

```
<--- 250 2.5.0 address OK
```

其中 address 与在 RCPT TO: 行中显示的完全相同。

对话可以用另一个 MAIL FROM: 行重复或者用以下交互式操作结束：

```
---> quit
<--- 221 OK
```

表 15-1 显示了每个收件人的可能的状态代码。此三列表在第一列中显示了短代码，在第二列中显示了其等效的长代码，在第三列中显示了状态文本。 2.x.x 状态代码是成功代码， 4.x.x 代码是可重试错误， 5.x.x 代码是不可重试错误。

表 15-1 收件人的 LMTP 状态代码

短代码	长代码	状态文本
250	2.5.0	确定
420	4.2.0	邮箱被锁定
422	4.2.2	超出配额
420	4.2.0	邮箱格式错误
420	4.2.0	邮箱不受支持
430	4.3.0	IMAP IOERROR
522	5.2.2	超出永久配额
523	5.2.3	邮件太大
511	5.1.1	邮箱不存在
560	5.6.0	邮件包含空字符
560	5.6.0	邮件包含 nl
560	5.6.0	邮件标题错误
560	5.6.0	邮件无空白行

否则，将存在对邮箱、本机系统 （因此为 UNIX）和文件的传送选项的更改。这些规则的目标是要生成地址，这些地址将导致邮件通过相应的 LMTP 通道被发送到后端服务器。生成的地址是以下格式的源路由地址：

```
@sourceroute:localpart@domain
```

第 16 章

休假自动邮件回复

对于自动生成的电子邮件 （尤其是休假邮件）响应 （自动回复）， MTA 使用邮件处理通知 (*MDN*) 和 Sieve 脚本撰写语言。 MDN 是由 MTA 发送给发件人和 / 或报告邮件传送部署的邮寄主管的电子邮件消息。 MDN 也称为已读回执、确认、回执通知或传送回执。 Sieve 是用于创建邮件过滤器的简单脚本撰写语言。

本节介绍了休假自动回复机制。在大多数情况下，不必修改默认配置；但是，您希望配置系统以便在 MTA 中继计算机上而不是在后端邮件存储上完成休假处理的情况除外。

本章由以下各节组成：

- 第 449 页的 “休假自动回复概述”
- 第 450 页的 “配置自动回复”
- 第 452 页的 “休假自动回复操作的原理”
- 第 453 页的 “休假自动回复属性”

休假自动回复概述

可以由各种 LDAP 休假属性自动生成休假 Sieve 脚本 （请参见第 453 页的 “休假自动回复属性”），也可以明确指定这些脚本以获得更大的灵活性。跟踪休假的基本机制是一组文件 （每个预期收件人一个），在将回复发送到各个发件人时，这些文件将保持跟踪。

默认情况下， MTA 将在后端存储系统中计算休假。但是，由于性能原因， MTA 中继做的工作不如后端存储做的多，因此您可以在邮件中继计算机上而不是在后端存储上计算 MTA 休假。但是，使用此功能可能会导致发出休假响应的次数多于预期的次数，因为不同的中继处理不同的邮件。如果不希望发出休假邮件的次数多于预期的次数，您可以在中继之间共享文件的跟踪。如果也无法接受这种方法，您可以始终在后端存储系统中计算休假。

配置自动回复

可以通过一组模式生成传送地址。所用的模式取决于为 mailDeliveryOption 属性定义的值。将为每个有效的 mailDeliveryOption 生成一个传送地址。这些模式由 MTA 选项 DELIVERY_OPTIONS （在 option.dat 文件中对该选项进行了定义）定义。option.dat 文件中 DELIVERY_OPTIONS 的默认自动回复规则为：

```
*^!autoreply=$M+$D@bitbucket
```

MTA 在自动回复 DELIVERY_OPTION MTA 选项中标注了 “^”。这将导致 MTA 检查休假日期。如果当前日期在休假日期之内，则处理将继续进行，并且 MTA 将在自动回复 DELIVERY_OPTION 中标注 “!”。然后， MTA 将基于用户条目中的各个自动回复 LDAP 属性创建一个休假 Sieve 脚本。自动回复规则可以有前缀字符 “!”、“#”、“^”和 “*”。

在邮箱传送选项中可以有 “!”标志。这将无条件地启用休假脚本的生成。但是，这样操作将很有意义：通过单独的传送选项启用自动回复方法，以便可以进一步用 “^”标志控制该自动回复方法。检查此阶段的日期比使用 Sieve 逻辑更有效。

表 16-1 在第一列中显示了用于自动回复规则的前缀字符，在第二列中显示了这些字符的定义。

表 16-1 用于 DELIVERY_OPTIONS 中的自动回复规则的前缀字符

前缀字符	定义
!	启用生成自动回复 Sieve 脚本。
#	允许在中继上进行处理。
^	仅在休假日期表明应该计算选项时才计算该选项。
*	规则仅适用于用户。

自动回复规则本身指定了为位桶通道指定的地址。生成自动回复后，将考虑用此方法传送邮件，但是 MTA 方法需要一个传送地址。传送到位桶通道的任何内容都将被放弃。

在后端存储系统中配置自动回复

DELIVERY_OPTIONS 中的默认自动回复规则将导致自动回复发生在服务于用户的邮件服务器上。如果希望在后端存储系统中计算休假邮件，则不必进行任何配置。这是默认性能。

在中继上配置自动回复

如果希望在中继上而不是在后端存储系统中计算休假以提高性能，请编辑 option.dat 文件并将字符 # 放到自动回复规则的 DELIVERY_OPTIONS 的前面。例如：

1. 使用 an 编辑器打开 option.dat 文件。
2. 添加或更改 DELIVERY_OPTIONS 选项，以使自动回复规则现在类似于：

   ```
   #*^!autoreply=$M+$D@bitbucket
   ```

   默认的 DELIVERY_OPTIONS 选项类似于：

   ```
   DELIVERY_OPTIONS=*mailbox=$M%$\$2I$_+$2S@ims-ms-daemon, \
    &members=*, \
    *native=$M@native-daemon, \
    /hold=@hold-daemon:$A, \
    *unix=$M@native-daemon, \
    &file=+$F@native-daemon, \
    &@members_offline=* \
    ,program=$M%$P@pipe-daemon, \
    #forward=**, \
    *^!autoreply=$M+$D@bitbucket
   ```

这将允许在中继上进行处理。如果 MTA 在中继上执行自动回复，则每个中继都可以独立跟踪特定通信人最近是否发送了一封离开邮件，或者此信息可以在中继之间共享。前一种情况简单一些，特别是在发出太多次离开邮件但无关紧要的时候。如果希望严格执行离开邮件的频率规则，则必须在中继之间共享信息。要在中继之间共享信息，应当以 NFS 形式装入这些文件

这些文件的位置由选项 VACATION_TEMPLATE 控制。应将该选项 （在 option.dat 中）设置为 /<path>/%A，其中 <path> 是在各种中继计算机之间共享的目录路径。模板需要为 file:URL，并且使用 $U 替换用户的名称。默认设置为：

```
VACATION_TEMPLATE=file:///opt/SUNWmsgsr/data/vacation/$3I/$1U/$2U/$U.vac
```

有关元字符的说明，请参见表 9-6 第 196 页。

注 现在休假文件模板具有对 UID 的访问权限，并允许基于用户的 UID 生成休假文件的路径。此外，用于确定休假文件路径的地址现在存储在用户的邮件属性中，以前使用的是当前收件人地址。

休假自动回复操作的原理

在调用时，休假操作按如下方式进行：

1. Sun Java System Messaging Server 将进行检查以确保休假操作由用户级别而不是系统级别 Sieve 脚本执行。如果在系统级别的脚本中使用休假，将产生一个错误。
2. “无休假通知”内部 MTA 标志被选中。如果设置了该标志，则处理将终止并且不会发送休假通知。
3. 邮件的返回地址现在被选中。如果该地址为空白，则处理将终止并且不会发送休假通知。
4. MTA 将进行检查以查看在标记了 `:addresses` 的变量中指定的用户地址或任何其他地址是否显示在当前邮件的 `To:`、`Cc:`、`Resent-to:` 或 `Resent-cc:` 标题字段中。如果在任何标题字符字段中均未找到任何地址，则处理将终止并且不会发送休假通知。
5. Messaging Server 将构造一个 `:subject` 变量和原因字符串的散列。将根据先前休假响应的每个用户的记录选取该字符串以及当前邮件的返回地址。如果在 `:days` 变量所允许的时间内已经发送了响应，则处理将终止并且不会发送响应。
6. Messaging Server 将从 `:subject` 变量、原因字符串和 `:mime` 变量构造一个休假通知。此响应邮件的两种基本形式可能为：
   - 在 RFC 2298 中指定的形式的邮件处理通知，其中第一部分包含原因文本。
   - 单个部分文本回复。（此形式只用于支持“回复”自动回复模式属性设置。）

请注意，通过 Messenger Express 配置休假邮件时，会将 `mailautoreplymode` 自动设置为 `reply`。

默认情况下，“无休假通知” MTA 标志是被清除的。可以通过使用非标准 `novacation` 操作由系统级别 Sieve 脚本设置该标志。只允许在系统级别 Sieve 脚本中使用 `novacation` Sieve 操作。如果在用户级别的脚本中使用该操作，将生成错误。您可以使用此操作实现站点范围内对休假回复 （例如对包含子字符串“`MAILER-DAEMON`”的地址的阻止回复）的限制。

每个用户每次响应的信息被存储在一组平面文本文件中，每个本地用户一个。这些文件的位置和命名方案是通过 `VACATION_TEMPLATE` MTA 选项的设置来指定的。该选项应被设置为 `file:URL`。

这些文件的维护是自动进行的并通过 `VACATION_CLEANUP` 整数 MTA 选项设置进行控制。每次打开其中一个文件时，将以该值为模计算当前时间的值 （以秒为单位）。如果结果为零，将扫描该文件并删除所有过期的条目。该选项的默认值为 200，这意味着在 200 次中有 1 次机会将执行清除操作。

用来读写这些平面文本文件的方法是以这样的方式设计的，即，它应该可以在 NFS 中正常操作。这使多个 MTA 可以在公用文件系统中共享单组文件。

休假自动回复属性

休假操作使用的用户 LDAP 目录属性集为：

- 由 LDAP_PERSONAL_NAME 定义的属性

  别名处理将跟踪此属性中指定的个人姓名信息，并将使用此信息来构建任何 MDN 或已生成的休假回复的 From: 字段。请小心使用，以免暴露个人信息。

- vacationStartDate

  休假开始日期和时间。该值的格式为 YYYYMMDDHHMMSSZ。该值被标准化为 GMT。如果当前时间在此属性所指定的时间之后，则应仅生成自动回复。如果缺少该属性，则不会强制指定开始日期。通过将 LDAP_START_DATE MTA 选项设置为另一个属性的名称，可以指示 MTA 查看此信息的另一个属性。

  该属性将由生成 Sieve 脚本的代码进行读取和检查。如果当前日期在休假开始日期之前，休假处理将被中止。由于目前 Sieve 缺少日期 / 时间测试和比较功能，因此该属性无法通过脚本自身进行处理。

- vacationEndDate

  休假结束日期和时间。该值的格式为 YYYYMMDDHHMMSSZ。该值被标准化为 GMT。如果当前时间在此属性所指定的时间之前，则应仅生成自动回复。如果缺少该属性，则不会强制指定结束日期。通过将 LDAP_END_DATE MTA 选项设置为另一个属性的名称，可以指示 MTA 查看此信息的另一个属性。

  该属性将由生成 Sieve 脚本的代码进行读取和检查。如果当前日期在休假结束日期之后，休假处理将被中止。由于目前 Sieve 缺少日期 / 时间测试和比较功能，因此该属性无法在脚本自身中进行处理。

- mailAutoReplyMode

  指定用户邮件帐户的自动回复模式。该属性的有效值为：

  - echo — 除了添加的 mailAutoReplyText 或 mailAutoReplyTextInternal 文本之外，还创建一个回送原始邮件文本的多部分文本。
  - reply — 将 mailAutoReplyText 或 mailAutoReplyTextInternal 指定的单部分回复发送给原始发件人。

这些模式将作为假期操作的非标准 :echo 和 :reply 变量显示在 Sieve 脚本中。echo 将生成一个 “已处理的”邮件处理通知 (MDN)，它包含作为返回内容的原始邮件。 reply 将产生一个仅包含回复文本的纯回复。非法值不会标明为休假操作的任何变量，这将生成一个仅包含原始邮件标题的 MDN。还请注意，选择回送的自动回复模式会导致将自动回复发送给每封邮件，无论上一个回复的发送日期多么近。

通过将 LDAP_AUTOREPLY_MODE MTA 选项设置为另一个属性的名称，可以指示 MTA 使用此信息的另一个属性。

- mailAutoReplySubject

  指定要在自动回复响应中使用的主题字段的内容。此内容必须为 UTF-8 字符串。该值作为休假操作的 :subject 变量被传送。通过将 LDAP_AUTOREPLY_SUBJECT MTA 选项设置为另一个属性的名称，可以指示 MTA 使用此信息的另一个属性。

  请注意，由于 Sieve 当前缺少执行某些替换的能力，因此目前无法实现使用 $SUBJECT 将原始邮件插入到标题中。

- mailAutoReplyText

  发送给所有发件人 （除了收件人域中的用户）的自动回复文本。如果未指定文本，外部用户将不会收到休假邮件。通过将 LDAP_AUTOREPLY_TEXT MTA 选项设置为另一个属性名称，可以指示 MTA 使用该信息的另一个属性。

- mailAutoReplyTextInternal

  发送给收件人域中的发件人的自动回复文本。如果未指定文本，则内部用户将获得邮件自动回复文本邮件。通过将 LDAP_AUTOREPLY_TEXT_INT MTA 选项设置为另一个属性的名称，可以指示 MTA 使用此信息的另一个属性。

  MTA 会将 mailAutoReplyText 或 mailAutoReplyTextInternal 属性值作为原因字符串传送到休假操作。

- mailAutoReplyTimeOut

  对任何给定邮件发件人的连续自动回复响应的有效期 （以小时为单位）。仅在 mailAutoReplyMode=reply 时才使用。如果值为 0，则每次收到一封邮件时就会发回一个响应。该值将被转换为休假操作的非标准 :hours 变量。（通常， Sieve 休假操作仅支持用于此目的的 :days 变量，但不允许值为 0。）

  如果用户条目中未显示该属性，将从 AUTOREPLY_TIMEOUT_DEFAULT MTA 选项获得一个默认超时值。通过设置 LDAP_AUTOREPLY_TIMEOUT MTA 选项，可以指示 MTA 使用该信息的另一个属性。

第 17 章

邮件过滤和访问控制

本章讨论了如何基于邮件的源 （发件人、 IP 地址等）或标题字符串来过滤邮件。采用两种邮件过滤机制，用映射表和 Sieve 服务器端规则 (SSR) 控制对 MTA 的访问。

使用映射表限制对 MTA 的访问，使得可以基于 From: 和 To: 地址、 IP 地址、端口号和源通道或目标通道过滤邮件。映射表允许启用或禁用 SMTP 中继。 Sieve 是一个邮件过滤脚本，允许基于标题中的字符串过滤邮件 （不能基于邮件正文中的字符串过滤邮件）。

如果要进行信封级别控制，请使用映射表来过滤邮件。如果要进行基于标题的控制，请使用 Sieve 服务器端规则。

本章分为两部分：

第 1 部分：映射表。允许管理员通过配置特定映射表来控制对 MTA 服务的访问。管理员可以控制别人能否通过 Messaging Server 发送邮件或接收邮件。

第 2 部分：邮箱过滤器。允许用户和管理员基于邮件标题中的字符串来过滤邮件并指定对已过滤的邮件的操作。使用 Sieve 过滤语言并可以在通道级别、 MTA 级别或用户级别过滤。

第 1 部分：映射表

第 1 部分包含以下各节：

- 第 456 页的 “使用映射表控制访问”
- 第 468 页的 “应用访问控制后”
- 第 469 页的 “测试访问控制映射”
- 第 470 页的 “添加 SMTP 中继”

- 第 472 页的 “配置 SMTP 中继阻止”
- 第 478 页的 “处理大量访问条目”
- 第 457 页的 “访问控制映射表标志”

使用映射表控制访问

您可以通过配置特定的映射表来控制对邮件服务的访问。这些映射表使您能够控制哪些人可以发送和 / 或接收邮件，哪些人不可以。表 17-1 列出了本节中说明的映射表。提供给 FROM_ACCESS、MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射的应用程序信息字符串包括 HELO/EHLO SMTP 命令中声明的系统名称。此名称显示在字符串末尾并用斜杠与字符串的其余部分 （通常情况下是 "SMTP"）分隔开。这个声明的系统名称在阻止一些蠕虫和病毒时非常有用。

访问控制映射表 — 操作

与所有映射表一样，访问控制映射表具有相同的通用格式 （请参见第 208 页的 “映射文件”）。这些访问控制映射表由映射表名称、后跟换行、再后跟一个或多个映射条目组成。映射条目由左侧的**搜索模式**和右侧的**模板**组成。搜索模式过滤特定邮件，模板指定对邮件所进行的操作。例如：

```
SEND_ACCESS

 *|Elvis1@sesta.com|*|*      $Y
 *|Nelson7@sesta.com|*|*     $Y
 *|AkiraK@sesta.com|*|*      $Y
 *|*@sesta.com|*|*              $NMail$ Blocked
```

在此示例中，将阻止所有来自 sesta.com 域的电子邮件，但 Elvis1、Nelson 和 AkiraK 中的电子邮件除外。

访问控制映射条目的搜索模式由多个搜索条件组成，搜索条件之间以垂直条 (|) 分隔。搜索条件的顺序取决于访问映射表，这将在后面的小节中介绍。例如，SEND_ACCESS 映射表具有以下搜索格式：

src-channel|*from-address*|*dst-channel*|*to-address*

其中， *src-channel* 是将邮件排队的通道； *from-address* 是邮件创始者的地址； *dst-channel* 是要将邮件排队的通道； *to-address* 是邮件要发送到的地址。在这四个字段中的任意一个字段中使用星号将使该字段匹配所有适当的通道或地址。

注 修改 mappings 文件之后，必须重新编译配置 （请参见 Sun Java System Messaging Server Administration Reference 中的 imsimta refresh 命令）。

表 17-1 访问控制映射表

映射表	说明
SEND_ACCESS （请参见第 460 页。）	用于基于信封的 From 地址、 To 地址、源通道和目标通道阻止外来连接。执行重写、别名扩展等操作后将检查 To 地址。
ORIG_SEND_ACCESS （请参见第 460 页。）	用于基于信封的 From 地址、 To 地址、源通道和目标通道阻止外来连接。执行重写之后、别名扩展之前将检查 To 地址。
MAIL_ACCESS （请参见第 462 页。）	用于基于 SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息阻止外来连接：即， SEND_ACCESS 中找到的通道和地址信息结合 PORT_ACCESS 中找到的 IP 地址和端口号信息。
ORIG_MAIL_ACCESS （请参见第 462 页。）	用于基于 ORIG_SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息阻止外来连接：即， ORIG_SEND_ACCESS 中找到的通道和地址信息结合 PORT_ACCESS 中找到的 IP 地址和端口号信息。
FROM_ACCESS （请参见第 463 页。）	用于基于信封 From 地址过滤邮件。如果 To 地址是不相关的地址，请使用该表。
PORT_ACCESS （请参见第 466 页。）	用于根据 IP 编号阻塞外来的连接。

MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射是最常规的，不仅包含 SEND_ACCESS 和 ORIG_SEND_ACCESS 中的地址和通道信息，而且还包含可以通过 PORT_ACCESS 映射表获取的所有信息 （包括 IP 地址和端口号信息）。

访问控制映射表标志

表 17-2 显示了与 SEND_ACCESS、ORIG_SEND_ACCESS、MAIL_ACCESS、ORIG_MAIL_ACCESS 和 FROM_ACCESS 映射表相关的访问映射标志。请注意， PORT_ACCESS 映射表支持略有不同的标志集 （请参见表 17-3）。

带有参数的标志必须按照表中所示的阅读顺序排列参数。例如：

```
ORIG_SEND_ACCESS

  tcp_local|*|tcp_local|*    $N$D30|Relaying$ not$ allowed
```

在此示例中，正确的顺序是延迟时间段后跟拒绝字符串。请注意，标志本身可以按任何顺序排列。因此，以下条目具有相同的结果：

```
30|Relaying$ not$ allowed$D$N
$N30|Relaying$ not$ allowed$D
30|$N$DRelaying$ not$ allowed
```

表 17-2 访问映射标志

标志	说明
$A	如果已使用 SASL，则设置该标志。请参见第 216 页的 “检查特殊标志”。
$B	将邮件重定向到 bitbucket。
$D	如果请求获得延迟发送收据，则设置该标志 （在 FROM_ACCESS 中不可用）。请参见第 216 页的 “检查特殊标志”。
$F	如果请求获得失败发送收据，则设置该标志 （在 FROM_ACCESS 中不可用）。请参见第 216 页的 “检查特殊标志”。
$H	将邮件保存为 .HELD 文件。
$S	如果请求获得成功发送收据，则设置该标志 （在 FROM_ACCESS 中不可用）。请参见第 216 页的 “检查特殊标志”。
$T	如果已使用 TLS，则设置该标志。请参见第 216 页的 “检查特殊标志”。
$U	如果在 ORIG_SEND_ACCESS、 SEND_ACCESS、 ORIG_MAIL_ACCESS 和 MAIL_ACCESS 中使用，则从映射一开始就采用整数参数，并相应地设置 MM_DEBUG 的值。此外，还将在可能的情况下启用通道级别调试。结果是基于源 IP 地址、原始地址和收件人地址等项目启用调试。
$Y	允许访问。
$V	导致对所有收件人执行强制放弃。
$Z	导致对所有收件人执行强制 jettison。
带有参数的标志，按照参数阅读顺序 +（请勿按字母顺序排列此列表！）	
$U*integer*	从映射一开始就采用整数参数，并相应地设置 MM_DEBUG。此外，还将在可能的情况下启用通道级别调试。结果是，现在可以基于源 IP 地址、原始地址和收件人地址等启用调试。
$J*address*	* 使用指定的 *address* 替换原始信封 From: 地址。

表 17-2 访问映射标志

标志	说明
$K*address*	* ++ 使用指定的 *address* 替换原始 Sender: 地址。
$I*user*|*identifier*	检查指定用户的组 ID。
$<*string*	+++ 如果探测匹配，将 *string* 发送到系统日志 （UNIX、user.notice 设备和严重性）或事件日志 (NT)。
$>*string*	+++ 如果访问被拒绝，将 *string* 发送到系统日志 （UNIX、user.notice 设备和严重性）或事件日志 (NT)。
$D*delay*	延迟响应，间隔为 *delay* （以百分之一秒为单位），正值将导致延迟应用于事务中的每个命令；负值将导致延迟只应用于地址移交 （对于 FROM_ACCESS 表为 SMTP MAIL FROM: 命令；对于其他表为 SMTP RCPT TO: 命令）。
$T*tag*	使用 *tag* 前缀。
$A*header*	将标题行 *header* 添加到邮件。
$G*conversion_tag*	如果在 ORIG_SEND_ACCESS、 SEND_ACCESS、 ORIG_MAIL_ACCESS 和 MAIL_ACCESS 中使用，此标志将从映射结果中读取值并将该值视为要应用到当前收件人的一组转换标记。如果与 FROM_ACCESS 一起使用，转换标记将应用于所有收件人。在从映射中读取的变量序列中，$G 位于 $A （标题地址）之后。请参见第 373 页的 “邮件转换标记”。
$S*x,y,z*	* 导致从映射结果中读取其他以 | 分隔的参数。此参数由一个到三个用逗号分隔的整数值组成。第一个值为事务建立一个新的最小 blocklimit，第二个值建立一个新的最小 recipientlimit，第三个值建立一个新的最小 recipientcutoff。在读取任何捕获参数后，将从映射结果中读取此参数。有关详细信息，请参见第 346 页的 “指定绝对邮件大小限制”。
$X*error-code*	如果拒绝邮件，发布指定的 *error-code* 扩展 SMTP 错误代码。
$,*spamadjust_arg*	使您可以从访问映射表执行筛选 spamadjust 操作。该参数与 spamadjust 参数的格式相同。另请注意，这些映射中有一些是基于各收件人而应用的，执行的任何 spamadjust 操作都适用于所有收件人。
$N*string*	使用可选的错误文本 *string* 拒绝访问。
$F*string*	*$N string* 的同义词；即，使用可选的错误文本 *string* 拒绝访问。

* 仅可用于 FROM_ACCESS 表。

+ 要使用多个带有变量的标志，请用垂直条字符 | 分隔变量，并按照此表中列出的顺序放置变量。

++ 要使 $K 标志在 FROM_ACCESS 映射表中生效，源通道必须包含 authrewrite 关键字。

+++ 处理有问题的发件人时，使用 $D 标志是一个好主意，它可以防止拒绝服务攻击。特别地，在任何 $> 条目或 $< 条目拒绝访问中使用 $D 是一个好主意。

SEND_ACCESS 和 ORIG_SEND_ACCESS 表

您可以使用 SEND_ACCESS 和 ORIG_SEND_ACCESS 映射表控制别人能否发送邮件、接收邮件，或同时控制这两方面。访问检查包括邮件的信封 From: 地址和信封 To: 地址、邮件进入的通道以及要尝试发出邮件的通道。

如果映射表 SEND_ACCESS 或 ORIG_SEND_ACCESS 存在，则对于通过 MTA 的每封邮件的每个收件人， MTA 将使用以下格式的字符串扫描表格 （请注意垂直条字符 | 的使用）：

src-channel|*from-address*|*dst-channel*|*to-address*

src-channel 是将邮件排队的通道； *from-address* 是邮件创始者的地址； *dst-channel* 是要将邮件排队的通道； *to-address* 是邮件要发送到的地址。在这四个字段中的任意一个字段中使用星号将使该字段匹配所有适当的通道或地址。

此处的地址是信封地址，即信封 From: 地址和信封 To: 地址。如果是 SEND_ACCESS，将在执行重写、别名扩展等操作后检查信封 To: 地址；如果是 ORIG_SEND_ACCESS，将在执行重写之后、别名扩展之前检查原先指定的信封 To: 地址。

如果搜索字符串匹配某个模式 （即，表中某个条目的左侧），则将检查映射的结果输出。如果输出包含标志 $Y 或 $y，则允许对该特定 To: 地址进行排队。如果输出包含 $N、 $n、 $F 或 $f 中的任意一个标志，则对该特定地址进行排队将被拒绝。在被拒绝的情况下，映射输出中可能提供可选的拒绝文本。此字符串将包括在 MTA 发布的拒绝错误中。如果没有输出字符串 （除 $N、 $n、 $F 或 $f 标志以外），则将使用默认的拒绝文本。有关其他标志的说明，请参见第 457 页的 “访问控制映射表标志”。

将 MTA 选项 ACCESS_ORCPT 设置为 1 时，将向传递给 SEND_ACCESS、ORIG_SEND_ACCESS、 MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射表 （包含原始收件人 [ORCPT] 地址）的探测值添加一个附加的以垂直条分隔的字段。如果邮件没有 ORCPT 地址，则使用初始的、未经修改的 RCPT TO: 地址代替。默认值为 0，探测值位于末尾处：

src-channel|*from-address*|*dst-channel*|*to-address*|*ORCPT_address*

在以下示例中，从 UNIX 用户代理 （例如 mail、 Pine 等）发送的、源于本地通道 (l) 的邮件以及传送到 Internet 的邮件是通过某种 TCP/IP 通道发送出去的。假定不允许本地用户 （邮寄主管除外）向 Internet 发送邮件，但可以从 Internet 接收邮件。则下面示例中所示的 SEND_ACCESS 映射表是可以实施此限制的一种方法。在映射表中，假定本地主机名为 sesta.com。在通道名称 "tcp_*" 中使用了通配符，以便匹配所有可能的 TCP/IP 通道名称 （例如 tcp_local）。

代码示例 17-1 SEND_ACCESS 映射表

```
SEND_ACCESS

  *|postmaster@sesta.com|*|*    $Y
  *|*|*|postmaster@sesta.com    $Y
  l|*@sesta.com|tcp_*|*         $NInternet$ postings$ are$ not$  \
    permitted
```

在拒绝邮件中，使用了美元符号，用以引用邮件中的空格。如果没有这些美元符号，拒绝邮件将提前结束，只能阅读到 "Internet"，而不是 "Internet postings are not permitted"。请注意，此示例忽略了其他可能的 “本地”邮件来源，例如来自基于 PC 的邮件系统或来自 POP 或 IMAP 客户机的邮件。

注 尝试发送邮件的客户机将决定是否把 MTA 拒绝错误文本实际提供给尝试发送邮件的用户。如果 SEND_ACCESS 被用于拒绝外来 SMTP 邮件，MTA 将只发布一段包括可选拒绝文本的 SMTP 拒绝代码；要由发送 SMTP 客户机来使用该信息以构造要发送回原始发件人的弹回信息。

MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射表

MAIL_ACCESS 映射表是 SEND_ACCESS 和 PORT_ACCESS 映射表的超集。它结合了 SEND_ACCESS 的通道和地址信息，以及 PORT_ACCESS 的 IP 地址和端口号信息。类似地， ORIG_MAIL_ACCESS 映射表是 ORIG_SEND_ACCESS 和 PORT_ACCESS 映射表的超集。MAIL_ACCESS 的探测字符串的格式为：

port-access-probe-info|*app-info*|*submit-type*|*send_access-probe-info*

类似地， ORIG_MAIL_ACCESS 的探测字符串的格式为：

port-access-probe-info|*app-info*|*submit-type*|*orig_send_access-probe-info*

如果是外来 SMTP 邮件，此处的 *port-access-probe-info* 通常由 PORT_ACCESS 映射表探测中包含的所有信息组成，否则为空。 *app-info* 包含在 SMTP 命令 HELO/EHLO 中声明的系统名称。此名称显示在字符串末尾并用斜杠与字符串的其余部分 （通常情况下是 "SMTP"）分隔开。这个声明的系统名称在阻止一些蠕虫和病毒时非常有用。对应于邮件如何提交到 Messaging Server， *submit-type* 可以为 MAIL、 SEND、 SAML 或 SOML 其中之一。通常情况下该值为 MAIL，表示它是作为邮件提交的；如果是向 SMTP 服务器提交广播请求 （或组合的广播 / 邮件请求），该值可能会是 SEND、 SAML 或 SOML。对于 MAIL_ACCESS 映射， *send-access-probe-info* 通常由包含在 SEND_ACCESS 映射表探测中的所有信息组成。类似地，对于 ORIG_MAIL_ACCESS 映射， *orig-send-access-probe-info* 通常由包含在 ORIG_SEND_ACCESS 映射表探测中的所有信息组成。

将 MTA 选项 ACCESS_ORCPT 设置为 1 时，将向传递给 SEND_ACCESS、 ORIG_SEND_ACCESS、 MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射表 （包含原始收件人 [ORCPT] 地址）的探测值添加一个附加的以垂直条分隔的字段。如果邮件没有 ORCPT 地址，则使用初始的、未经修改的 RCPT TO: 地址代替。默认值为 0，探测值位于末尾处。示例：

port-access-probe-info|*app-info*|*submit-type*|*send_access-probe-info*|*ORCPT_address*

将外来 TCP/IP 连接信息与通道和地址信息包含在同一映射表中，可以更加方便地实施某些种类的控制，例如在来自特定 IP 地址的邮件中强制允许显示哪些信封 From: 地址。这对限制电子邮件伪造，或鼓励用户适当地配置其 POP 和 IMAP 客户机的 From: 地址很有用。例如，如果站点希望使信封 From: 地址 vip@siroe.com 只显示在来自 IP 地址 1.2.3.1 和 1.2.3.2 的邮件中，并确保来自子网 1.2.0.0 中所有系统的邮件上的信封 From: 地址都来自 siroe.com，则可以使用 MAIL_ACCESS 映射表，如下面示例所示。

代码示例 17-2 MAIL_ACCESS 映射表

```
MAIL_ACCESS

! Entries for vip's two systems
!
  TCP|*|25|1.2.3.1|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|*  $Y
  TCP|*|25|1.2.3.2|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|*  $Y
!
! Disallow attempts to use vip's From: address from other
! systems
!
  TCP|*|25|*|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|*  \
      $N500$ Not$ authorized$ to$ use$ this$ From:$ address
!
! Allow sending from within our subnet with siroe.com From:
! addresses
!
  TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*|*@siroe.com|*|*  $Y
!
! Allow notifications through
!
  TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*||*|*  $Y
!
! Block sending from within our subnet with non-siroe.com
! addresses
!
  TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*|*|*|*  \
      $NOnly$ siroe.com$ From:$ addresses$ authorized
```

FROM_ACCESS 映射表

FROM_ACCESS 映射表可用于控制谁可以发送邮件，或使用已验证的地址覆盖原来的 From: 地址，或同时用于这两方面。

FROM_ACCESS 映射表的输入探测字符串与 MAIL_ACCESS 映射表的输入探测字符串类似，只是减少了目标通道和地址，添加了已验证的发件人信息（如果有）。因此，如果 FROM_ACCESS 映射表存在，则对于每个邮件提交尝试，Messaging Server 将使用如下格式的字符串搜索表格（请注意垂直条字符 | 的使用）：

port-access-probe-info|*app-info*|*submit-type*|*src-channel*|*from-address*|*auth-from*

如果是外来 SMTP 邮件，此处的 *port-access-probe-info* 通常由 PORT_ACCESS 映射表探测中包含的所有信息组成，否则为空。 *app-info* 包含在 SMTP 命令 HELO/EHLO 中声明的系统名称。此名称显示在字符串末尾并用斜杠与字符串的其余部分 （通常情况下是 "SMTP"）分隔开。这个声明的系统名称在阻止一些蠕虫和病毒时非常有用。对应于邮件如何提交到 MTA， *submit-type* 可以为 MAIL、 SEND、 SAML 或 SOML 其中之一。通常情况下该值为 MAIL，表示它是作为邮件提交的；如果是向 SMTP 服务器提交广播请求 （或组合的广播 / 邮件请求），该值可能会是 SEND、 SAML 或 SOML。 *src-channel* 是邮件来自的通道 （即将邮件进行排队）； *from-address* 是邮件原来的创始者的地址； *auth-from* 是已验证的创始者地址 （如果此信息可用），如果已验证的信息不可用，则为空白。

如果探测字符串匹配某个模式 （即，表中某个条目的左侧），将检查映射的结果输出。如果输出包含标志 $Y 或 $y，则允许对该特定 To: 地址进行排队。如果输出包含 $N、 $n、 $F 或 $f 中的任意一个标志，则对该特定地址进行排队将被拒绝。在被拒绝的情况下，映射输出中可能提供可选的拒绝文本。此字符串将包括在 Messaging Server 发布的拒绝错误中。如果没有输出字符串（除 $N、$n、$F 或 $f 标志以外），则将使用默认的拒绝文本。有关其他标志的说明，请参见第 457 页的“访问控制映射表标志”。

除了基于创始者确定是否允许提交邮件， FROM_ACCESS 还可用于通过 $J 标志更改信封 From: 地址，或通过 $K 标志修改 authrewrite 通道关键字的效果 （在已接收的邮件上添加一个 Sender: 标题地址）。例如，此映射表可用于使原始信封 From: 地址被已验证的地址简单地替换。

代码示例 17-3 FROM_ACCESS 映射表

```
FROM_ACCESS

  *|SMTP|*|tcp_auth|*|        $Y
  *|SMTP|*|tcp_auth|*|*       $Y$J$3
```

使用 FROM_ACCESS 映射表修改某些 authrewrite 设置为非零值的源通道上的效果时，如果要按原样使用已验证的地址，则无需使用 FROM_ACCESS。

例如，在 tcp_local 通道上设置 authrewrite 2 时，则无需以下 FROM_ACCESS 映射表，因为 authrewrite 本身就已能够获得此效果 （按照原样添加已验证的地址）：

```
FROM_ACCESS

  *|SMTP|*|tcp_auth|*|      $Y
  *|SMTP|*|tcp_auth|*|*     $Y$K$3
```

但是， FROM_ACCESS 的真正目的在于允许进行更加复杂和细致的更改，如下面示例所示。如果要向外来邮件添加一个 Sender: 标题行 （显示 SMTP AUTH 已验证的提交者地址），则 authrewrite 关键字本身即可担当此任。但是，假设只有在 SMTP AUTH 已验证的提交者地址与信封 From: 地址不同时，才将这样一个 Sender: 标题行添加到外来邮件 （即如果地址匹配，则不必添加 Sender: 标题行），并进一步假设您不希望 SMTP AUTH 和信封 From: 地址仅仅因信封 From: 包括可选的子地址信息而被视作有所不同。

```
FROM_ACCESS

! If no authenticated address is available, do nothing
  *|SMTP|*|tcp_auth|*|              $Y
! If authenticated address matches envelope From:, do nothing
  *|SMTP|*|tcp_auth|*|$2*           $Y
! If authenticated address matches envelope From: sans
! subaddress, do nothing
  *|SMTP|*|tcp_auth|*+*@*|$2*@$4*    $Y
! Fall though to...
! ...authenticated address present, but didn't match, so force
! Sender: header
  *|SMTP|*|tcp_auth|*|*              $Y$K$3
```

PORT_ACCESS 映射表

分发程序可以基于 IP 地址和端口号选择性地接受或拒绝外来连接。分发程序启动时，将查找名为 PORT_ACCESS 的映射表。如果存在，分发程序将按以下格式格式化连接信息：

TCP|*server-address*|*server-port*|*client-address*|*client-port*

分发程序将尝试匹配所有 PORT_ACCESS 映射条目。如果映射结果包含 $N 或 $F，将立即关闭连接。映射的任何其他结果都表示可以接受连接。 $N 或 $F 可以后跟一条拒绝消息 （可选）。如果存在，该消息将在关闭连接之前被发送回连接。请注意，消息被发送回连接之前，其字符串将被附加一个 CRLF 结束符。

注 MMP 不使用 PORT_ACCESS 映射表。如果希望拒绝来自某些 IP 地址的 SMTP 连接并且正在使用 MMP，则必须使用 TCPAccess 选项。请参见第 159 页的 “用 MMP 配置邮件访问”。如果希望使用映射表来控制 SMTP 连接，请使用 INTERNAL_IP 映射表 （请参见第 471 页的 “允许为外部站点进行 SMTP 中继”）。

如果映射探测匹配，后跟可选字符串的标志 $< 可使 Messaging Server 将字符串发送给系统日志 (UNIX) 或事件日志 (NT)。如果访问被拒绝，后跟可选字符串的标志 $> 可使 Messaging Server 将字符串发送到系统日志 (UNIX) 或事件日志 (NT)。如果设置了 LOG_CONNECTION MTA 选项的第 1 位和 $N 标志以拒绝连接，则再指定 $T 标志会将 "T" 条目写入连接日志。如果设置了 LOG_CONNECTION MTA 选项的第 4 位，则可以将站点提供的文本包含在 PORT_ACCESS 条目中，以便包含在 "C" 连接日志条目中。要指定这样的文本，可以在条目的右侧包括两个垂直条字符，后跟所需的文本。表 17-3 列出了可用的标志。

表 17-3 PORT_ACCESS 映射表

标志	说明
$Y	允许访问。
带有变量的标志按照变量的阅读顺序排序 +	
$< string	如果探测匹配，将字符串发送到系统日志 (UNIX) 或事件日志 (NT)。
$> string	如果访问被拒绝，将字符串发送到系统日志 (UNIX) 或事件日志 (NT)。
$N string	使用可选的错误文本字符串拒绝访问
$F string	$N string 的同义词；即，使用可选的错误文本字符串拒绝访问

表 17-3 PORT_ACCESS 映射表

标志	说明
$T text	如果设置了 LOG_CONNECTION MTA 选项的第 1 位和 $N 标志以拒绝连接，则 $T 会将 "T" 条目写入连接日志；可选文本 （必须显示在两个垂直条字符之后）可以被包含到连接日志条目中。

+ 要使用多个带有变量的标志，请用垂直条字符 | 分隔变量，并按照此表中列出的顺序放置变量。

例如，除单独要拒绝的不包含说明文本的特定主机以外，以下映射将只接受来自单一网络的 SMTP 连接 （到端口 25，常规 SMTP 端口）：

```
PORT_ACCESS

  TCP|*|25|192.123.10.70|*  $N500
  TCP|*|25|192.123.10.*|*   $Y
  TCP|*|25|*|*              $N500$ Bzzzt$ thank$ you$ for$  \
     playing.
```

请注意，对 PORT_ACCESS 映射表进行任何更改后，都需要重新启动分发程序，以便使对分发程序的更改生效。（如果您使用的是已编译的 MTA 配置，则需要先重新编译配置，以将更改并入已编译的配置中。）

PORT_ACCESS 映射表专用于执行基于 IP 的拒绝。要在电子邮件级别进行更加通用的控制， SEND_ACCESS 或 MAIL_ACCESS 映射表可能更加适合。

限制指定 IP 地址到 MTA 的连接

通过使用 Port Access 映射表中的共享库 conn_throttle.so，可以限制特定 IP 地址连接到 MTA 的频繁程度。限制特定 IP 地址的连接对于防止拒绝服务攻击中使用的过多连接可能会有用。

conn_throttle.so 是一个在 PORT_ACCESS 映射表中使用的共享库，它可以限制特定 IP 地址过于频繁地连接到 MTA。所有配置选项都被指定为连接限制共享库的参数，如下所示：

$[*msg_svr_base*/lib/conn_throttle.so,throttle,*IP-address*,*max-rate*]

IP-address 是远程系统的点分十进制地址。 *max-rate* 是应对此 IP 地址强制的最大速率（连接次数 / 分钟）。

对于处罚性的例程，可以使用例程名称 `throttle_p` 而非 `throttle`。如果过去连接次数太多，`throttle_p` 将拒绝以后的连接。如果最大速率为 100，并且在过去的一分钟里尝试的连接次数为 250，则不仅远程站点将在该分钟内最初 100 次连接之后被阻止，在接下的分钟内它们还会被阻止。换句话说，系统将在每分钟之后从尝试连接的总数中减去最大速率，只要连接的总数大于最大速率，就将阻止远程系统。

如果指定的 IP 地址没有超过最大每分钟连接速率，共享库调用将失败。

如果超过了该速率，调用将成功，但什么也不会返回。这可以在 $C/$E 组合中来完成，如以下示例所示：

```
PORT_ACCESS

  TCP|*|25|*|* \
$C$[msg_svr_base/lib/conn_throttle.so,throttle,$1,10] \
$N421$ Connection$ not$ accepted$ at$ this$ time$E
```

其中，

`$C` 将继续执行从下一个表格条目开始的映射进程，并将此条目的输出字符串用作映射进程的新输入字符串。

`$[`*msg_svr_base*`/lib/conn_throttle.so,throttle,$1,10]` 是库调用，其中 `throttle` 为库例程， `$1` 为服务器 IP 地址，而阈值 10 为每分钟的连接次数。

`$N421$ Connection$ not$ accepted$ at$ this$ time` 将拒绝访问并返回 421 SMTP 代码 （瞬态负完成）以及消息 "Connection not accepted at this time"。

`$E` 将终止此时的映射进程。它使用此条目的输出字符串作为映射进程的最终结果。

应用访问控制后

Messaging Server 将尽早检查访问控制映射。此操作的执行取决于所使用的电子邮件协议 （必须要检查的信息可用时）。

对于 SMTP 协议，在发送端能够发送收件人信息或邮件数据之前，响应 MAIL FROM: 命令时，将发生一个 `FROM_ACCESS` 拒绝。在发送端发送邮件数据之前，响应 RCPT TO: 命令时，将发生一个 `SEND_ACCESS` 或 `MAIL_ACCESS` 拒绝。如果 SMTP 邮件被拒绝， Messaging Server 将永远不会接收或查看邮件数据，这就将执行此类拒绝的开销减至了最低。

如果有多个访问控制映射表， Messaging Server 将对所有这些映射表进行检查。即，FROM_ACCESS、SEND_ACCESS、ORIG_SEND_ACCESS、MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射表都可能生效。

测试访问控制映射

imsimta test -rewrite 实用程序 — 特别是与 -from、 -source_channel、 -sender 和 -destination_channel 选项一起使用时 — 在测试访问控制映射时会很有用。有关详细信息，请参见 Sun Java System Messaging Server Administration Reference (http://docs.sun.com/doc/819-0106)。下面的示例显示了样例 SEND_ACCESS 映射表和探测结果。

MAPPING TABLE:

```
SEND_ACCESS

  tcp_local|friendly@siroe.com|l|User@sesta.com     $Y
  tcp_local|unwelcome@varrius.com|l|User@sesta.com  $NGo$ away!
```

PROBE:

```
$ TEST/REWRITE/FROM="friendly@siroe.com" -
_$  /SOURCE=tcp_local/DESTINATION=l User@sesta.com
...
Submitted address list:
  l
    User (SESTA.COM) *NOTIFY FAILURES* *NOTIFY DELAYS* Submitted
notifications list:


$ TEST/REWRITE/FROM="unwelcome@varrius.com" -
_$  /SOURCE=tcp_local/DESTINATION=l User@sesta.com
...
Submitted address list:
Address list error -- 5.7.1 Go away! User@sesta.com

Submitted notifications list:
```

添加 SMTP 中继

默认情况下， Messaging Server 被配置为阻止尝试的 SMTP 中继，即拒绝从未验证的外部源 （外部系统是除服务器本身所在的主机以外的任何其他系统）向外部地址尝试提交邮件。此默认配置在阻止 SMTP 中继时相当主动，因为它将所有其他系统都认作外部系统。

如果 IMAP 和 POP 客户机尝试通过 Messaging Server 系统的 SMTP Server 将邮件提交到外部地址时，并且未使用 SMTP AUTH (SASL) 进行验证，将会发现其提交尝试被拒绝。因此，您可能要修改配置，以便它可以识别您自己的应始终从其接受中继的内部系统和子网。

将哪些系统和子网识别为内部通常由 INTERNAL_IP 映射表控制，该表可在 *msg_svr_base*/config/mappings 中找到。

例如，在 IP 地址为 123.45.67.89 的 Messaging Server 系统上，默认的 INTERNAL_IP 映射表如下所示：

```
INTERNAL_IP

   $(123.45.67.89/32)   $Y
   127.0.0.1   $Y
   *   $N
```

此处使用 $(IP-pattern/signicant-prefix-bits) 语法的初始条目指定匹配 123.45.67.89 全部 32 位的 IP 地址是匹配的 IP 地址并被视为内部地址。第二个条目将回送 IP 地址 127.0.0.1 视为内部地址。最后一个条目指定所有其他 IP 地址均不被视为内部地址。请注意，每个条目前都必须至少有一个空格。

您可以通过在最后的 $N 条目之前指定其他 IP 地址或子网来添加其他条目。这些条目必须在左侧指定 IP 地址或子网 （使用 $(.../...) 语法来指定子网）并在右侧指定 $Y。或者可以修改现有的 $(.../...) 条目，以接受更通用的子网。

例如，如果此同一样例站点具有一个 C 类网络 （即，它拥有 123.45.67.0 的全部子网），则此站点可以通过更改匹配地址使用的位数来修改初始条目。在以下的映射表中，我们将 32 位更改为 24 位。这使 C 类网络上的所有客户机都可以通过此 SMTP 中继服务器来中继邮件。

```
INTERNAL_IP

   $(123.45.67.89/24)   $Y
   127.0.0.1   $Y
   *   $N
```

如果站点仅拥有 123.45.67.80-123.45.67.99 范围内的 IP 地址，则此站点将希望使用：

```
INTERNAL_IP

! Match IP addresses in the range 123.45.67.80-123.45.67.95
   $(123.45.67.80/28)   $Y
! Match IP addresses in the range 123.45.67.96-123.45.67.99
   $(123.45.67.96/30)   $Y
   127.0.0.1   $Y
   *   $N
```

请注意， `imsimta test -match` 实用程序在检查 IP 地址是否匹配特定 $(.../...) 测试条件时很有用。`imsimta test -mapping` 实用程序更普遍的用途是检查 `INTERNAL_IP` 映射表是否返回了各种 IP 地址输入所需的结果。

修改 `INTERNAL_IP` 映射表之后，请确保发出 `imsimta restart` 命令 （如果未使用已编译的配置运行）或 `imsimta refresh` 命令 （如果使用已编译的配置运行），以便使更改生效。

有关映射文件和通用映射表格式的详细信息以及 `imsimta` 命令行实用程序的信息，请参见 Messaging Server Reference Manual。

允许为外部站点进行 SMTP 中继

所有内部 IP 地址都应按上述说明添加到 `INTERNAL_IP` 映射表中。如果有要允许从其进行 SMTP 中继的友好或伙伴系统 / 站点，最简单的方法是将它们与您的真实内部 IP 地址一起包含到 `INTERNAL_IP` 映射表中。

如果不想将它们看作真实的内部系统 / 站点 （例如，如果出于记录或其他控制目的，您希望区分**真实内部系统**与**具有中继权限的友好非内部系统**），则可以使用其他方法来配置系统。

一种方法是设置一个特殊的通道，用于接收来自此类友好系统的邮件。您可以通过创建与现有 *tcp_internal* 通道类似的、带有正式主机名 *tcp_friendly-daemon* 的 *tcp_friendly* 通道，以及创建与 INTERNAL_IP 映射表类似的、列出了友好系统 IP 地址的 FRIENDLY_IP 映射表来完成此设置。然后在当前重写规则之后：

```
! Do mapping lookup for internal IP addresses
[]    $E$R${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
```

添加一个新的重写规则：

```
! Do mapping lookup for "friendly", non-internal IP addresses []
$E$R${FRIENDLY_IP,$L}$U%[$L]@tcp_friendly-daemon
```

另外一种方法是将以下形式的新条目添加到 ORIG_SEND_ACCESS 映射表的最后的 $N 条目之上：

```
  tcp_local|*@siroe.com|tcp_local|*    $Y
```

其中 siroe.com 是友好域的名称，并添加以下形式的 ORIG_MAIL_ACCESS 映射表：

```
ORIG_MAIL_ACCESS

   TCP|*|25|$(match-siroe.com-IP-addresses)|*|SMTP|MAIL|    \
tcp_local|*@siroe.com|tcp_local|*     $Y
   TCP|*|*|*|*|SMTP|MAIL|tcp_local|*|tcp_local|*    $N
```

其中 $(...) IP 地址语法与以前章节所述的语法相同。只要地址正确，ORIG_SEND_ACCESS 检查就会成功，我们还可以进一步执行 ORIG_MAIL_ACCESS 检查，此检查更加严格并且仅在 IP 地址与 siroe.com IP 地址对应时才会成功。

配置 SMTP 中继阻止

您可以使用访问控制映射来阻止别人通过您的 Messaging Server 系统中继 SMTP 邮件。例如，您可以阻止别人使用您的邮件系统向成百上千的 Internet 邮箱中继垃圾邮件。

默认情况下， Messaging Server 将阻止所有 SMTP 中继活动，包括本地 POP 和 IMAP 用户的中继。

阻止未经授权的中继但允许合法本地用户进行中继，这需要配置 Messaging Server 以使其知道如何区分这两类用户。例如，使用 POP 或 IMAP 的本地用户依赖于 Messaging Server 充当 SMTP 中继。

要阻止 SMTP 中继，您必须能够：

- 区分内部邮件和外部邮件
- 第 474 页的 “区分已验证用户的邮件”
- 第 475 页的 “阻止邮件中继”

要启用由内部主机和客户机进行 SMTP 中继，您必须将 “内部” IP 地址或子网添加到 `INTERNAL_IP` 映射表。

MTA 如何区分内部邮件和外部邮件

为了阻止邮件中继活动， MTA 必须首先能够区分源自您的站点的内部邮件和源自 Internet 并通过您的系统传送回 Internet 的外部邮件。您要允许的是前一类邮件，要阻止的是后一类邮件。在入站 SMTP 通道 （通常为 `tcp_local` 通道）中使用 `switchchannel` 关键字 （默认设置）可以实现此区分。

`switchchannel` 关键字通过使 SMTP 服务器查找与外来 SMTP 连接关联的实际 IP 地址来进行工作。 Messaging Server 将该 IP 地址和重写规则结合使用，以区分源自域内的 SMTP 连接和来自域外的连接。然后，此信息可用于在内部和外部通信之间分离邮件通信。

下面所述的 MTA 配置为默认设置，以便服务器可以区分内部和外部邮件通信。

- 在配置文件中，紧接本地通道之前，是一个带有 `noswitchchannel` 关键字的 `defaults` 通道：

  ```
  ! final rewrite rules
  defaults noswitchchannel
  ! Local store
  ims-ms ...
  ```

- 外来 TCP/IP 通道指定了 `switchchannel` 和 `remotehost` 关键字，例如：

  ```
  tcp_local smtp single_sys mx switchchannel remotehost
  TCP-DAEMON
  ```

- 在外来 TCP/IP 通道定义之后，是一个具有不同名称的类似通道，例如：

  ```
  tcp_intranet smtp single_sys mx allowswitchchannel routelocal
  tcp_intranet-daemon
  ```

将地址重写到通道时， routelocal 通道关键字使 MTA 尝试 “短路”通过此通道的地址中的所有显式路由，借以阻止通过显式源路由的地址，在内部 SMTP 主机间以循环方式进行的可能的中继尝试。

使用以上配置设置，域内生成的 SMTP 邮件将通过 tcp_intranet 通道进入。所有其他 SMTP 邮件将通过 tcp_local 通道进入。邮件将基于其进入的通道被区分为内部邮件和外部邮件。

这是如何起作用的？答案就是 switchchannel 关键字。该关键字被应用到 tcp_local 通道。邮件进入 SMTP 服务器时，该关键字使服务器查看与外来连接关联的源 IP 地址。服务器尝试对外来连接的真实 IP 地址进行反向指向信封重写，查找关联的通道。如果源 IP 地址匹配 INTERNAL_IP 映射表中的 IP 地址或子网，调用该映射表的重写规则将使地址重写到 tcp_intranet 通道。

由于 tcp_intranet 通道标有 allowswitchchannel 关键字，所以邮件将被切换到 tcp_intranet 通道，并从该通道进入。如果邮件从其 IP 地址没有包含在 INTERNAL_IP 映射表中的系统进入，反向指向信封重写会重写到 tcp_local，或者可能重写到某些其他通道。但是，它不会重写到 tcp_intranet 通道，并且由于默认情况下，其他所有通道被标记为 noswitchchannel，所以邮件不会切换到另一通道而是保留在 tcp_local 通道中。

注 请注意，使用字符串 "tcp_local" 的任何映射表或转换文件条目可能都需要更改为 "tcp_*" 或 "tcp_intranet" （取决于用法）。

区分已验证用户的邮件

您的站点可能具有不属于您的物理网络的 “本地”客户机用户。当这些用户提交邮件时，邮件提交将从外部 IP 地址进入 — 例如，任意 Internet 服务提供商。如果您的用户使用可以执行 SASL 验证的邮件客户机，则可以将他们已验证的连接与任意其他外部连接区分开。然后您可以允许已验证的提交，同时拒绝未验证的中继提交尝试。在入站 SMTP 通道 （通常为 tcp_local 通道）中使用 saslswitchchannel 关键字可以区分已验证的和未验证的连接。

saslswitchchannel 关键字使用变量来指定要切换到的通道；如果 SMTP 发件人验证成功，则其提交的邮件将被视为进入指定的切换到的通道。

要添加区分已验证的提交，请执行以下步骤：

1. 在配置文件中，添加带有独特名称的新 TCP/IP 通道定义，例如：

   ```
   tcp_auth smtp single_sys mx mustsaslserver noswitchchannel
   TCP-INTERNAL
   ```

   此通道应不允许常规通道切换 （即，此通道上应通过之前的默认设置行显式标有或暗示具有 noswitchchannel）。此通道上应具有 mustsaslserver。

2. 通过添加 maysaslserver 和 saslswitchchannel tcp_auth 来修改 tcp_local 通道，如以下示例所示：

   ```
   tcp_local smtp mx single_sys maysaslserver saslswitchchannel tcp_auth  \
   switchchannel
   |TCP-DAEMON
   ```

使用此配置后，能够使用本地密码进行验证的用户所发送的 SMTP 邮件将进入 tcp_auth 通道。从内部主机发送的未验证的 SMTP 邮件仍将进入 tcp_internal。所有其他 SMTP 邮件将进入 tcp_local。

阻止邮件中继

现在要讨论此示例的要点：阻止未经授权的人员通过您的系统中继 SMTP 邮件。首先，请记住您要允许本地用户中继 SMTP 邮件。例如，POP 和 IMAP 用户依赖使用 Messaging Server 来发送其邮件。请注意，本地用户可能在物理上是本地 （在这种情况下，其邮件从内部 IP 地址进入）；也可能在物理上是远程，但可以将自身验证为本地用户。

您要阻止外部 Internet 上的任意人员使用您的服务器作为中继。使用以下各节所述的配置，您可以区分此类用户并正确地进行阻止。具体来说，您要阻止邮件进入 tcp_local 通道和从同一通道返回。要达到此目的，可以使用 ORIG_SEND_ACCESS 映射表。

ORIG_SEND_ACCESS 映射表可用于基于源通道和目标通道来阻止通信。在这种情况下，来自 tcp_local 通道和返回该通道的通信将被阻止。这可以通过以下 ORIG_SEND_ACCESS 映射表实现：

```
ORIG_SEND_ACCESS

   tcp_local|*|tcp_local|*        $NRelaying$ not$ permitted
```

在此示例中，条目声明邮件不能进入 tcp_local 通道，也不能从该通道直接返回。即，此条目不允许外部邮件进入您的 SMTP 服务器，并不允许外部邮件直接中继回 Internet。

系统使用的是 ORIG_SEND_ACCESS 映射表而非 SEND_ACCESS 映射表，以便阻止不会应用于最初匹配 ims-ms 通道的地址 （但其可能通过别名或邮件列表定义扩展回外部地址）。使用 SEND_ACCESS 映射表，需要很长的长度，才能允许外部人员发送到可扩展回外部用户的邮件列表，或发送到可将其邮件转发回外部地址的用户。

使用 DNS 查找 （包括用于 SMTP 中继阻止的 RBL 检查）

在 Messaging Server 中，有多种不同的方法可以确保所有接收的用于传送或转发的邮件都来自具有有效 DNS 名称的地址。最简单的方法是将 mailfromdnsverify 通道关键字放入 tcp_local 通道。

Messaging Server 还提供了 dns_verify 程序，它使您可以使用 ORIG_MAIL_ACCESS 中的以下规则，确保所有接收的用于传送或转发的邮件都来自具有有效 DNS 名称的地址：

```
ORIG_MAIL_ACCESS

  TCP|*|*|*|*|SMTP|MAIL|*|*@*|*|* \
$[msg_svr_base/lib/dns_verify.so, \
dns_verify,$6|$$y|$$NInvalid$ host:$ $$6$ -$ %e]
```

从句法上来说，以上示例中的换行符在此类映射条目中很显著。反斜杠字符是一种合法地继续到下一行的方法。

dns_verify 映像也可用于检查类似于 RBL （实时黑名单）、 MAPS （邮件滥用防止系统）、 DUL （拨号用户列表）或 ORBS （开放中继修正系统）列表的外来连接，作为另一种防止 UBE 的尝试。对于新的 mailfromdnsverify 关键字，还有一种单独的 “配置简单”的方法可用于这样的检查，而不必执行 dns_verify 调用。这种简单方法是使用 dispatcher.cnf 文件中的 DNS_VERIFY_DOMAIN 选项。例如，在 [SERVICE=SMTP] 部分中，将选项的实例设置为要检查的各个列表：

```
[SERVICE=SMTP]
PORT=25
! ...rest of normal options...
DNS_VERIFY_DOMAIN=rbl.maps.vix.com
DNS_VERIFY_DOMAIN=dul.maps.vix.com
!...etc...
```

在这种情况下，邮件在 SMTP 级别被拒绝 （即，邮件在 SMTP 对话期间被拒绝），因此永远不会被发送到 MTA。这种简单方法的缺点在于，它将对所有正常的外来 SMTP 邮件 （包括那些来自内部用户的邮件）执行检查。这种方法效率较低，并且在 Internet 连接性降低的情况下可能会发生问题。一种备用方法是从 PORT_ACCESS 映射表或 ORIG_MAIL_ACCESS 映射表调用 dns_verify。在 PORT_ACCESS 映射表中，您可以使初始条目不检查本地内部 IP 地址或邮件提交者，较后的条目对其余 IP 地址或邮件提交者进行所需的检查。或者，在 ORIG_MAIL_ACCESS 映射表中，如果您只将检查应用于从 tcp_local 通道进入的邮件，则对于来自内部系统 / 客户机的邮件将跳过检查。示例使用了指向 dns_verify 的条目，如下所示。

```
PORT_ACCESS

! Allow internal connections in unconditionally
  *|*|*|*|*  $C$|INTERNAL_IP;$3|$Y$E
! Check other connections against RBL list
  TCP|*|25|*|* \
$C$[msg_svr_base/lib/dns_verify.so, \
dns_verify_domain_port,$1,rbl.maps.vix.com.]EXTERNAL$E


ORIG_MAIL_ACCESS

  TCP|*|25|*|*|SMTP|*|tcp_local|*@*|*|* \
$C$[msg_svr_base/lib/dns_verify.so, \
dns_verify_domain,$1,rbl.maps.vix.com.]$E
```

支持基于 DNS 的数据库

dns_verify 程序支持基于 DNS 的数据库，该数据库用于确定可能发送未经许可的批量邮件的外来 SMTP 连接。某些公用 DNS 数据库不包含通常用于此用途的 TXT 记录。实际上，它们只包含 A 记录。

在典型设置中，在特定 IP 地址的 DNS 中找到的 TXT 记录包含一个可在拒绝邮件时返回到 SMTP 客户机的错误消息。但是，如果未找到 TXT 记录但找到了 A 记录，则 Messaging Server 5.2 以前的 dns_verify 版本将返回消息 "*No error text available*"。

dns_verify 现在支持一个选项，该选项可在没有可用的 TXT 记录时指定使用的默认文本。例如，以下 PORT_ACCESS 映射表显示了如何启用此选项：

```
PORT_ACCESS

    *|*|*|*|* $C$|INTERNAL_IP;$3|$Y$E  \
    TCP|*|25|*|*  \
```

```
$C$[<msg_svr_base/lib/dns_verify.so  \
,dns_verify_domain_port,$1,dnsblock.siroe.com,Your$ host$ ($1)$  \
found$ on$ dnsblock$ list]$E
    * $YEXTERNAL
```

在此示例中，如果在对域 dnsblock.siroe.com 的查询中找到了远程系统，但没有可用的 TXT 记录，则系统将返回以下消息 "*Your host a.b.c.d found on dnsblock list*"。

处理大量访问条目

在映射表中使用大量条目的站点应考虑将其映射表组织为具有若干配备通用通配符的条目，这些条目可以调用通用数据库来进行特定的查找。针对特定查找，使用若干映射表条目调用通用数据库比直接在映射表中使用大量的条目效率要高得多。

一个特例是某些站点希望对谁可以发送和接收 Internet 电子邮件进行基于单个用户的控制。使用诸如 ORIG_SEND_ACCESS 的访问映射表可以很方便地实现此类控制。对于这种用法，通过将大量特定信息（例如特定地址）存储在通用数据库中，同时结构化映射表条目以对通用数据库进行适当调用，可以显著提高效率和性能。

例如，请考虑下面所示的 ORIG_SEND_ACCESS 映射表。

```
ORIG_SEND_ACCESS

! Users allowed to send to Internet
!
  *|adam@siroe.com|tcp_local|*    $Y
  *|betty@siroe.com|tcp_local|*   $Y
! ...etc...
!
! Users not allowed to send to Internet
!
  *|norman@siroe.com|tcp_local|*  $NInternet$ access$ not$ permitted
  *|opal@siroe.com|tcp_local|*    $NInternet$ access$ not$ permitted
! ...etc...
!
! Users allowed to receive from the Internet
!
  tcp_*|*|*|adam@siroe.com        $Y
  tcp_*|*|*|betty@siroe.com       $Y
! ...etc...
!
! Users not allowed to receive from the Internet
!
  tcp_*|*|*|norman@siroe.com      $NInternet$ e-mail$ not$ accepted
  tcp_*|*|*|opal@siroe.com        $NInternet$ e-mail$ not$ accepted
! ...etc...
```

与通过每个用户单独输入表中的此类映射表相比，下面示例中显示了一种更有效的设置 （如果包括成百上千个用户条目，则更为有效），它显示了常规数据库的样例源文本文件和样例 ORIG_SEND_ACCESS 映射表。要将此源文件编译成数据库格式，请运行 imsimta crdb 命令：

```
% imsimta crdb input-file-spec  output-database-spec
```

有关 imsimta crdb 实用程序的详细信息，请参见 Sun Java System Messaging Server Administration Reference。

DATABASE ENTRIES

```
SEND|adam@domain.com    $Y
SEND|betty@domain.com   $Y
! ...etc...
SEND|norman@domain.com  $NInternet$ access$ not$ permitted
SEND|opal@domain.com    $NInternet$ access$ not$ permitted
! ...etc...
RECV|adam@domain.com    $Y
RECV|betty@domain.com   $Y
! ...etc...
RECV|norman@domain.com  $NInternet$ e-mail$ not$ accepted
RECV|opal@domain.com    $NInternet$ e-mail$ not$ accepted
```

MAPPING TABLE

```
ORIG_SEND_ACCESS

! Check if may send to Internet
!
  *|*|*|tcp_local       $C${SEND|$1}$E
!
! Check if may receive from Internet
!
  tcp_*|*|*|*           $C${RECV|$3}$E
```

此示例中，在通用数据库中左侧任意字符串 SEND| 和 RECV| 的使用 （以及由此在映射表生成的通用数据库探测中）提供了一种区分所生成的两类探测的方法。如图所示，用 $C 和 $E 标志环绕通用数据库探测在映射表调用通用数据库中很典型。

以上示例显示了根据通用数据库条目检查简单映射表探测的情况。具有复杂得多的探测的映射表也可以从使用通用数据库中受益。

第 2 部分：邮箱过滤器

邮箱过滤器 （也称为 Sieve 过滤器），过滤在邮件标题中包含指定字符串的邮件并对这些邮件应用指定操作。管理员可以过滤通过通道或 MTA 传送到用户的邮件流。Messaging Server 过滤器存储在服务器上并由服务器评估，因此，这些过滤器有时称为服务器端规则 (SSR)。

本部分包含以下各节：

- 第 482 页的 “Sieve 过滤概述”
- 第 482 页的 “创建用户级别的过滤器”
- 第 483 页的 “创建通道级别的过滤器”
- 第 485 页的 “创建 MTA 范围内的过滤器”
- 第 486 页的 “调试用户级别的过滤器”

Sieve 过滤器支持

Messaging Server 过滤器基于 Sieve 过滤语言 (Draft 9 of the Sieve Internet Draft)。有关 Sieve 语法和语义的更多信息，请参见 RFC3028。此外， Messaging Server 还支持以下 Sieve 扩展：

- **`jettison`**。在无提示删除邮件方面， `jettison` 与 `discard` 类似；不同的是，discard 只取消隐含保留而不进行任何操作，而 `jettison` 将强制执行 `discard`。这种行为差异仅在涉及到多个 Sieve 过滤器时才比较明显。例如，系统级别的 discard 可由明确指定 `keep` 的用户 Sieve 过滤器替换，而系统级别的 `jettison` 将替换用户 Sieve 执行的任何操作。
- **户主 Sieve 过滤器**。提供了一个用户为另一个用户指定 Sieve 过滤器的方法。使用由以下 MTA 选项控制的用户条目中的两个 LDAP 属性：
  - `LDAP_PARENTAL_CONTROLS` — 指定包含字符串值 `Yes` 或 `No` 的属性。`Yes` 表示将对此条目应用户主 Sieve， `No` 表示将不应用此类 Sieve。无默认值。
  - `LDAP_FILTER_REFERENCE` — 指定包含 DN 的属性，该 DN 指向可以找到户主 Sieve 的目录条目。无默认值。

  包含户主 Sieve 的条目必须包含由以下 MTA 选项指定的两个属性：

  - `LDAP_HOH_FILTER` — 指定包含户主 Sieve 属性。此选项的默认值为 `mailSieveRuleSource`。

- LDAP_HOH_OWNER — 指定包含户主拥有者的电子邮件地址的属性。此选项的默认值为 mail。

这两个属性必须同时存在才能使户主 Sieve 运行。

Sieve 过滤概述

Sieve 过滤器由一个或多个要应用于邮件的条件操作组成 （取决于邮件标题中的字符串）。作为管理员，您可以创建通道级别的过滤器和 MTA 范围内的过滤器，用以防止传送不需要的邮件。用户可以使用 Messenger Express 为其自己的邮箱创建基于用户的过滤器。 Messenger Express 联机帮助对此进行了详细的说明。

服务器按照以下优先级应用过滤器：

1. 用户级别的过滤器

   如果个人邮箱过滤器明确接受或拒绝一个邮件，则过滤器对该邮件的处理完成。但是如果收件人用户没有邮箱过滤器 — 或用户的邮箱过滤器没有明确应用到有问题的邮件 — Messaging Server 接着将应用通道级别的过滤器。设置基于用户的过滤器。

2. 通道级别的过滤器

   如果通道级别的过滤器明确接受或拒绝一个邮件，则过滤器对该邮件的处理完成。否则， Messaging Server 接着将应用 MTA 范围内的过滤器 （如果有）。

3. MTA 范围内的过滤器

默认情况下，所有用户均没有邮箱过滤器。用户使用 Messenger Express 界面创建一个或多个过滤器时，他们的过滤器将存储在目录中，并在目录同步进程期间由 MTA 进行检索。

创建用户级别的过滤器

基于用户的邮件过滤器将应用于发往特定用户的邮箱的邮件。只能使用 Messenger Express 创建基于用户的邮件过滤器。

创建通道级别的过滤器

通道级别的过滤器将应用于在通道内排队的每个邮件。此类过滤器的典型用途是阻止通过特定通道的邮件。

要创建通道级别的过滤器，请执行以下步骤：

1. 使用 Sieve 编写过滤器。
2. 将过滤器存储在位于以下目录的文件中：

   `../config/`*file*`.filter`

   该文件必须可全局读取，并属于 `MTA` 的 `uid`。
3. 将以下内容包括在通道配置中：

   `destinationfilter file:IMTA_TABLE:`*file*`.filter`
4. 重新编译配置并重新启动分发程序。

   请注意，对过滤器文件所作的更改无需重新编译或重新启动分发程序。

`destinationfilter` 通道关键字将为排队**到**应用邮件过滤功能的通道的邮件启用邮件过滤。`sourcefilter` 通道关键字将为**来自**应用邮件过滤功能的通道队列的邮件启用邮件过滤。这些关键字都有一个必需参数，该参数指定了与通道关联的相应通道过滤器文件路径。

`destinationfilter` 通道关键字的语法为：

`destinationfilter` *URL-pattern*

`sourcefilter` 通道关键字的语法为：

`sourcefilter` *URL-pattern*

其中 *URL-pattern* 是一个 URL，指定了到有问题的通道的过滤器文件的路径。在以下示例中， *channel-name* 为通道的名称。

`destinationfilter file:///usr/tmp/filters/`*channel-name*`.filter`

`filter` 通道关键字使应用邮件过滤的通道启用了邮件过滤。该关键字有一个必需参数，该参数指定了与通过通道接收邮件的每个信封收件人关联的过滤器文件路径。

`filter` 通道关键字的语法为：

`filter` *URL-pattern*

URL-pattern 是一个 URL，在进行特殊替换序列处理后，将生成给定收件人地址的过滤器文件路径。*URL-pattern* 可以包含特殊替换序列，遇到此序列时，将被源自收件人地址（有问题的 `local-part@host.domain`）的字符串替代。表 17-4 第 484 页中显示了这些替换序列。

`fileinto` 关键字指定在应用了邮箱过滤器 `fileinto` 运算符时如何更改地址。以下示例指定了文件夹名称应作为子地址插入原始地址，替代原先存在的任何子地址：

```
fileinto $U+$S@$D
```

表 17-4 `filter` 通道关键字 *URL-pattern* 替换标记（不区分大小写）

标记	含义
*	执行组扩展。
**	扩展属性 `mailForwardingAddress`。这可以是一个导致产生若干传送地址的多值属性。
$$	在 $ 字符中替换
$\	强制后续文本转为小写
$^	强制后续文本转为大写
$_	不对后续文本执行大小写转换
$~	在与地址本地部分关联的主目录的文件路径中替换
$1S	与 `$S` 相同，但如果没有可用的子地址，则什么也不插入
$2S	与 `$S` 相同，但如果没有可用的子地址，则什么也不插入，并删除前面的字符
$3S	与 `$S` 相同，但如果没有可用的子地址，则什么也不插入，并忽略以后的字符
$A	在地址 local-part@ host.domain 中替换
$D	在 host.domain 中替换
$E	插入第二个备用属性 `LDAP_SPARE_1` 的值
$F	插入传送文件的名称（`mailDeliveryFileURL` 属性）
$G	插入第二个备用属性 `LDAP_SPARE_2` 的值
$H	在主机中替换
$I	插入托管域（`domainUidSeparator` 指定的分隔符右侧的 UID 的一部分）。如果没有可用的托管域，则失败
$1I	与 `$I` 相同，但如果没有可用的托管域，则什么也不插入
$2I	与 `$I` 相同，但如果没有可用的托管域，则什么也不插入，并删除前面的字符
$3I	与 `$I` 相同，但如果没有可用的托管域，则什么也不插入，并忽略以后的字符
$L	在本地部分中替换

表 17-4 filter 通道关键字 *URL-pattern* 替换标记 （不区分大小写）

标记	含义
$M	插入 UID，分流任何托管域
$P	插入方法名称 （mailProgramDeliveryInfo 属性）
$S	插入与当前地址关联的子地址。子地址是原始地址的用户部分中子地址分隔符 （通常为 +）之后的部分，可由 MTA 选项 SUBADDRESS_CHAR 指定。如果没有给定子地址，则失败
$U	插入当前地址的邮箱部分。这可以是 @ 符号左侧的全部地址，也可以是地址左侧、子地址分隔符 + 之前的部分。

创建 MTA 范围内的过滤器

MTA 范围内的过滤器将应用于排队到 MTA 的所有邮件。此类过滤器的典型用途是阻止未经许可的批量邮件或其他不需要的邮件，而不管邮件的目的地为何。要创建 MTA 范围内的过滤器，请执行以下步骤：

1. 使用 Sieve 编写过滤器
2. 将过滤器存储在以下文件中：

   ../imta/config/imta.filter

   此过滤器文件必须可全局读取。如果该文件存在，将自动进行使用。
3. 重新编译配置并重新启动分发程序

使用已编译的配置时， MTA 范围内的过滤器文件将被包含到已编译的配置中。

将已放弃的邮件路由出 FILTER_DISCARD 通道

默认情况下，通过邮箱过滤器放弃的邮件将立即从系统放弃 （删除）。但是，用户初次设置邮箱过滤器 （并可能犯错误）时，或出于调试目的，则使删除操作延迟一段时间可能会很有用。

要使邮箱过滤器放弃的邮件临时保留在系统中以日后删除，请首先将 filter_discard 通道添加到 MTA 配置，并使用 notices 通道关键字指定删除邮件前保留邮件的时间长度 （通常为天数），如以下示例所示：

```
filter_discard notices 7
FILTER-DISCARD
```

然后在 MTA 选项文件中设置选项 FILTER_DISCARD=2。 filter_discard 队列区域中的邮件应被看作位于用户的个人废纸篓文件夹的扩展中。因此，请注意对于 filter_discard 队列区域中的邮件，系统永远不会发送警告消息，也不会在请求弹回或返回时，将此类邮件返回其发件人。而对于此类邮件采取的唯一操作是，在最后通知值过期，或使用实用程序 （例如 imsimta return）请求手动弹回时，最终无提示地删除这些邮件。

在 Messaging Server 6 2004Q2 之前，由 FILTER_DISCARD MTA 选项控制 jettison Sieve 操作对 filter_discard 通道的使用。现在，此操作由选项 FILTER_JETTISON 控制，该选项从 FILTER_DISCARD 设置中接受其默认值。而 FILTER_DISCARD 的默认值为 1（放弃将转至 bitbucket 通道）。

调试用户级别的过滤器

如果用户抱怨 Sieve 过滤器的表现未达到预期效果，您可以采取许多措施来调试过滤器。下面对这些步骤进行了介绍。

1. 为了使 fileinto 过滤能够工作，请在 imta.cnf 文件 （ims-ms 通道将其标记为以下形式）中检查该过滤：

   ```
   fileinto $u+$s@$d
   ```

2. 从用户 LDAP 条目中获取用户级别过滤器。

   用户级别过滤器储存在 MailSieveRuleSource 属性下的 LDAP 条目中。要使用 ldapsearch 命令来检索此过滤器，请记住它们是 base64 编码，因此您需要使用 -Bo 参数选项对输出进行解码。

   ```
   ./ldapsearch -D "cn=directory manager" -w password -b
   "o=alcatraz.sesta.com,o=isp" -Bo uid=test
   ```

   以下所述的 imsimta test -rewrite 命令也将自动对它们进行解码。

3. 检验 MTA 是否正在查看用户过滤器。

   发出命令：

   ```
   # imsimta test -rewrite -filter -debug user@sesta.com
   ```

   此命令应该输出在前面的步骤中检索的用户 Sieve 过滤器。如果未看见过滤器，则需要指出为什么 LDAP 条目未返回这些过滤器。如果 imsimta test -rewrite 输出显示过滤器，则表明 MTA 正在查看用户过滤器。下一步将使用 imsimta test -expression 命令测试过滤器的解释。

4. 使用 imsimta test -exp 调试用户过滤器。需要以下信息：

   a. mailSieveRuleSource 属性中的用户 Sieve 语言语句。请参见以上步骤。

   b. 触发过滤器的 rfc2822 邮件。

   c. 描述过滤器应对邮件进行什么操作。

5. 创建文本文件 （例如：temp.filter），该文本文件包含基于用户 mailSieveRuleSource: values 的 Sieve 语言语句。示例：

```
require "fileinto";
if anyof(header :contains
["To","Cc","Bcc","Resent-to","Resent-cc",
   "Resent-bcc"] "commsqa"){
   fileinto "QMSG";
}
```

   预期结果：如果 commsqa 是此邮件的收件人，则将邮件归档到名为 QMSG 的文件夹中。

6. 创建名为 test.msg 的文本文件，该文件包含用户提供的 rfc2822 邮件文件的内容。

   您可以使用用户邮件存储区域中的 .msg 文件，也可以创建名为 test_rfc2822.msg 的文本文件，该文件包含用户提供的 rfc2822 邮件文件的内容。

7. 使用 imsimta test -exp 命令：

```
# imsimta test -exp -mm -block -input=temp.filter -message=test_rfc2822.msg
```

8. 检查输出。

   imsimta test -exp 命令的最后几行将显示 Sieve 解释的结果。结果类似于：

```
Sieve Result: []
```

   或：

```
Sieve Result: [action]
```

   其中， *action* 是作为在此邮件上应用 Sieve 过滤器的结果而要执行的操作。

   如果过滤器的条件匹配，则会得到显示为结果的某个操作。如果没有匹配项，Sieve 结果将为空，原因是 Sieve 过滤器中存在逻辑错误或 .msg 文件不包含匹配信息。如果收到任何其他错误，则 Sieve 脚本文件中存在语法错误，您需要对其进行调试。

   有关输出的详细信息，请参见 第 488 页的 “imsimta test -exp 输出”。

9. 如果过滤器的语法有效并且结果正确，下一步将检查 tcp_local_slave.log 调试日志文件。

   可能会出现正在测试的邮件文件与正在发送的邮件文件不相同的情况。要查看正在接收什么邮件的唯一方法是：检查 tcp_local_slave.log 文件。此日志将向您显示正在发送到 MTA 的实际邮件以及如何将过滤器应用到该邮件。

   有关获取 tcp_local_slave.log 调试文件的更多信息，请参见第 352 页的 “调试关键字”中的 slave_debug 关键字。

imsimta test -exp 输出

完整命令 imsimta test -exp 如下：

```
# imsimta test -exp -mm -block -input=temp.filter -message=rfc2822.msg
```

下面是一个输出示例：

代码示例 17-4 imsimta test -exp 输出

```
# imsimta test -exp -mm -block -input tmp.filter -message=rfc2822.msg
Expression: if header :contains ["to"] ["pamw"]          (1)
Expression: {
Expression: redirect "usr3@sesta.com";
Expression: keep;
Expression: }
Expression:
Expression: Dump: header:2000114;0  3  1  :contains  1  "to"  1
"pamw"  if  8  ;
Dump: redirect:2000121;0  1  1  "usr3@sesta.com"  ;  keep:2000117;0  (2)
Dump: 0
Result: 0
Filter result: [ redirect "usr3@sesta.com" keep ]   (3)
```

1) Expression: 输出行显示从 tmp.filter 文本文件中读取和解析的过滤器。这些在调试脚本中不是特别有用。

2) Dump: 输出行是计算机解释 Sieve 语句的结果。不应看到有任何错误，并且输出看起来应与输入相匹配。例如 dump 显示了 redirect, usr3@sesta.com，与过滤器文件中的行 redirect "usr3@sesta.com"; 类似。

如果未显示此匹配文本，则应当引起注意，否则，它们在调试脚本时也不是特别有用。

3) 在输出的底部，您将得到 `Filter result:` 语句。如前面所述，可能有两种结果：

`Sieve Result: []` 或： `Sieve Result: [`*action*`]`

其中 action 是 Sieve 脚本执行的操作。请注意，有时预期的结果为空。例如，对于 discard 过滤器，您应当测试该过滤器是否始终丢弃每个 .msg 文件，它们是测试该过滤器时需要参照的文件。如果在方括号间存在某个操作，例如：

```
Filter result: [ fileinto "QMSG" keep]
```

这表明 `rfc2822.msg` 文件中的文本与过滤器条件匹配。在这个特定示例中，过滤器将把邮件归档到 `QMSG` 文件夹中，并在收件箱中保存一份副本。本示例中产生的操作是 `fileinto` 和 `keep`。

测试过滤器时，应当测试两个结果的各个 `.msg` 文件。应始终测试是否已过滤匹配过滤器的邮件，并测试是否未过滤不想匹配的邮件。

请记住，对于通配符匹配，您必须使用 `:matches` 测试而不要使用 `:contains`。例如，如果要匹配 `from=*@sesta.com`，则必须使用 `:matches`，否则测试将由于不满足测试条件而失败。

imsimta test -exp 语法

`imsimta test -exp` 将针对指定的 RFC2822 邮件测试 Sieve 语言语句，并将过滤器的结果发送到标准输出。

语法如下：

```
imsimta test -exp -mm -block -input=Sieve_language_scriptfile
-message=rfc2822_message_file
```

其中，

`-block` 将所有输入视为一个 Sieve 脚本。默认情况下，将每行作为一个单独的脚本，并分别对其进行评估。仅在到达文件末端时评估 Sieve。

`-input=`*Sieve_file* 是包含 Sieve 脚本的文件。默认情况下，将从 stdin 中读取测试脚本行或脚本块。

`-message=`*message_file* 是一个文本文件，包含测试 Sieve 脚本所参照的 RFC 2822 邮件。这只能是 RFC 2822 邮件。而不能是队列文件 （不是 zz*.00 文件）。

激活后，此命令将读取脚本信息，在测试邮件的上下文中评估该信息，并写出结果。结果显示将进行什么操作以及脚本中最终语句的评估结果。

其他有用的限定符包括：

`-from=`*address* 指定要在信封测试中使用的信封 `from:` 地址。默认情况下，使用由 `RETURN_ADDRESS` MTA 选项指定的值。

`-output=`*file* 将结果写入 *file*。默认情况下，将脚本测试结果写入 stdout 中。

第 18 章

管理邮件存储

本章介绍了邮件存储和邮件存储管理界面。本章包含以下各节：

- 第 492 页的 “概述”
- 第 493 页的 “邮件存储目录布局”
- 第 496 页的 “邮件存储如何删除邮件”
- 第 497 页的 “指定管理员对存储的访问权限”
- 第 499 页的 “关于共享文件夹”
- 第 503 页的 “共享文件夹任务”
- 第 509 页的 “关于邮件存储配额”
- 第 512 页的 “配置邮件存储配额”
- 第 518 页的 “设置自动删除邮件 （过期和清除）功能”
- 第 529 页的 “配置邮件存储分区”
- 第 532 页的 “执行邮件存储维护过程”
- 第 543 页的 “备份并恢复邮件存储”
- 第 556 页的 “监视用户访问”
- 第 557 页的 “邮件存储故障排除”

概述

邮件存储包含特定 Messaging Server 实例的用户邮箱。邮件存储的大小随邮箱、文件夹和日志文件的数量的增加而增加。可以通过指定对邮箱大小 （磁盘配额）的限制、指定对允许的邮件总数的限制以及为存储中的邮件设置生存期策略来控制存储的大小。

向系统添加更多用户时，磁盘存储要求会相应增加。根据服务器支持的用户的数量，邮件存储可能需要一个物理磁盘或多个物理磁盘。将此附加磁盘空间集成到系统中的方法有两种。最简单的方法是添加附加邮件存储分区 （请参见第 529 页的“配置邮件存储分区”）。

同样，如果要支持多个托管域，您可能需要将一个服务器实例专用于一个大型域。通过此配置，您可以为特定域指定存储管理员。还可以通过添加更多分区扩展邮件存储。

为管理邮件存储，除了 Sun Java System Console 界面，Messaging Server 还提供了一系列命令行实用程序。表 18-1 介绍了这些命令行实用程序。有关使用这些实用程序的信息，请参见第 532 页的 “执行邮件存储维护过程”和 Messaging Server Reference Manual。

表 18-1 邮件存储命令行实用程序

实用程序	说明
configutil	设置和修改存储的配置参数。
deliver	将邮件直接传送至 IMAP 或 POP 邮件客户机可以访问的邮件存储。
hashdir	标识包含用于特定用户的邮件存储的目录。
imsconnutil	监视邮件存储的用户访问。
imexpire	根据管理员指定的条件 （如生存期）自动从邮件存储中删除邮件。
iminitquota	从 LDAP 目录重新初始化配额限制并重新计算要使用的磁盘空间。
imsasm	处理用户邮箱的保存和恢复。
imsbackup	备份已存储邮件。
imsexport	将 Certificate Management System 邮箱导出至 UNIX /var/mail 格式文件夹中。
imsrestore	恢复已备份的邮件。
imscripter	IMAP 服务器协议脚本撰写工具。执行一个命令或一序列命令。
mboxutil	列出、创建、删除、重命名或移动邮箱；报告配额使用情况。
mkbackupdir	创建备份目录并使其与邮件存储中的信息同步。

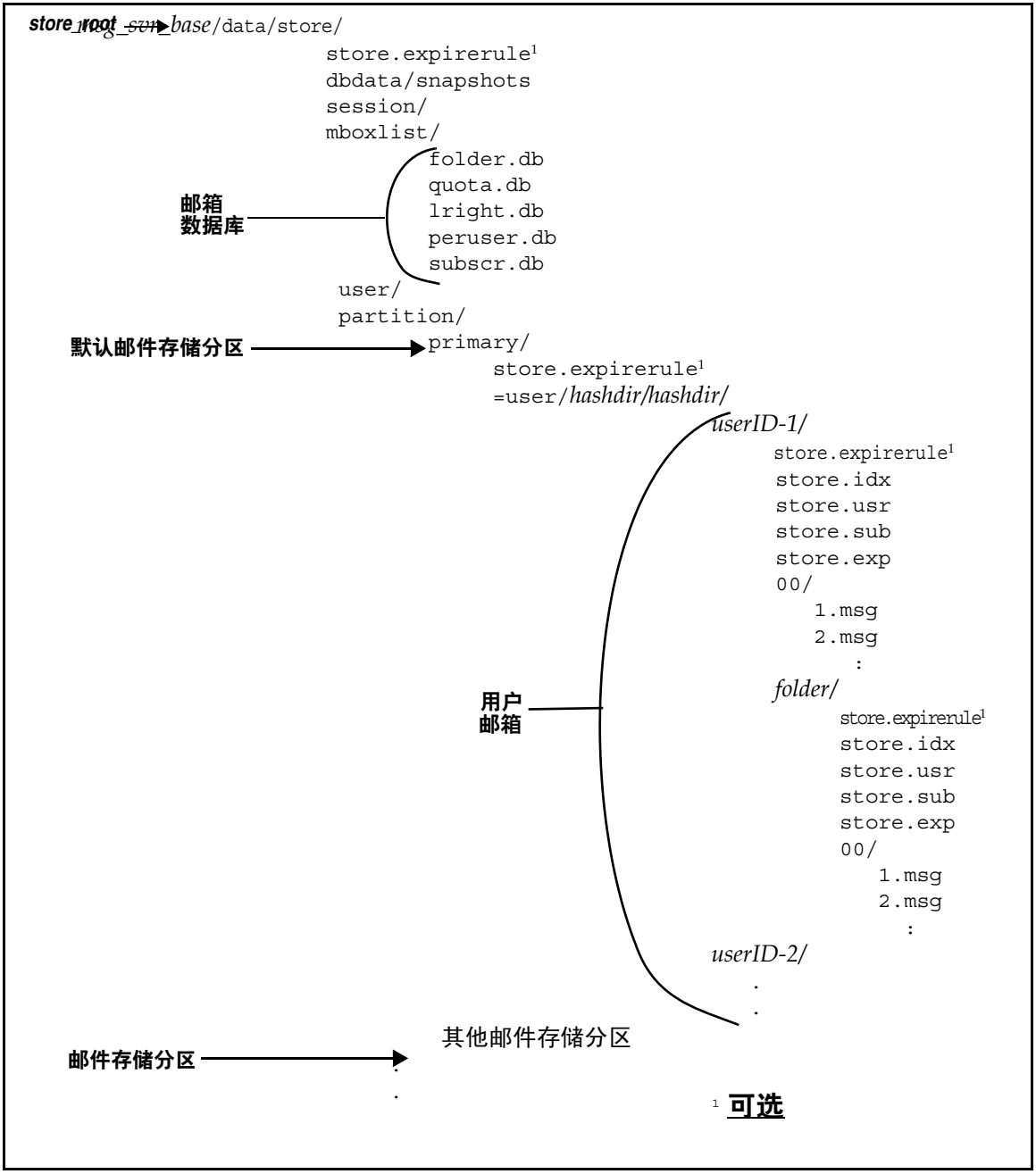
表 18-1 邮件存储命令行实用程序

实用程序	说明
MoveUser	将用户的帐户从一个邮件传送服务器移动到另一个邮件传送服务器。
imquotacheck	计算邮件存储中每个用户的邮箱总大小，并与其指定的配额进行比较。 imquotacheck 通知的本地化版本未正确转换 % 和 $ 符号。要更正编码，请将邮件文件中的每个 $ 替换为 \24，将每个 % 替换为 \25。
readership	收集共享 IMAP 文件夹中的读者身份信息。
reconstruct	重建已被损坏或破坏的邮箱。
stored	执行后台任务和每日任务，擦除和删除磁盘上存储的邮件。

邮件存储目录布局

图 18-1 显示了服务器实例的邮件存储目录布局。邮件存储用于提供对邮箱内容的快速访问。表 18-2 中介绍了存储目录。

图 18-1 邮件存储目录布局



邮件存储由许多邮箱数据库和用户邮箱组成。邮箱数据库由有关用户、邮箱、分区、配额的信息和其他与邮件存储相关的数据组成。用户邮箱包含用户的邮件和文件夹。邮箱存储在**邮件存储分区**，即专门用于存储邮件存储的**磁盘**分区上的一个区域。有关详细信息，请参见第 529 页的 “配置邮件存储分区”。虽然为了易于维护，我们建议每个邮件存储分区使用一个磁盘分区，但是邮件存储分区与磁盘分区并不相同。

邮箱 （例如 INBOX）位于 *store_root* 中。例如，样例目录路径可能如下所示：

store_root/partition/primary/=user/53/53/=mack1

下表介绍了邮件存储目录。

表 18-2 邮件存储目录说明

位置	内容 / 说明
msg_svr_base	默认值：/opt/SUNWmsgsr Messaging Server 计算机上用于保存服务器程序文件、配置文件、维护文件和信息文件的目录。
store_root	*msg_svr_base*/data/store/ 邮件存储的顶层目录。包含 mboxlist、 user 和 partition 子目录。
./store.expirerule	包含自动删除邮件规则 （过期规则）。此可选文件可位于不同位置。请参见第 518 页的 “设置自动删除邮件 （过期和清除）功能”。
store_root/dbdata/snapshots	邮件存储数据库备份快照。
store_root/mboxlist/	包含邮箱数据库，即存储有关邮箱的信息和配额信息的数据库 (Berkeley DB)。 folder.db 包含有关邮箱的信息，包括存储邮箱的分区的名称、 ACL 和 store.idx 中某些信息的副本。在 folder.db 中每个邮箱具有一个条目。 quota.db 包含有关配额和配额使用情况的信息。在 quota.db 中每个用户具有一个条目。 lright.db — 按 ACL 查找权限排列的文件夹的索引。 peruser.db 包含有关每个用户标志的信息。这些标志表示特定用户是否已阅读或已删除邮件。 subscr.db 包含有关用户订阅的信息。
store_root/session/	包含活动邮件存储进程的信息。
store_root/user/	不使用。
store_root/partition/	包含邮件存储分区。已创建默认 primary 分区。将您定义的所有其他分区放在此目录中。
store_root/partition/primary/=user/	包含分区的子目录中的所有用户邮箱。邮箱以散列结构存储，以便进行快速搜索。要查找包含特定用户邮箱的目录，请使用 hashdir 实用程序。

表 18-2 邮件存储目录说明

位置	内容 / 说明
.../=user/*hashdir*/*hashdir*/*userid*/	ID 为 *userid* 的用户的顶层邮件文件夹。这是用户的 INBOX。对于默认域，*userid* 是 *uid*。对于托管域， *userid* 是 *uid*@*domain*。外来邮件被传送到此邮件文件夹。
.../*userid*/*folder*	邮件传送服务器上用户定义的邮箱。
.../*userid*/store.idx	一个索引，提供有关 /*userid*/ 目录中存储的邮件的以下信息：邮件数量、此邮箱所用的磁盘配额、上次附加邮箱的时间、邮件标志、每封邮件的变量长度信息 （包括标题和 MIME 结构）以及每封邮件的大小。该索引还包括每个用户的 mboxlist 信息的备份副本和每个用户的配额信息的备份副本。
.../*userid*/store.usr	包含已访问文件夹的用户的列表。对于每个列出的用户，此目录都包含有关用户上次访问文件夹的时间、用户已读邮件列表和用户已删除邮件列表的信息。
.../*userid*/store.sub	包含有关用户订阅的信息。
.../*userid*/store.exp	包含已擦除但未从磁盘删除的邮件文件的列表。仅在有被擦除的邮件时才显示此文件。
.../*userid*/*nn*/ or .../*userid*/*folder*/*nn*/	*nn* 是一个包含格式为 *message_id*.msg 的邮件的散列目录；*nn* 可以是从 00 至 99 之间的数字。 *message_id* 也是一个数字。示例：邮件 1 至 99 存储在 .../00 目录中。第一封邮件是 1.msg，第二封邮件是 2.msg，第三封邮件是 3.msg，依此类推。邮件 100 至 199 存储在 01 目录中；邮件 9990 至 9999 存储在 99 目录中；邮件 10000 至 10099 存储在 00 目录中，依此类推。

邮件存储如何删除邮件

从邮件存储中删除邮件分三个阶段：

1. **删除**。客户机将邮件标志设置为**删除**。此时邮件被标记为删除，但是通过去掉删除标志，客户机仍然可以恢复邮件。如果有第二个客户机，则已删除标志可能不会立即被该客户机识别。可以设置 configutil 参数 local.imap.immediateflagupdate 以使标志立即更新。

2. **擦除**。邮件将从邮箱中删除。从技术上讲，邮件将从邮件存储索引文件 store.idx 中删除。邮件本身仍然在磁盘上，但是一旦邮件被擦除，客户机将不能再恢复邮件。

   过期是擦除的一个特例。符合管理员定义的一组删除条件 （例如邮件大小、生存期等）的邮件将被擦除。请参见第 518 页的 “设置自动删除邮件 （过期和清除）功能”。

3. **清除**。默认情况下， stored 实用程序将在每天晚上 11 点从磁盘上清除所有已被擦除的邮件。可以使用控制邮件清除时间安排的 local.schedule.purge 和控制清除宽限期 （邮件被清除之前的时间段）的 store.cleanup 配置此功能。

指定管理员对存储的访问权限

邮件存储管理员可以查看和监视用户邮箱，并指定邮件存储的访问控制。存储管理员具有对任何服务 （POP、 IMAP、 HTTP 或 SMTP）的代理验证权限，这意味着他们可以使用任何用户的权限对任何服务进行验证。这些权限允许存储管理员运行特定的实用程序以管理存储。例如，存储管理员使用 `MoveUser` 可以将用户帐户和邮箱从一个系统移动到另一个系统。

本节介绍如何将存储权限授予邮件存储以进行 Messaging Server 安装。

注	其他用户可能也具有对存储的管理员权限。例如，某些管理员可能具有这些权限。

您可以执行以下小节中所述的管理员任务：

- 添加管理员
- 修改管理员条目
- 删除管理员条目

添加管理员

Console 要通过 Console 添加管理员条目，请执行以下操作：

1. 从 Console 中打开要配置的 Messaging Server。
2. 单击 “配置” 选项卡，并在左窗格中选择 “邮件存储”。
3. 单击 “管理员” 选项卡。

   该选项卡包含现有管理员 ID 的列表。
4. 单击 “管理员 UID” 窗口旁边的 “添加” 按钮。
5. 在 “管理员 UID” 字段中，键入要添加的管理员的用户 ID。

   键入的用户 ID 必须是 Sun Java System Directory Server 所知晓的。
6. 单击 “确定” 以将管理员 ID 添加到 “管理员” 选项卡中显示的列表。
7. 单击 “管理员” 选项卡中的 “保存” 以保存新修改的 “管理员” 列表。

命令行 要通过命令行添加管理员条目，请使用以下命令：

```
configutil -o store.admins -v "adminlist"
```

其中 *adminlist* 是以空格分隔的管理员 ID 的列表。如果指定多个管理员，必须将列表包含在引号中。此外，管理员必须是服务管理员组的成员 （位于 LDAP 用户条目：`memberOf:cn=Service Administrators,ou=Groups,o=usergroup`）。

修改管理员条目

Console 要通过 Console 修改邮件存储 “管理员 UID”列表中的现有条目，请执行以下操作：

1. 单击 “管理员”选项卡。
2. 单击 “管理员 UID”窗口旁边的 “编辑”按钮。
3. 将更改输入 “管理员 UID”字段。
4. 单击 “确定”以提交更改并关闭 “编辑管理员”窗口。
5. 单击 “管理员”选项卡中的 “保存”以提交并保存已修改的 “管理员”列表。

命令行 要通过命令行修改邮件存储 “管理员 UID”列表中的现有条目，请运行以下命令：

```
configutil -o store.admins -v "adminlist"
```

删除管理员条目

Console 要使用 Console 从邮件存储 “管理员 UID”列表中删除条目，请执行以下操作：

1. 单击 “管理员”选项卡。
2. 在 “管理员 UID”列表中选择一项。
3. 单击 “删除”以删除该项。
4. 单击 “保存”以提交并保存对 “管理员”列表的更改。

命令行 要通过命令行删除存储管理员，可以如下所示编辑管理员列表：

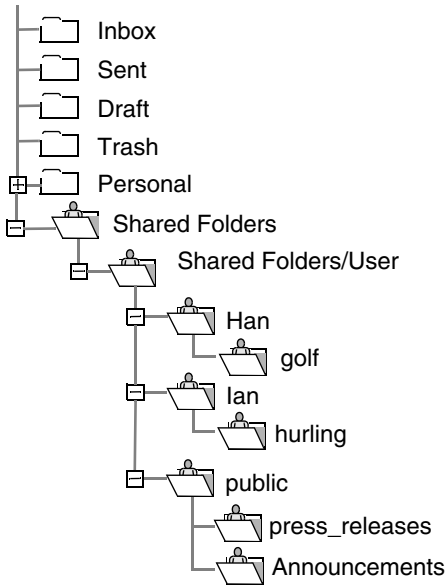
```
configutil -o store.admins -v "adminlist"
```

关于共享文件夹

共享文件夹是可以由一组用户访问和读取的文件夹。也就是说，多个用户被授予对共享文件夹的访问权限。例如，用户可以创建一个名为 `golf` 的文件夹，并允许其他用户查看该文件夹的内容。

默认情况下， Messaging Server 在所有电子邮件帐户中都创建一个名为 `Shared Folders/Users` 的文件夹。用户在该文件夹中创建和访问共享文件夹。图 18-2 中显示了共享文件夹在客户机上如何显示的示例。在第 505 页的 “设置分布式共享文件夹”中将进一步说明该示例。

图 18-2 Ed 的客户机共享邮件文件夹列表的示例



用户可以创建专用共享文件夹，并为其电子邮件客户机提供对这些文件夹的访问权限 （如果客户机支持共享文件夹）。这些共享文件夹将会显示在已被授予访问权限的其他用户的 `Shared Folders` 中。

共享文件夹对于启动、共享和归档正在进行的有关特定主题的对话非常有用。例如，一组软件开发者可以创建用于讨论特定项目的开发的共享文件夹。邮件发送到共享文件夹时，每个订阅共享文件夹的用户 （可以通过单个地址或一组地址添加订户）都可以打开此邮箱并阅读邮件。

有两种共享文件夹：

- **专用** — 专用共享文件夹是特定用户所拥有的共享文件夹。文件夹的所有者可以将访问权限授予其他用户。
- **公用** — 公用共享文件夹没有拥有者。管理员可创建公用用户帐户，该帐户可用于托管公用文件夹。公用文件夹的电子邮件地址类似如下所示：

  `public+`*`foldername`*`@`*`domain`*

  例如，您可能需要一个文件夹 （例如 `public+software_dev@siroe.com`）用于邮寄有关公司内部特殊兴趣组的信息。可以授予有兴趣的员工对此公用文件夹的访问权限。

通常，只有特定邮件存储中的用户才可以使用共享文件夹。但是， Messaging Server 允许您创建可以从多个邮件存储中访问的特殊共享文件夹。这些文件夹称为**分布式共享文件夹**。有关详细信息，请参见第 505 页的 “设置分布式共享文件夹”。

共享文件夹访问权限

在存储在 `folder.db` 中的访问控制列表 (ACL) 中维护访问权限。通过设置 ACL 可以完成授予访问权限的操作。使用 IMAP `SETACL` 命令、 `-s` 选项和 `readership` 命令行实用程序 （请参见第 504 页的 “更改公用文件夹的访问控制权限”）或使用 Messenger Express 界面均可以设置 ACL。

ACL 标识符

每个 ACL 条目都有一个标识符，用于指定条目所适用的用户或用户组。以短划线 ("-") 开头的标识符表示否定权限 （这些条目被拒绝用于用户或组）。

`anyone` 是一个特殊的标识符。 `anyone` 的访问权限适用于所有用户。类似地，`anyone@`*`domain`* 的访问权限适用于同一域中的所有用户。

组标识符以 `group=` 开始。

ACL 权限字符

每个 ACL 条目都有一个由字符串表示的权限集。字符串由 RFC 2086 定义。要计算用户的权限集，服务器将加上所有授予此用户以及此用户所属的所有组的权限，然后减去所有拒绝此用户以及此用户所属的组的权限。

下表列出了 Messaging Server 可以识别的字符，并给出了它们的名称和每个字符的简短说明，还显示了具有此权限的用户可以发出的 IMAP 命令。

表 18-3 ACL 权限字符

字符	说明
l	查找 — 用户可以查看和订阅共享文件夹。（允许的 IMAP 命令：LIST 和 LSUB）
r	读取 — 用户可以读取共享文件夹。（允许的 IMAP 命令：对文件夹进行操作的命令 SELECT、 CHECK、 FETCH、 PARTIAL、 SEARCH、 COPY）
s	已读 — 指示系统保存多个会话的已读信息。（设置 IMAP STORE SEEN 标志）
w	写入 — 用户在读取和删除邮件时可以进行标记。（设置 IMAP STORE 标志，而不是 SEEN 和 DELETED）
i	插入 — 用户可以将电子邮件从一个文件夹复制和移动到另一个文件夹。（允许的 IMAP 命令：APPEND、 COPY 到文件夹中）
p	邮寄 — 用户可以将邮件发送到共享文件夹电子邮件地址。（无需任何 IMAP 命令）
c	创建 — 用户可以创建新的子文件夹。（允许的 IMAP 命令：CREATE）
d	删除 — 用户可以从共享文件夹中删除条目。（允许的 IMAP 命令：EXPUNGE 和设置 STORE DELETED 标志）
a	管理员 — 用户具有管理权限。（允许的 IMAP 命令：SETACL）

组 ACL

ACL 条目的标识符可以指定组的名称。此条目的访问权限适用于该组的所有成员。服务器通过 inetMailUser 对象类的 aclGroupAddr 属性确定组的成员资格。组通过在 aclGroupAddr 属性上有一个过滤器的动态邮递列表来表示。以下示例显示了定义组的 LDIF 记录，包括 aclGroupAddr 属性：

```
dn:cn=lee-staff,ou=Groups, o=sesta.com
cn: lee-staff
mailHost: mail.sesta.com
inetMailGroupStatus: active
mgrpErrorsTo: lee.jones@sesta.com
description: Dynamic Group of Lee's staff
objectClass: top
objectClass: groupofuniquenames
objectClass: inetmailgroup
objectClass: inetmailgroupmanagement
objectClass: inetlocalmailrecipient
objectClass: groupofurls
mail: lee-staff@sesta.com
memberURL: ldap:///o=sesta.com??sub?
(&(aclGroupAddr=lee-staff@sesta.com)(objectclass=inetmailuser))
```

在文件夹的 ACL 中使用组电子邮件地址时，不必创建组。实际上，在向组添加成员时，创建这样的动态组并对用户条目设置 aclGroupAddr 属性是有意义的。一旦创建了这样的组，就可以通过使用属性 mgrpRfc822MailMember 中相应的电子邮件地址添加静态外部成员。不应使用 uniqueMember 属性添加成员，也不应通过创建 memberURL 属性的其他值添加成员。这样做会导致 MTA 视为邮递列表成员的成员与 IMAP 服务器视为组成员的成员之间断开连接。

用户登录到 IMAP 服务器或使用 HTTP 访问服务客户机 （例如 Messenger Express）登录时，服务器将获取 aclGroupAddr 属性 （以及其他与邮件存储相关的属性）并在内存中缓存组的名称。服务器使用此信息确定用户的访问权限，无论客户机何时发出要求访问权限验证的命令 （例如 LIST 或 SELECT）。

共享文件夹任务

本节介绍了共享文件夹的管理员任务：

- 第 503 页的 “创建公用文件夹”
- 第 504 页的 “更改公用文件夹的访问控制权限”
- 第 505 页的 “启用或禁用共享文件夹列表”
- 第 505 页的 “设置分布式共享文件夹”
- 第 507 页的 “监视和维护共享文件夹数据”

创建公用文件夹

由于公用文件夹需要访问 LDAP 数据库和使用 `readership` 命令，因此必须由系统管理员创建公用文件夹。

1. 添加将用作所有公用文件夹的容器的 LDAP 用户条目，例如一个名为 `public` 的条目：

```
dn:cn=public,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: public
mail: public@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: public
inetUserStatus: active
mailUserStatus: active
mailQuota:-1
mailMsgQuota: 100
```

2. 使用 `mboxutil` 命令行实用程序在公用帐户内创建文件夹。例如：

```
mboxutil -c user/public/golftournament
```

3. 使用 readership 命令行实用程序为此文件夹设置相应的 ACL。

   要使此文件夹公用，必须指定一组可以访问它的用户。可以通过使用 readership 命令设置 ACL 来完成此操作。有关如何设置 ACL 的说明，请参见下面的第 504 页的 “更改公用文件夹的访问控制权限”。

更改公用文件夹的访问控制权限

有时，您可能需要更改公用文件夹的访问控制，或者需要为新建的公用文件夹设置访问控制。

要执行该操作，请使用 readership 命令行实用程序。命令的格式如下：

```
readership -s foldername identifier rights_chars
```

其中 *foldername* 是您要为其设置权限的公共文件夹的名称， *userid* 是您要为其指定权限的个人或组，而 *rights_chars* 是您要指定的权限 （这些是符合 RFC 2086 规范的访问权限字符）。有关每个字符的含义，请参见第 500 页的 “ACL 权限字符”。您也可以使用 Messenger Express 界面更改公用文件夹的访问控制。

示例

例如，如果您希望 sesta 域中的每个用户对公用文件夹 golftournament 都具有查找、读取和标记电子邮件 （但不能邮寄）的访问权限，请发出以下命令：

```
readership -s User/public/golftournament anyone@sesta lwr
```

要指定对某个组的查找、读取、标记电子邮件和邮寄电子邮件的权限，请发出以下命令：

```
readership -s User/public/golftournament group=golfinterest lwrp
```

如果要将此文件夹的管理员权限和邮寄权限指定给单个用户 jdoe，请发出以下命令：

```
readership -s User/public/golftournament jdoe lwrpa
```

要拒绝单个用户或组对公用文件夹的访问，请为 userid 加上前缀短划线。例如，要拒绝对 jsmith 的查找、读取和写入权限，请发出以下命令：

```
readership -s User/public/golftournament -jsmith lwr
```

启用或禁用共享文件夹列表

响应 LIST 命令时，根据配置选项 local.store.sharedfolders 中的设置，服务器将返回或不返回共享文件夹。将选项设置为 off 将禁用该选项。默认情况下，该设置处于启用状态 （设置为 on）。

SELECT 和 LSUB 命令不受此选项的影响。 LSUB 命令将返回每个已订阅的文件夹，包括共享文件夹。用户可以选择 （SELECT）其拥有或订阅的共享文件夹。

设置分布式共享文件夹

通常，只有特定邮件存储中的用户才可以使用共享文件夹。但是， Messaging Server 允许您创建可以从多个邮件存储中访问的**分布式共享文件夹**。即，可以将对分布式共享文件夹的访问权限授予邮件存储组内的所有用户。但是，请注意 Web 邮件客户机 （HTTP 访问客户机，如 Messenger Express）不支持远程共享文件夹访问。用户可以列出和订阅文件夹，但不能查看或更改内容。

设置分布式共享文件夹要满足以下要求：

- 邮件存储 userid 在邮件存储的组内必须是唯一的。
- 部署内的目录数据必须相同。

必须通过设置表 18-4 第 505 页 中列出的配置变量，将远程邮件存储 （即不保留共享文件夹的邮件存储）配置为代理服务器。

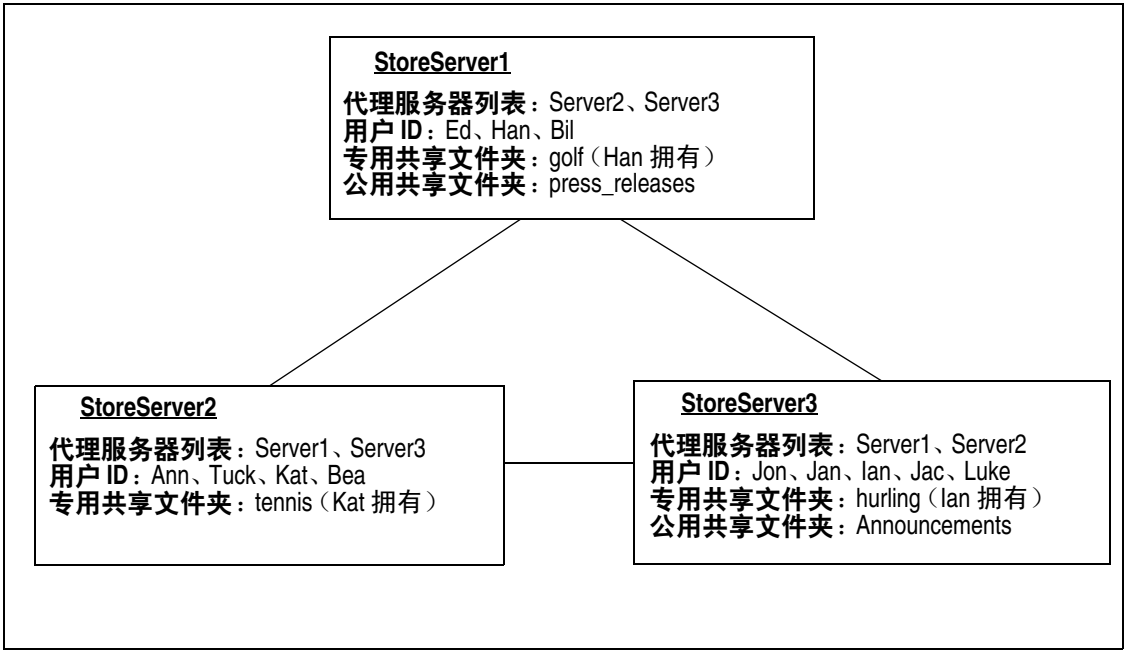
表 18-4 用于配置分布式共享文件夹的变量

名称	值	数据格式
local.service.proxy.serverlist	邮件存储服务器列表	以空格分隔的字符串
local.service.proxy.admin	默认存储管理登录名	字符串
local.service.proxy.adminpass	默认存储管理密码	字符串
local.service.proxy.admin.*hostname*	特定主机的存储管理登录名	字符串
local.service.proxy.adminpass.*hostname*	特定主机的存储管理密码	字符串

设置分布式共享文件夹示例

图 18-3 显示了三个分别名为 StoreServer1、 StoreServer2 和 StoreServer3 的邮件存储服务器的分布式文件夹示例。

图 18-3 分布式共享文件夹示例



通过设置表 18-4 中所示的变量，这些服务器被相互连接成为对等代理邮件存储。每个服务器均有一个专用共享文件夹：*golf*（Han 拥有）、 *tennis*（Kat 拥有）和 *hurling*（Luke 拥有）。此外，还有两个分别名为 *press_releases* 和 *Announcements* 的公用共享文件夹。三个服务器中任何一个服务器上的用户均可以访问这三个共享文件夹中的任何一个。图 18-2 第 499 页 显示了 Ed 的共享文件夹列表。下面是此配置中每个服务器的 ACL 的示例。

```
$ StoreServer1 :> readership -l
Ed: user/Han/golf
Ian: user/Han/golf
anyone: user/public/press_releases
```

```
$ StoreServer2 :> readership -l
Jan: user/Kat/tennis
Ann: user/Kat/tennis
anyone: user/public+Announcements user/public+press_releases
```

```
$ StoreServer3 :> readership -l
Tuck: user/Ian/hurling
Ed: user/Ian/hurling
Jac: user/Ian/hurling
anyone: user/public/Announcements
```

监视和维护共享文件夹数据

readership 命令行实用程序允许您监视和维护保留在 folder.db、 peruser.db 和 lright.db 文件中的共享文件夹数据。 folder.db 包含每个保留 ACL 的副本的文件夹的记录。 peruser.db 包含每个用户和邮箱的条目，列出了各种标志设置和用户上一次访问文件夹的日期。 lright.db 包含所有用户及其具有查找权限的共享文件夹的列表。

readership 命令行实用程序使用以下选项：

表 18-5 readership 选项

选项	说明
-d days	对于每个共享文件夹，返回在指定天数内选择了该文件夹的用户的数量报告。
-p months	从 peruser.db 删除未在指定月份内选择其共享文件夹的用户的数据。
-l	列出 lright.db 中的数据。
-s *folder_identifier_rights*	为指定文件夹设置访问权限。这将更新 lright.db 和 folder.db。

通过使用各种选项，您可以执行以下功能：

- 第 508 页的 “监视共享文件夹的使用情况”
- 第 508 页的 “列出用户及其共享文件夹”
- 第 508 页的 “删除不活动的用户”
- 第 509 页的 “设置访问权限”

监视共享文件夹的使用情况

要查出有多少用户正在访问共享文件夹，请发出以下命令：

```
readership -d days
```

其中 *days* 是要检查的天数。请注意，此选项将返回活动用户的数量，而不是活动用户的列表。

示例：要查出在上一个 30 天内选择了共享文件夹的用户的数量，请发出以下命令：

```
readership -d 30
```

列出用户及其共享文件夹

要列出用户和他们对其具有访问权限的共享文件夹，请发出以下命令：

```
readership -l
```

输出示例：

```
$ readership -l
group=lee-staff@siroe.com: user/user2/lee-staff
richb: user/golf user/user10/Drafts user/user2/lee-staff user/user10/Trash
han1: user/public+hurling@siroe.com user/golf
gregk: user/public+hurling@siroe.com user/heaving user/tennis
```

删除不活动的用户

如果要删除不活动的用户 （在指定的时间段内没有访问共享文件夹的用户），请发出以下命令：

```
readership -p months
```

其中 *months* 是要检查的月数。

示例：删除在过去六个月中没有访问共享文件夹的用户：

```
readership -p 6
```

设置访问权限

您可以将访问权限指定给新的公用文件夹，或者更改当前公用文件夹的访问权限。

有关如何使用此命令设置访问权限的示例，请参见第 504 页的 “更改公用文件夹的访问控制权限”。

关于邮件存储配额

邮件存储配额是一种用于设置用户或域可以使用多少磁盘空间或邮件的限制或**配额**的方式。本节包含有关以下内容的信息：

- 第 509 页的 “用户配额”
- 第 510 页的 “域配额”
- 第 510 页的 “电话学应用程序服务器的异常”

有关详细信息，请参见第 537 页的 “监视配额限制”。

用户配额

可以通过磁盘空间或邮件数量来指定用户配额。磁盘空间配额用于指定每个用户的磁盘空间容量 （以字节为单位）。磁盘配额应用于所有用户邮件的总大小 （不管用户拥有多少邮件文件夹）或者用户邮件的总数量。邮件配额使您可以限制用户邮箱中存储的邮件的数量。

配额信息存储在用户 LDAP 属性 （表 18-6）和 `configutil` 变量 （表 18-7）中。（有关最新和完整的信息，请参见 Sun Java System Communcations Services Schema Reference Manual [`http://docs.sun.com/doc/819-0113`]。）除了设置配额本身， Messaging Server 还允许您控制以下功能：

- **配额通知** — 用户达到**磁盘配额阈值**时，向用户发送警告邮件。
- **强制配额** — 一旦超出配额，将停止向邮件存储中传送邮件；或者即使超出配额，仍允许传送邮件。

  如果由于超过配额而停止传送邮件，则外来邮件将保留在 MTA 队列中，直到出现以下情况之一：

  - 用户邮件的大小或数量不再超出配额，此时 MTA 将传送邮件。
  - 未传送邮件在 MTA 队列中保留的时间超过指定的宽限期，此时邮件将被返回给发件人。（请参见第 517 页的 “设置宽限期”）。

用户删除和擦除邮件后或者服务器根据您建立的生存期策略删除邮件后，便会释放一些磁盘空间。

- **默认配额** — 为所有用户设置默认配额，或为特定用户设置不同配额。要确定用户是否超出配额， Messaging Server 将首先检查以确定是否已为单个用户设置配额。如果未设置配额， Messaging Server 将检查为所有用户设置的默认配额。

域配额

与用户配额类似，域的配额也可以通过字节数或邮件数来进行设置。此配额是指特定域中所有用户的所有累积字节或邮件数。

电话学应用程序服务器的异常

为支持统一的邮件传送要求， Messaging Server 提供了覆盖由邮件存储强加的配额限制的能力。这可以保证已被特定代理 （即电话学应用程序服务器 [TAS]）接受的邮件的传送。 TAS 接受的邮件可以通过特殊的 MTA 通道传送，该通道可以确保邮件被传送到存储而不受配额的限制。有关配置 TAS 通道的详细信息，请参见第 12 章 “配置通道定义”。

表 18-6 显示了配额用户 LDAP 属性。有关最新和完整的信息，请参见 Sun Java System Communcations Services Schema Reference Manual (http://docs.sun.com/doc/819-0113)。

表 18-6 邮件存储配额属性

属性	说明
mailQuota	允许的用户邮箱磁盘空间的字节数。特殊值： 0 — 不允许为用户邮箱分配空间。 -1 — 在空间使用上没有限制。 -2 — 使用系统默认配额。（configutil 参数 store.defaultmailboxquota）
mailMsgQuota	允许用户拥有的最大邮件数。这是存储中所有文件夹的累积计数。特殊值： 0 — 不允许用户邮箱中有邮件。 -1 — 在允许的邮件数上没有限制。 -2 — 使用系统默认配额。（configutil 参数 store.defaultmessage.quota。）

表 18-6 邮件存储配额属性

属性	说明
mailUserStatus	邮件用户的状态。可以是下列值之一： active — 正常处理邮件。默认值是 active。 inactive — 用户的邮件帐户已无效。返回瞬态错误。 deleted — 帐户被标记为删除并准备清除。返回永久性错误。阻塞对邮箱的访问。 hold — 邮件被发送到保留队列，并且不允许访问邮箱 overquota — 在此状态下， MTA 不会将邮件传送到邮箱。这是在 configutil 参数 store.overquotastatus 打开时所设置的状态。
mailDomainDiskQuota	域中所有邮箱可以使用的磁盘空间字节数。值 -1 表示在空间使用上没有限制 （默认值）。要对域磁盘进行强制配额，请运行以下命令： imquotacheck -f -d *domain*
mailDomainMsgQuota	域中所允许的最大邮件数 （即针对存储中所有邮箱的总计数）。值 -1 表示没有限制 （默认值）。要对域邮件进行强制配额，请运行以下命令： imquotacheck -f -d *domain*
mailDomainStatus	邮件域的状态。值和默认值与 mailUserStatus 相同。

表 18-7 邮件存储 configutil 参数

参数	说明
store.quotaenforcement	在关闭状态下启用强制配额，系统将仍更新配额数据库，但始终传送邮件。默认值：On
store.quotanotification	启用配额通知。默认值：On
store.defaultmailboxquota	存储默认配额 （按字节数）。默认值：-1 （无限制）
store.defaultmessagequota	存储默认配额 （按邮件数，数字值）。默认值：-1 （无限制）
store.quotaexceededmsg	配额警告邮件。如果没有，则不发送通知。默认值：无。
store.quotaexceededmsginterval	发送超过配额通知的时间间隔 （以天为单位）。默认值：7
store.quotagraceperiod	在将传送到邮箱的邮件退回给发件人之前，邮箱保持超过配额状态的时间 （以小时为单位，小时数）。默认值：120
store.quotawarn	配额警告阈值。在向客户机发送超过配额警告之前，超出配额的百分比。默认值：90
local.store.quotaoverdraft	用于提供与从 Netscape Messaging Server 迁移的系统的兼容性。当设置为 ON 时，允许传送一个使磁盘使用量超过配额的邮件。用户超过配额后，邮件将被延迟或退回，并发送配额警告邮件，同时配额宽限期计时器将启动。（默认值为当邮件存储达到阈值时发送配额警告邮件。）默认值：Off，但是如果设置了 store.overquotastatus，则将其视为 on，否则用户将始终不会超过配额，从而始终不会使用 overquotastatus。

表 18-7 邮件存储 configutil 参数

参数	说明
local.store.overquotastatus	邮件在 MTA 中被排队之前启用强制配额。这可以防止 MTA 队列填满。如果设置此参数，并且用户尚未超过配额，但外来邮件促使用户超过配额，那么邮件将被传送，但 mailuserstatus LDAP 属性被设置为 overquota，因此 MTA 将不再接受任何邮件。默认值：off

配置邮件存储配额

本节介绍了以下任务：

- 第 512 页的 “指定默认用户配额”
- 第 513 页的 “指定单个用户配额”
- 第 513 页的 “指定域配额”
- 第 513 页的 “部署配额通知”
- 第 516 页的 “启用或禁用强制配额”
- 第 517 页的 “设置宽限期”

指定默认用户配额

要设置应用于未设置各自配额的用户的默认配额，请执行以下步骤：

Console 要通过 Console 指定默认用户配额，请执行以下操作：

1. 单击 “配置”选项卡，并在左窗格中选择 “邮件存储”。
2. 单击 “配额”选项卡。
3. 要为 “默认用户磁盘空间配额”字段指定默认用户磁盘配额，请选择以下选项之一：

   无限制。如果不需要设置默认磁盘配额，请选择此选项。

   指定大小。如果要将默认用户磁盘配额限制为特定大小，请选择此选项。在按钮旁边的字段中键入一个数字，然后从下拉式列表中选择 “KB”或 “MB”。
4. 要指定邮件数配额，请在 “默认的用户邮件存储空间配额”框中键入数字。
5. 单击 “保存”。
6. 在使用默认邮件存储配额的用户条目中将 MB 属性设置为 -1。请参见表 18-6。

命令行 要通过命令行指定默认用户配额，请执行以下操作：

要指定总邮件大小的默认用户配额，请运行以下命令：

`configutil -o store.defaultmailboxquota -v [ -1 | number ]`

其中 `-1` 表示无配额； *number* 表示字节数。

要以邮件总数的形式指定默认的用户配额，请运行以下命令：

`configutil -o store.defaultmessagequota -v [ -1 | number ]`

其中 `-1` 表示无配额； *number* 表示邮件数。

在使用默认邮件存储配额的用户条目中将 `mailQuota` 属性设置为 `-2`。请参见表 18-6。

指定单个用户配额

每个用户均可以有各自的配额。要设置特定于用户的配额，请在用户的 LDAP 条目中设置 `mailQuota` 或 `mailmsgquota` 属性。（请参见表 18-6。）要进行强制配额，请将 `configutil store.quotaenforcement` 设置为 `on`。

指定域配额

您可以为特定域设置磁盘空间配额或邮件配额。这些配额是指特定域中所有用户的累积字节或邮件数。要设置域配额，请在用户的 LDAP 条目中设置 `mailDomainDiskQuota` 或 `mailDomainMsgQuota` 属性 （请参见表 18-6）并运行 `imquotacheck -f`。

部署配额通知

配额通知是指当用户接近他们的配额时，向其发送警告邮件的过程。使用此功能需要执行以下三个步骤：

- 第 514 页的 “启用配额通知”
- 第 514 页的 “定义配额警告邮件”
- 第 515 页的 “指定配额阈值”

启用配额通知

Console 要通过 Console 启用配额通知，请执行以下操作：

1. 单击 “配额”选项卡。
2. 选取 “启用配额通知”框。要禁用配额通知，则取消选取此框。
3. 定义配额警告邮件。请参见第 514 页的 “定义配额警告邮件”。
4. 单击 “保存”。

命令行 要通过命令行启用或禁用配额通知，请运行以下命令：

```
configutil -o store.quotanotification -v [ yes | no ]
```

如果未设置邮件，则不会向用户发送任何配额警告邮件。有关配额警告邮件格式的示例，请参见下一节。

定义配额警告邮件

定义将发送给要超出其磁盘配额的用户的邮件，如下所示。邮件被发送到用户的邮箱。

Console 要通过 Console 定义配额警告邮件，请执行以下操作：

1. 单击 “配额”选项卡。
2. 从下拉式列表中选择要使用的语言。
3. 在下拉式列表下面的邮件文本字段中键入要发送的邮件。
4. 单击 “保存”。

命令行 要通过命令行定义配额警告邮件，请运行以下命令：

```
configutil -o store.quotaexceededmsg -v 'message'
```

邮件必须是 RFC 822 格式。必须包含一个标题 （至少具有一个主题行），接着是 $$，然后是邮件主体。 "$" 表示一个新的行。可能需要在 $ 前面添加一个 \，使 $ 不再具有特殊含义 （取决于所使用的 shell）。（$ 通常是 shell 的换码符。）示例：

```
configutil -o store.quotaexceededmsg -v 'Subject: WARNING:User quota
exceeded$$User quota threshold exceeded - reduce space used.í
```

此外，支持以下变量：

[ID] — 用户 ID

[DISKUSAGE] — 磁盘使用量

[NUMMSG] — 邮件数

[PERCENT] — store.quotawarn 百分比

[QUOTA] — mailquota 属性

[MSGQUOTA] — mailmsgquota 属性

以下为使用这些变量的一个示例：

```
configutil -o store.quotaexceededmsg -v 'Subject: Overquota
Warning$$[ID],$$Your mailbox size has exceeded [PERCENT] of its alloted
quota.$Disk Usage: [DISKUSAGE]$Number of Messages: [NUMMSG]$Mailquota:
[QUOTA]$Message Quota: [MSGQUOTA]$$-Postmaster'
```

要定义发送警告邮件的频率，请运行以下命令：

```
configutil -o store.quotaexceededmsginterval -v number
```

其中 *number* 表示天数。例如， 3 表示每 3 天发送一次邮件。

指定配额阈值

配额阈值是在向客户机发送警告之前超出配额的百分比。用户的磁盘使用率超出指定的阈值时，服务器将向用户发送警告邮件。

注 当 local.store.quotaoverdraft=on 时，电子邮件通知不会被触发，直至用户的磁盘使用量超过配额的 100%，与使用 store.quotawarn 设置的阈值无关。

对于其客户机支持 IMAP ALERT 机制的 IMAP 用户，邮件将在每次用户选择邮箱时显示在用户的屏幕上，并且邮件还将被写入 IMAP 日志。

Console 要通过 Console 指定配额阈值，请执行以下操作：

1. 单击 “配额”选项卡。
2. 在 “配额警告阈值”字段中输入警告阈值的数值。

   此数值表示允许的配额的百分比。例如，如果指定 90%，则将在使用了 90% 的允许的磁盘配额后警告用户。默认值为 90%。要关闭此功能，请输入 100%。
3. 单击 “保存”。

命令行 要通过命令行指定配额阈值，请运行以下命令：

```
configutil -o store.quotawarn -v number
```

其中 *number* 表示允许的配额的百分比。

启用或禁用强制配额

默认情况下，用户或域可以超出其配额，除了收到超过配额通知 （如果已设置）外没有任何影响。强制配额将锁定邮箱，使其不能再接收邮件，直到磁盘使用量降至低于配额级别。

启用用户级别的强制配额

Console 要通过 Console 启用强制配额，请执行以下操作：

1. 单击 “配额”选项卡。
2. 选取 “启用强制配额”框。要禁用强制配额，则取消选取此框。
3. 单击 “保存”。

命令行 要启用或禁用强制配额，请运行以下命令：

```
configutil -o store.quotaenforcement -v [ on | off]
```

请注意，超过配额邮件保存到 MTA 队列中，并将向发件人发送通知，该通知说明未传送他们的邮件，但会在稍后尝试重新传送。传送重试将继续，直到宽限期过期并且所有邮件均被退回给发件人，或者磁盘使用量降至配额以下并且邮件可以从 MTA 中取消排队并传送到邮件存储。如果要在邮件进入邮件队列之前将超过配额的邮件返回，请使用以下命令行：

```
configutil -o store.overquotastatus -v on
```

启用域级别的强制配额

要对特定域的配额进行强制，请使用以下命令：

```
imquotacheck -f -d domain
```

如果不使用 `-d` 选项，就可以为所有域启用强制配额。当域超出其配额时，`maildomainstatus` 属性将设置为 `overquota`，它将停止所有到该域的传送。如果域不是 `overquota`，则值被设置为 `active`。

禁用强制配额

如果出现用户配额正被强制执行的情况，那么即使您已禁用了它们，请检查以下参数：

应该关闭或不设置这些 `configutil` 参数：

- `store.quotaenforcement`
- `local.store.overquotastatus`

- local.store.quotaoverdraft

请注意，当 store.overquotastatus 为 on 时，它始终将 store.quotaoverdraft 视为 on，否则用户将永远不会超过配额以触发拒绝。此外，当 store.quotaoverdraft 为 on 时，仅允许用户接受一个比配额小的邮件。即它将永远不会接受比用户配额大的邮件。

对这些参数做出更改后，请确保重新启动邮件传送服务。

这些邮件存储属性应处于活动状态：

- maildomainstatus
- mailuserstatus

请注意，如果邮件大于邮箱配额则它们将被退回，与强制配额配置无关。

设置宽限期

宽限期将指定邮件被退回发件人之前邮箱可以超出配额 （磁盘空间或邮件数量）的时间。邮件被 MTA 接受，但保留在 MTA 队列中而不被传送到邮件存储，直到发生以下情况之一：

- 邮箱不再超出配额，此时邮件将被传送到邮箱。
- 用户保留超出配额的时间比指定的宽限期长，此时服务器将退回所有邮件，包括队列中的邮件。该时间限制由 quotagraceperiod configutil 参数控制。
- 邮件保留在邮件队列中的时间比最大邮件队列时间长。该设置由 notices MTA 通道关键字控制 （请参见第 246 页的 “设置通知邮件传送间隔”）。

例如，如果您的宽限期设置为两天，而您超出了配额一天，则将继续接收新邮件并将其保留在邮件队列中，并继续进行传送尝试。第二天后，邮件将被退回给发件人。

注 宽限期不是邮件在邮件队列中保留的时间，而是退回所有外来邮件（包括邮件队列中的邮件）之前邮箱可以超出配额的时间。如果用户已达到配额阈值 （请参见第 515 页的 “指定配额阈值”）并被警告，宽限期将启动。

Console 要通过 Console 设置邮件在队列中保存时间的宽限期，请执行以下操作：

1. 单击 “配额” 选项卡。
2. 在 “超过空间配额宽限期” 字段中输入一个数字。
3. 从下拉式列表中，指定 Day(s) 或 Hour(s)。

4. 单击 “保存”。

命令行 要通过命令行指定配额宽限期，请运行以下命令：

```
configutil -o store.quotagraceperiod -v number
```

其中 *number* 表示小时数。

Netscape Messaging Server 配额兼容性模式

在磁盘使用量超过 Netscape Messaging Server 中的配额后，服务器会延迟或退回邮件传送、发送超过配额通知并启动宽限期。 Messaging Server 提供了一个参数 `local.store.quotaoverdraft`，可以保留此行为。

设置为 `ON` 时，将传送邮件直到磁盘使用量超过配额。那时，邮件将被延迟 （邮件保留在 MTA 邮件队列中，不会被传送到邮件存储），同时会向用户发送超过配额警告邮件，并且宽限期将启动。宽限期确定了邮箱超过配额多长时间后才会退回超过配额邮件。（默认值为当邮件存储达到阈值时发送配额警告邮件。）此参数的默认值为 `Off`。

设置自动删除邮件 （过期和清除）功能

自动删除邮件功能 （也称为过期和清除）根据管理员定义的一组条件自动从邮件存储中删除邮件。此功能可用于自动删除旧的和过大的邮件、已读 / 已删除邮件、带特定主题行的邮件等等。此功能允许使用以下删除条件：

- 按文件夹 （邮箱）、用户、域、整个邮件存储或特定分区
- 邮箱中邮件的数量
- 邮箱的总大小
- 邮件在邮箱中已经存在的时间 （以天为单位）
- 邮件的大小和宽限期 （在清除前超大邮件将在邮件存储中保留的天数）
- 邮件是否已标记为**已读**或**已删除**
- 标题字符串

此功能由 `imexpire` 实用程序执行，它将擦除和清除邮件。有关邮件删除过程的详细信息，请参见第 496 页的 “邮件存储如何删除邮件”。

注 服务器将不发出警告便删除邮件，因此通知用户有关自动删除邮件的策略很重要。意外的邮件删除会给用户和管理员带来恐慌。

imexpire 操作原理

可以从命令行调用 imexpire 或通过 imsched 守护程序安排其自动运行的时间。管理员使用 Console 或 configutil 命令行实用程序配置全局过期规则（即用于整个邮件存储的规则）。可以通过在邮件存储分区、用户或邮箱目录中创建过期规则文件 (store.expire) 来配置本地过期规则（应用于文件夹或用户的规则）。

imexpire 在启动时装入所有过期规则。默认情况下，imexpire 为每个分区创建一个线程。每个线程都将在其指定的分区下查看用户文件夹列表，同时装入本地过期规则文件。过期功能将按照适用于该文件夹的过期规则检查每个文件夹，并根据需要擦除邮件。如果在邮箱目录下存在 store.exp 文件，并且邮件由于超出了 store.cleanupage 配置参数指定的时间而被擦除 / 过期，清除功能将在邮件散列目录下永久删除邮件文件，并从 store.exp 文件中永久删除 UID 记录。

也可以通过在 *msg_svr_base*/config/ 中名为 expire_exclude_list 的文件中添加指定的用户的 ID（每行一个），以从过期规则中排除这些用户。

部署自动删除邮件功能

可以通过命令行或使用 Console GUI 部署自动删除邮件。此过程需要三个步骤：

1. 定义自动删除邮件策略：哪些邮件将被自动删除？哪些用户、域和分区将使邮件自动被删除？哪些大小、邮件生存期、标题将定义删除条件。请参见第 519 页的 “定义自动删除邮件策略”。
2. 指定 imexpire 规则以实现此策略。请参见第 520 页的 “设置实现自动删除邮件策略的规则”。
3. 指定 imexpire 时间安排。请参见第 527 页的 “安排自动删除邮件和日志记录级别”。

定义自动删除邮件策略

通过指定删除条件定义自动删除邮件策略。imexpire 允许使用以下条件进行删除：

邮件的生存期。自动删除存在的时间超过 *X* 天的邮件。属性：messagedays。

邮件计数。自动删除文件夹中超出 X 封邮件的邮件。属性：messagecount。

超大邮件的生存期。自动删除在 Y 天宽限期后超过 X 字节的邮件。属性：messagesize 和 messagesizedays。

已读和已删除邮件标志。自动删除带有**已读**或**已删除**标志设置的邮件。可以将这些条件设置为 "and" 或 "or"。如果设置为 or，则邮件的已读 / 删除标志将导致自动删除而不管其他条件。如果设置为 and，则邮件的已读 / 删除标志必须设置为与所有其他指定的条件一起使用。属性：seen 和 deleted。

邮件的标题字段。允许您将标题和字符串指定为删除邮件的条件。例如，删除所有标题为 "Subject: Work from Home!" 的邮件

邮件的文件夹。允许您指定要从其中删除邮件的文件夹。属性：folderpattern

注 imexpire 不允许根据邮件被读取后已存在的时间删除或保留邮件。例如，不能指定删除已经有 200 天未被读取的邮件。

自动删除邮件策略的示例

示例 1：删除超过 1,000 封邮件的文件夹中所有存在时间达到 365 天的邮件。

示例 2：删除域 siroe.com 中 180 天以上的邮件。

示例 3：删除所有已标记为**已删除**的邮件。

示例 4：删除 sesta.com 中已标记为**已读**、 30 天以上、大于 100 千字节、位于超过 1,000 封邮件的文件夹中、带有标题 X-spam 的邮件。

设置实现自动删除邮件策略的规则

要实现上一节中定义的自动删除邮件策略，必须设置 imexpire 规则。通过如下方法设置规则：

- 通过 GUI （请参见图 18-4 第 525 页）
- 通过将规则放到 store.expirerule 文件中。以下所示为两个 store.expirerule 规则的示例：

```
Rule1.folderpatter:user/.*/trash
Rule1.messagedays:2
Rule2.folderpattern:user/.*
Rule2.messagedays: 14
```

在此示例中，规则 1 指定垃圾文件夹中的所有邮件将在两天后被删除。规则 2 指定邮件存储中的所有邮件将在 14 天后被删除。

本节包含以下几个部分：

- 第 521 页的 “过期规则原则”
- 第 523 页的 “通过文本方式设置 imexpire 规则”
- 第 524 页的 “设置 imexpire 文件夹模式”
- 第 524 页的 “使用 Console 设置自动删除邮件规则”

过期规则原则

本节介绍设置 `store.expirerule` 文件规则的原则。

注 在早期的 Messaging Server 发行版中，可以使用 `configutil` 参数 `store.expirerule.`*attribute* 来设置过期规则 （请参见 Sun Java System Messaging Server Administration Reference）。现在仍然可以使用，但不支持使用标题约束的过期规则 （例如：使用特定主题行作为邮件过期规则）。因此，最好使用 Console GUI 或 `store.expirerule` 文件规则。

- 规则在名为 `store.expirerule` 的文件中指定。
- 可以使用相同的规则指定多个过期条件。（如上例所示。）
- 规则可以应用到整个邮件存储 （全局规则）、分区、用户或文件夹。只能使用 `store.expirerule` 规则创建非全局规则。
  - 通过使用 `configutil` 参数 `store.expirerule.`*rulename.attribute* 创建全局规则，或者通过在 *msg_svr_base*`/config/store.expirerule` 中指定规则创建全局规则。
  - 可以通过在 *store_root*`/partition/`*partition_name*`/store.expirerule` 中指定规则创建分区规则。
  - 可以通过在 *store_root*`/partition/`*partition_name*`/`*userid*`/store.expirerule` 中指定规则创建用户规则，或者通过将 `folderpattern` 规则指定为 `user/`*userid*`/.*` 来创建用户规则。

- 可以通过在 *store_root*/partition/*partition_name*/*userid*/*folder*/store.expirerule 中指定规则创建文件夹规则，或者通过将 folderpattern 规则指定为 user/*userid*/*folder* 来创建文件夹规则。

注 还可以通过指定 folderpattern 属性将用户规则和文件夹规则放在全局过期文件 (*msg_svr_base*/config/store.expirerule) 中。

- 多个过期规则可以同时应用于一个邮箱。邮箱的过期策略由全局规则和本地规则组成。本地规则适用于同一目录下的邮箱及其所有子文件夹。
- imexpire 将统一应用于一个邮箱的所有过期规则，除非存在为此邮箱指定的专用规则 （请参见表 18-8）。产生的规则集表示基于所有适用规则的最严格的过期策略。例如，如果规则 X 的过期策略指定最大邮件保存时间为 10 天，规则 Y 指定为 5 天，则统一规则为 5 天。

表 18-8 imexpire 属性

属性	说明 （属性值）
exclusive	指定规则是否为专用规则。如果指定为 exclusive，则只有此规则应用于指定的邮箱，而所有其他规则都将被忽略。如果存在多个专用规则，则将使用最后装入的专用规则。例如，如果指定了全局专用规则和本地专用规则，则将使用本地规则。如果有多个全局专用规则，则使用 configutil 列出的最后一个全局规则。 (yes/no)
folderpattern	指定此规则影响的文件夹。格式必须以 user/ 开头，表示目录 *store_root*/partition/*/。请参见图 18-4 第 525 页 和表 18-9 第 524 页。（POSIX 正则表达式）
messagecount	文件夹中邮件的最大数量。传送附加的邮件时，最早的邮件将被擦除。（整数）
foldersize	传送附加的邮件时，擦除最早的邮件之前文件夹的最大大小。（以字节为单位的整数）
messagedays	邮件被擦除前的生存期 （以天为单位）。（整数）
messagesize	在标记为将被擦除前，邮件的最大大小 （以字节为单位）。（整数）
messagesizedays	宽限期。超大邮件可以保留在文件夹中的天数。（整数）
邮件标题字段	指定标题字段和标记要删除的邮件的字符串。值不区分大小写，正则表达式不会被识别。例如：Rule1.Subject: Get Rich Now! 对于标题**过期**和**过期日期**，如果在这些标题字段中指定的日期值早于 messagedays 属性，则 imexpire 将删除邮件。如果指定了多个过期标题字段，则将使用最早的过期日期。（字符串）。
regexp	在创建规则时启用 UNIX 正则表达式。（1 或 0）。如果未指定，则将使用 IMAP 表达式。
seen	seen 是用户打开邮件时，系统设置的邮件状态标志。如果属性 seen 设置为 and，则邮件必须已被阅读并在规则实施前必须满足其他条件。如果属性 seen 设置为 or，则邮件仅需已被阅读或在规则实施前满足另一个条件。 (and/or)。

表 18-8 imexpire 属性

属性	说明 （属性值）
deleted	deleted 是用户删除邮件时，系统设置的邮件状态标志。如果属性 deleted 设置为 and，则邮件必须被删除并在规则实施前必须满足另一个条件。如果属性 deleted 设置为 or，则邮件仅需已被阅读或在规则实施前满足另一个条件。 **(and/or)**。

通过文本方式设置 *imexpire* 规则

通过在 store.expirerule 文件中指定规则来设置自动删除邮件规则。store.expirerule 文件中每行包含一个过期条件。全局规则配置文件 (*msg_svr_base*/data/store/store.expirerule) 的过期条件的格式如下：

rule_name.*attribute*:*value*

代码示例 18-1 显示了 *msg_svr_base*/config/store.expirerule 中的一组过期规则。

规则 1 设置全局过期策略 （即应用于所有邮件的策略），如下所示：

- 在创建规则时启用 UNIX 正则表达式。
- 3 天后删除大于 100,000 字节的邮件。
- 删除用户已删除的邮件。
- 删除所有 Subject: 标题中有字符串 "Viagra Now!" 或 "XXX Porn!" 的邮件。
- 将所有文件夹限制为容纳 1,000 封邮件。达到 1,000 封邮件后，系统将从文件夹中删除最早的邮件以保持总数为 1,000。
- 删除所有 365 天以前的邮件。

规则 2 为托管域 siroe.com 中的用户设置自动删除邮件策略。它将邮箱大小限制为 1 兆字节，删除已删除的邮件，并删除 14 天前的邮件。

规则 3 为用户 f.dostoevski 的 inbox 文件夹中的邮件设置自动删除邮件策略。它将删除主题行带有表达式 "On-line Casino" 的邮件。

代码示例 18-1 imexpire 规则示例

```
Rule1.regexp:1
Rule1.folderpattern: user/.*
Rule1.messagesize:100000
Rule1.messagesizedays:3
Rule1.deleted: or
Rule1.Subject: Vigara Now!
Rule1.Subject: XXX Porn!
Rule1.messagecount: 1000
Rule1.messagedays:365
Rule2.regexp:1
Rule2.folderpattern: user/.*@siroe.com/.*
Rule2.exclusive: yes
Rule2.deleted: or
Rule2.messagedays:14
Rule2.messagecount:1000
Rule3.folderpattern: user/f.dostoevski/inbox
Rule3.Subject: *On-line Casino*
```

设置 *imexpire* 文件夹模式

通过将 imexpire 属性 regex 设置为 1，可以使用 POSIX 正则表达式指定文件夹模式。如果未指定，则将使用 IMAP 表达式。格式必须以 user/ 开头，后跟一种模式。表 18-9 显示了各种文件夹的文件夹模式。

表 18-9 使用正则表达式的 imexpire 文件夹模式

文件夹模式	范围
user/*userid*/.*	将规则应用于 *userid* 的所有文件夹中的所有邮件。
user/*userid*/Sent	将规则应用于 *userid* 在文件夹 Sent 中的邮件：
user/.*	将规则应用到整个邮件存储。
user/.*/trash	将规则应用于所有用户的 trash 文件夹。
user/.*@siroe.com/.*	将规则应用到托管域 siroe.com 中的文件夹：
user/[^@]*/.*	将规则应用到默认域中的文件夹。

使用 *Console* 设置自动删除邮件规则

1. 如下所示调出自动删除邮件 GUI：

   “主 Console” > “服务器组” > “Messaging Server”（打开） > “Messaging Server Console” > “配置”选项卡 > “邮件存储” > “过期 / 清理” > “添加”

图 18-4 中显示了 GUI 的草图。

图 18-4 自动删除邮件 （过期 / 清除） GUI 草图

2. 输入新规则的名称。

3. 输入将从其中自动删除邮件的文件夹。

   请参见上述第 524 页的 “设置 imexpire 文件夹模式”。

4. 如果此规则是与指定条件相匹配的文件夹的专用规则，则请选取 “*Exclusive*” 框。

   如果已选取此框，则此规则将优先于与指定模式相匹配的所有其他规则。有关专用复选框的详细信息，请参见表 18-8 第 522 页。

5. 要创建基于文件夹大小的规则，请执行以下操作：

   - 选取 “文件夹大小约束” 复选框。在 “邮件计数” 字段中，指定在最早的邮件被删除之前文件夹中将保留的邮件的最大数目。在 “文件夹大小” 字段中，指定最早的邮件被删除之前最大的文件夹大小 （以字节为单位）。

6. 要创建基于邮件生存期的规则，请选取 “邮件生存期约束” 复选框：

   在 “天数” 字段中，指定邮件可以在文件夹中保存的时间 （以天为单位）。

7. 要创建基于邮件大小的规则，请执行以下操作：

   - 选取 “邮件大小限制约束” 复选框。在 “邮件大小限制” 字段中，输入文件夹中允许的邮件的最大大小。在 “宽限期” 字段中，输入超大邮件被删除前在文件夹中保存的时间。

8. 要创建基于是否已设置 “已读” 或 “已删除” 标志的规则，请执行以下操作：

   - 选取 “邮件标志约束” 复选框。
   - 对于 “已读：” 字段，选择 “和” 将指定邮件必须已被阅读**并**在规则实施前必须满足另一个条件。选择 “或” 将指定邮件仅需已被阅读**或**在规则实施前满足另一个条件。
   - 对于 “已删除：” 字段，选择 “和” 将指定邮件必须被删除**并**在规则实施前必须满足另一个条件。选择 “或” 将指定邮件仅需被删除**或**在规则实施前满足另一个条件。

9. 要创建基于标题字段及其值的规则，请执行以下操作：

   - 选取 “标题约束” 复选框。
   - 用以下格式输入以逗号分隔的标题和值的列表：

     header1:*value1*, *header2*:*value2*

     示例：`Subject:Work at Home!,From:virus@sesta.com`

   对于标题**过期**和**过期日期**，如果其日期值早于 “邮件生存期约束”，则系统将删除该邮件。如果指定了多个过期标题字段，将采用最早的过期日期。（字符串）。

10. 单击 “确定” 以将新规则添加到 “自动删除邮件” 列表中。

安排自动删除邮件和日志记录级别

将通过 imsched 时间安排守护程序激活自动删除邮件。默认情况下， imsched 将在每天 23:00 点调用 imexpire，邮件将被擦除并被清除。可以通过设置表 18-10 中介绍的 configutil 参数 local.schedule.expire、 local.schedule.purge 和 store.cleanupage 自定义此时间安排。

对于大型邮件存储，可能会花费很长时间才能完成过期和清除，因此您可能需要通过试验决定运行这些进程的频率。例如，如果过期 / 清除周期花费 10 小时，您可能不希望默认时间安排为每天运行过期和清除一次。使用 local.schedule.purge 安排过期和清除，可以为清除指定单独的时间安排。如果未设置 local.schedule.purge，则 imexpire 将在过期后执行清除。

表 18-10 过期和清除 configutil 日志和调度参数

参数	说明

local.schedule.expire	运行 imexpire 的时间间隔。使用 UNIX crontab 格式：
	minute hour day-of-month month-of-year day-of-week
	这些值以空格或 Tab 分隔符分隔，可以分别为 0-59、 0-23、 1-31、 1-12 或 0-6（其中 0 = 星期天）。每个时间字段都可以为以下内容之一：一个星号 （表示所有合法值）、一个以逗号分隔的值的列表或一个以连字符分隔的两个值表示的范围。请注意，可以同时用几号和星期几指定时间，但是通常不同时使用这两者，因为这种情况很少发生。如果同时指定了这两者，则需要同时满足两者。例如，设置月份的第 17 日和星期二将要求同时满足两个值。
	时间间隔示例：
	1) 在 12:30am、 8:30am 和 4:30pm 运行 imexpire：
	`30 0,8,16 * * *  /opt/SUNWmsgsr/lib/imexpire`
	2) 在工作日早晨 3:15am 运行 imexpire：
	`15 3 * * 1-5  /opt/SUNWmsgsr/lib/imexpire`
	3) 仅在星期一运行 imexpire：
	`0 0 * * 1  /opt/SUNWmsgsr/lib/imexpire`
	默认值：`0 23 * * *  /opt/SUNWmsgsr/lib/imexpire`

local.schedule.purge	运行 purge 的时间间隔。使用 UNIX crontab 格式： *minute hour day-of-month month-of-year day-of-week*。 默认值：0 0,4,8,12,16,20 * * * /opt/SUNWmsgsr/lib/purge -num=5（每四小时。）
store.cleanupage	purge 将永久删除邮件前已过期或已擦除的邮件的生存期 （以小时为单位）。 默认值：无

表 18-10 过期和清除 configutil 日志和调度参数

参数	说明
local.store.expire.loglevel	指定日志级别： 1 = 记录整个过期会话的摘要。 2 = 为每个过期的邮箱记录一条消息。 3 = 为每个过期的邮件记录一条消息。 默认值：1

使用 *Console* 进行 *imexpire* 时间安排

如下所示调出自动删除邮件 GUI：

“主 Console” > “服务器组” > “Messaging Server”（打开） > “Messaging Server Console” > “配置”选项卡 > “邮件存储” > “过期 / 清理”

此 Console 页面在顶部列出过期规则，在底部列出过期和清除时间安排。要安排过期和清除的日程，请使用 “过期 / 清理时间安排”中的下拉式菜单为过期和清除设置月份、月份日期、星期日期 （其中 0 = 星期天）、小时和分钟。

注 可以按几号和星期几设置日期值。如果同时设置了两者，则需同时满足两者的条件。如果设置星期的第 3 天 （星期三）和月份的第 17 天，则将仅在每月的第 17 天恰好为星期三时进行清除 / 过期。

设置 *imexpire* 日志记录级别

imexpire 将在完成时记录默认日志文件的摘要。如果从命令行调用过期命令，则 -v （详细）和 杁 （调 EO）緞 OAOUO 窭 æ imexpire 记录 stderr 的详细状态 / 调试消息。如果通过 imsched 调用 imexpire，则 configutil 参数 local.store.expire.loglevel 可以设置为 1、 2 或 3 以进行不同级别的日志记录。Loglevel 1 是默认值，将记录整个过期会话的摘要。Loglevel 2 将对每个过期邮箱记录一条消息。 Loglevel 3 将对每个过期邮件记录一条消息。

从自动删除邮件中排除指定的用户

通过在 *msg_svr_base*/config/ 中名为 expire_exclude_list 的文件中添加指定用户的用户 ID （每行一个），以从过期规则中排除这些用户。

配置邮件存储分区

邮箱存储在邮件存储分区中，即专门用于存储邮件存储的磁盘分区的区域。虽然为了易于维护，我们建议每个邮件存储分区使用一个磁盘分区和一个文件系统，但是邮件存储分区与磁盘分区并不相同。邮件存储分区是专门指定为邮件存储的目录。

默认情况下，用户邮箱存储在 *store_root*/partition/ 目录中 （请参见图 18-1 第 494 页）。partition 目录是可能包含一个或多个分区的逻辑目录。在启动时，partition 目录包含一个名为 primary 分区的子分区。

您可以根据需要向 partition 目录添加分区。例如，您可能希望对单个磁盘进行分区以组织您的用户，如下所示：

store_root/partition/mkting/
store_root/partition/eng/
store_root/partition/sales/

随着磁盘存储需求的增加，您可能需要将这些分区映射到不同的物理磁盘驱动器。

您应该限制任意一个磁盘上的邮箱数量。在多个磁盘之间分发邮箱将会改善邮件传送时间 （尽管不必更改 SMTP 接收速率）。在每个磁盘分配的邮箱数量取决于磁盘容量和分配给每个用户的磁盘空间容量。例如，如果为每个用户分配较少的磁盘空间，则可以为每个磁盘分配更多的邮箱。

如果邮件存储需要多个磁盘，则可以使用 RAID （廉价磁盘冗余阵列）技术方便地对多个磁盘进行管理。使用 RAID 技术，您可以在一系列磁盘之间传播数据，而磁盘表现为一个逻辑卷从而简化了磁盘管理。您可能还希望将 RAID 技术用于冗余，即复制用于故障恢复的存储。

注	要改善磁盘访问，邮件存储和邮件队列应位于单独的磁盘上。

添加分区

添加分区时，您将指定分区在磁盘中存储的绝对物理路径和逻辑名称 （称为分区昵称）。

分区昵称允许您将用户映射到逻辑分区名称，而不管物理路径。设置用户帐户和指定用户的邮件存储时，可以使用分区昵称。输入的名称必须是字母数字名称并且必须使用小写字母。

要创建和管理分区，用于运行服务器的用户 ID 必须具有对物理路径中指定的位置的写入权限。

注 添加分区后，必须停止然后重新启动服务器以刷新配置信息。

Console 要通过使用 Console 向存储添加分区，请执行以下操作：

1. 从 Console 中打开要配置的 Messaging Server。
2. 单击 “配置”选项卡，并在左窗格中选择 “邮件存储”。
3. 在右窗格中单击 “分区”选项卡。
4. 单击 “添加”按钮。
5. 输入分区昵称。

   这是指定分区的逻辑名称。
6. 输入分区路径。

   这是指定分区的绝对路径名称。
7. 要将此分区指定为**默认邮件存储分区**，请单击标有 “使之成为默认分区”的选择框。

注 默认分区是在已创建用户并且未在用户条目中指定 `mailMessageStore` LDAP 属性时所使用的分区。应在所有用户条目中指定 `mailMessageStore` LDAP 属性，从而不需要默认分区。

8. 单击 “确定”以提交此分区配置条目并关闭窗口。
9. 单击 “保存”以提交并保存当前 “分区”列表。

命令行 要通过命令行向存储添加分区，请运行以下命令：

```
configutil -o store.partition.nickname.path -v path
```

其中 *nickname* 是分区的逻辑名称，而 *path* 表示分区存储位置的绝对路径名称。

要指定默认主分区的路径，请运行以下命令：

```
configutil -o store.partition.primary.path -v path
```

将邮箱移动到其它磁盘分区

默认情况下，将在 primary 分区中创建邮箱。如果分区已满，则不能存储附加的邮件。有几种方法可以解决此问题：

- 减少用户邮箱的大小
- 如果使用的是卷管理软件，请添加附加磁盘。
- 创建附加分区 （第 529 页的 “添加分区”）并将邮箱移到新分区

如果有可能，我们建议使用卷管理软件向系统添加附加磁盘空间，因为此过程对于用户是最透明的。不过，您也可以通过执行以下操作将邮箱移到其他分区：

1. 确保在迁移进程期间用户与其各自的邮箱断开了连接。可以通过通知用户在邮箱移动期间注销或脱机来完成此操作，或者通过设置 mailAllowedServiceAccess 属性以便在注销后不允许使用 POP、 IMAP 和 HTTP 服务。（请参见 Sun Java System Communcations Services Schema Reference Manual。）

注 将 mailAllowedServiceAccess 设置为不允许 POP、 IMAP、 HTTP 访问不会断开与邮箱的任何开放连接。移动邮箱前必须确保关闭所有连接。

2. 使用以下命令移动用户邮箱：

   mboxutil -r user/<*userid*>/INBOX user/<*userid*>/INBOX <*partition_name*>

   示例：

   mboxutil -r user/ofanning/INBOX user/ofanning/INBOX secondary

3. 将已移动用户的 LDAP 条目中的 mailMessageStore 属性设置为新分区的名称。

   示例：mailMessageStore:secondary

4. 通知用户现在允许邮件存储连接。如果可用，则更改 mailAllowedServiceAccess 属性以允许 POP、 IMAP 和 HTTP 服务。

更改默认邮件存储分区定义

默认分区是在已创建用户并且未在用户条目中指定 mailMessageStore LDAP 属性时所使用的分区。应在所有用户条目中指定 mailMessageStore LDAP 属性 （该属性指定用户的邮件存储分区），从而不需要默认分区。此外，不应由于负载平衡或任何其他原因而更改默认分区。在仍存在依赖于默认分区定义的用户时更改默认分区是无效且危险的。

如果确实需要更改默认分区，请确保在使用 configutil 参数 store.defaultpartition 更改默认分区的定义之前，旧默认分区 （左后方的）上的所有用户已将他们的 mailMessageStore 属性设置为他们当前的分区 （不再是默认分区）。

执行邮件存储维护过程

本节提供有关用于执行邮件存储的维护和恢复任务的实用程序的信息。您应该始终阅读服务器可能发送的用于警告和警报的邮寄主管邮件。您还应监视日志文件以获取有关服务器如何执行操作的信息。有关日志文件的详细信息，请参见第 21 章 “管理日志记录”。

本节包含以下内容：

- 第 532 页的 “管理邮箱”
- 第 537 页的 “监视配额限制”
- 第 538 页的 “监视磁盘空间”
- 第 538 页的 “使用 stored 实用程序”

管理邮箱

本节介绍了以下用于管理和监视邮箱的实用程序：mboxutil、hashdir、readership。

mboxutil 实用程序

使用 mboxutil 命令执行对邮箱的典型维护任务。mboxutil 任务包括以下内容：

- 列出邮箱
- 列出并删除孤立的和非活动的邮箱
- 创建邮箱
- 重命名邮箱
- 将邮箱从一个分区移动到另一个分区
- 删除孤立的或非活动的邮箱

- 您还可以使用 mboxutil 命令查看有关配额的信息。有关更多信息，请参见第 537 页的 “监视配额限制”。

注 请注意，不应在执行中中止 mboxutil 进程。如果使用 SIGKILL (kill -9) 中止了该进程，则可能潜在地需要每个服务器重新启动并完成恢复。

表 18-11 列出了 mboxutil 命令。有关详细的语法和使用要求，请参见 Messaging Server Reference Manual。

表 18-11 mboxutil 选项

选项	说明
-a	已作废。用于列出所有用户配额信息。使用 imquotacheck
-c *mailbox*	创建指定邮箱。可以与 -f 一起使用。 在创建第二个邮箱前必须已存在一个邮箱。
-d *mailbox*	删除指定邮箱。 要从邮件存储中删除用户，请使用 -d *mailbox* 的以下值： user/*userid*/INBOX 例如，要从邮件存储中删除用户 john，则使用 -d user/john/INBOX。要删除用户 john 的邮箱中的 mm 文件夹，请使用 -d user/john/mm。 建议的删除用户的方法是在 LDAP 目录中将用户状态标记为已删除 （通过使用 Delegated Administrator 实用程序 commadmin user delete 命令或 Delegated Administrator Console）。下一步，使用 commadmin user purge 命令将被标记为已删除超过指定天数的用户清除。 如果使用的是上一段中介绍的 Delegated Administrator 实用程序，则无需使用 mboxutil -d 命令来删除邮箱。
-e	用于清除邮件存储中所有已删除的邮件。此选项还可与 -p *pattern* 选项一起使用，以清除名称与 *pattern* 匹配的所有已删除的邮箱。
-f *file*	用于指定存储邮箱名称的文件。 -f 选项可以与 -c、 -d 或 -r 选项一起使用。 文件包含一个在其上执行了 mboxutil 命令的邮箱的列表。以下是数据文件中条目的示例： user/daphne/INBOX user/daphne/projx user/daphne/mm
-k *mailbox cmd*	已作废。在文件夹级别中锁定指定邮箱；运行指定命令；命令完成后，取消锁定邮箱。
-l	在服务器上列出所有邮箱。 如果要为不同的语言环境创建多字节文件夹，您应编辑：*msg_svr_base*/bin/msg/bundles/encbylang.properties 以将适当的字符集与 LANG 环境变量相关联。

表 18-11 mboxutil 选项

选项	说明
-o	检查孤立帐户。此选项将在当前邮件传送服务器主机中搜索在 LDAP 中没有相应条目的收件箱。例如， -o 选项将查找已从 LDAP 删除或已移动到另一个服务器主机的所有者的收件箱。对于找到的每个孤立帐户， mboxutil 将把以下命令写入标准输出： mboxutil-d user/*userid*/INBOX 除非已指定 -w
-p *MUTF7_IMAP_pattern*	与 -l 选项一起使用时，仅列出名称与 *MUTF7_IMAP_pattern* 匹配的那些邮箱。 还可以与 -d 或 -e 选项一起使用，以删除或清除名称与 *MUTF7_IMAP_pattern* 匹配的邮箱。 您可以使用 IMAP 通配符。此选项需要的是格式为 IMAP M-UTF-7 的模式。不建议您使用此方法来搜索非 ascii 邮箱。要搜索非 ascii 邮箱，请使用 -P 选项。
-P *regexp*	仅列出那些名称与指定的 POSIX 正则表达式匹配的邮箱。此选项需要本地语言的 *regexp*
-q *domain*	已作废。使用 imquotacheck -d *domain*
-r *oldname newname* [*partition*]	将邮箱从 *oldname* 重命名为 *newname*。要将文件夹从一个分区移动到另一个分区，请使用 *partition* 选项指定新分区。可以与 -f 标志一起使用以使用文件。 此选项可用于重命名用户。例如， mboxutil -r user/user1/INBOX user/user2/INBOX 可以将所有邮件和邮箱从 user1 移到 user2，并在新的 INBOX 中显示新邮件。（如果 user2 已经存在，则此操作将会失败。）
-R *mailbox*	用于恢复已删除但尚未被清除的邮件。 在邮箱被清除或过期时，已删除邮件的 uid 将存储在 store.exp 文件中。 cleanup 页面已通过之后， imexpire 将物理删除这些邮件。错误地发布了清除或过期消息时，此选项可用于将已删除但尚未被 imexpire 清除的邮件恢复至原始邮箱。
-s	在与 -l 选项一起使用时，仅显示邮箱名称。将不显示其他任何数据。
-t *num*	列出在指定天数未被访问的邮箱 (*num*)。 -t 选项必须与 -o 选项 （它用于标识孤立邮箱）一起使用。 从而使 -t 选项可以同时标识非活动邮箱 （基于最近一次访问的日期）和孤立邮箱（在 LDAP 目录中没有相应用户条目的邮箱）。 要标识（列出）孤立的邮箱或非活动邮箱，请使用 mboxutil -o -w *file* -t *num*℄ 要将这些孤立邮箱和非活动邮箱标记为删除，请使用 mboxutil -d -f *file*，其中 *file* 与前面的 -w *file* 所使用的文件是同一个文件。 要使用此功能，config 变量 local.enablelastaccess 已被启用的天数必须至少为 -t 选项所指定的天数。
-u *user*	已作废。用于列出用户信息。使用 imquotacheck -u *user*
-w *file*	与 -o 选项一起使用。将由 -o 选项 （标识孤立帐户）生成的邮箱名称写入文件。
-x	与 -l 选项一起使用时，将显示邮箱的路径和访问控制。

注 POSIX 正则表达式可用于 mboxutil 命令中。

邮箱命名惯例

必须用以下格式指定邮箱名称：user/*userid*/*mailbox*，其中 *userid* 是拥有邮箱的用户， *mailbox* 是邮箱的名称。对于托管域， *userid* 是 *uid@domain*。

例如，以下命令将为用户 ID 为 crowe 的用户创建名为 INBOX 的邮箱。INBOX 是用于将邮件传送给用户 crowe 的默认邮箱。

```
mboxutil -c user/crowe/INBOX
```

重要提示：名称 INBOX 是为每个用户保留的默认邮箱。 INBOX 是唯一不区分大小写的文件夹名称。所有其他文件夹名称都区分大小写。

示例

要列出所有用户的所有邮箱，请运行以下命令：

```
mboxutil -l
```

要列出所有邮箱并且包含路径和 ACL 信息，请运行以下命令：

```
mboxutil -l -x
```

要为用户 daphne 创建名为 INBOX 的默认邮箱，请运行以下命令：

```
mboxutil -c user/daphne/INBOX
```

要为用户 delilah 删除名为 projx 的邮件文件夹，请运行以下命令：

```
mboxutil -d user/delilah/projx
```

要为用户 druscilla 删除名为 INBOX 的默认邮箱及**所有邮件文件夹**，请运行以下命令：

```
mboxutil -d user/druscilla/INBOX
```

要将用户 desdemona 的邮件文件夹 memos 重命名为 memos-april，请运行以下命令：

```
mboxutil -r user/desdemona/memos user/desdemona/memos-april
```

要将用户 dimitria 的邮件帐户移动到新分区，请运行以下命令：

```
mboxutil -r user/dimitria/INBOX user/dimitria/INBOX partition
```

其中 *partition* 用于指定新分区的名称。

要将用户 dimitria 的名为 personal 的邮件文件夹移动到新分区，请运行以下命令：

```
mboxutil -r user/dimitria/personal user/dimitria/personal partition
```

删除孤立帐户

要搜索孤立帐户 （孤立帐户是在 LDAP 中没有相应条目的邮箱），请使用以下命令：

mboxutil -o

命令输出如下所示：

```
mboxutil:Start checking for orphaned mailboxes
user/annie/INBOX
user/oliver/INBOX
mboxutil: Found 2 orphaned mailbox(es)
mboxutil: Done checking for orphaned mailboxes
```

使用以下命令创建列出可转换为脚本文件的孤立邮箱的文件，用于删除孤立邮箱（示例文件名为 orphans.cmd）：

mboxutil -o -w orphans.cmd

命令输出如下所示：

```
mboxutil:Start checking for orphaned mailboxes
mboxutil: Found 2 orphaned mailbox(es)
mboxutil: Done checking for orphaned mailboxes
```

使用以下命令删除孤立文件：

mboxutil -d -f orphans.cmd

hashdir 实用程序

邮件存储中的邮箱以散列结构存储以便进行快速搜索。因此，要查找包含特定用户的邮箱的目录，请使用 hashdir 实用程序。

此实用程序可以识别包含特定帐户的邮件存储的目录。此实用程序将报告邮件存储的相对路径，例如 d1/a7/。该路径相对于基于用户 ID 的级别之前的目录级别。实用程序会将路径信息发送到标准输出。

例如，要查找用户 crowe 的邮箱的相对路径，请运行以下命令：

```
hashdir crowe
```

readership 实用程序

`readership` 实用程序将报告有多少用户 （而不是邮箱所有者）已经阅读了共享 IMAP 文件夹中的邮件。

IMAP 文件夹的所有者可以授予其他用户阅读文件夹中的邮件的权限。允许其他用户访问的文件夹称为**共享文件夹**。管理员可以使用 `readership` 实用程序查看有多少用户 （而不是所有者）正在访问共享文件夹。

此实用程序将扫描所有邮箱并为每个共享文件夹生成一行输出，报告阅读者的数量，接着是一个空格和邮箱的名称。

每个阅读者都是在过去的指定天数内选择了共享文件夹的独特验证身份。用户阅读自己的个人邮箱时系统不进行计数。系统不报告个人邮箱，除非至少有一个文件夹所有者以外的阅读者。

例如，以下命令行将在过去 15 天内选择了共享 IMAP 文件夹的任何身份都作为阅读者进行计数：

```
readership -d 15
```

监视配额限制

通过使用 `imqutoacheck` 监视配额使用情况和限制，该命令生成列出已定义的配额和限制的报告，并提供有关配额使用情况的信息。以千字节为单位报告配额和使用情况数字。此实用程序也可以将邮箱大小与用户分配的配额进行比较。此外，您可以选择通过电子邮件向已超出的配额量达到所设置的百分比的用户发送通知。

注 在 `imquotacheck` 中某些功能已更改。（在 Messaging Server 6.x 中，`imquotacheck` 实用程序已取代了 `quotacheck` 实用程序。）在 Messaging Server 5.x 中，当您使用 `quotacheck` 实用程序检索用户列表时，`quotacheck` 搜索本地 `mboxlist` 数据库。此功能复制 `mboxutil` 实用程序中的搜索功能。

在 Messaging Server 6.x 中，此复制功能已从 `imquotacheck` 实用程序中删除。如果您使用 `imquotacheck` 执行用户搜索，将针对 LDAP 目录执行搜索，而不是针对本地 `mboxlist` 数据库。要从本地 `mboxlist` 数据库检索用户列表，请使用 `mboxutil` 实用程序。

要列出配额超出规则文件中的最小阈值的所有用户的使用情况，请运行以下命令：

```
imquotacheck
```

列出域 siroe.com 的配额信息：

```
imquotacheck -d siroe.com
```

要依据默认规则文件向所有用户发送通知，请运行以下命令：

```
imquotacheck -n
```

要依据指定的 *rulefile*、 *myrulefile* 和指定的邮件模板文件 *mytemplate.file* 向所有用户发送通知 （有关详细信息，请参见 Sun Java System Messaging Server Administration Reference），请运行以下命令：

```
imquotacheck -n -r myrulefile -t mytemplate.file
```

要列出所有用户的使用情况 （将忽略规则文件），请运行以下命令：

```
imquotacheck -i
```

要列出用户 user1 的每个文件夹的使用情况 （将忽略规则文件），请运行以下命令：

```
imquotacheck -u user1 -e
```

监视磁盘空间

您可以指定系统监视磁盘空间和分区使用情况的频率，以及系统应在什么情况下发送警告。有关详细信息，请参见第 713 页的 “监视磁盘空间”。

使用 stored 实用程序

stored 实用程序将为服务器执行以下监视和维护任务：

- 后台任务和日常邮件传送任务。
- 死锁检测和死锁数据库事务的回滚。
- 启动时清除临时文件。
- 生存期策略的实现
- 定期监视服务器状态、磁盘空间、服务响应时间等等 （请参见第 724 页的 “stored”）。
- 必要时发出警报。
- 根据需要恢复数据库 （请参见第 560 页的 “邮件存储启动和恢复”）。

stored 实用程序将在每天的 11 PM 自动执行一次清除和过期操作。您可以选择运行其他清除和过期操作。

表 18-12 列出了一些 stored 选项。表后还提供了一些通用使用示例。有关详细的语法和使用要求，请参见 Messaging Server Reference Manual。

表 18-12 stored 选项

选项	说明
-d	已作废。使用 start-msg store 启动将作为守护程序运行的 stored，执行系统检查并激活警报、死锁检测和数据库修复。
-t	检查 stored 的状态。此命令的返回代码将表明状态。
-v	详细输出。
-v -v	更多详细输出。

要打印状态，请输入：

```
stored -t -v
```

如果要更改自动清除和过期操作的时间，请使用 configutil 实用程序，如下所示：

```
configutil -o store.expirestart -v 21
```

有时，您可能需要重新启动 stored 实用程序；例如邮箱列表数据库被破坏时。要在 UNIX 中重新启动 stored，请在命令行中使用以下命令：

msg_svr_base/sbin/stop-msg store
msg_svr_base/sbin/start-msg store

如果任一服务器守护程序崩溃，则必须停止所有守护程序并重新启动所有守护程序，包括 stored。

由于重复存储相同的邮件而减少邮件存储大小

将某邮件发送给多个收件人时，该邮件将被置于每个收件人的邮箱中。某些邮件传送系统将同一邮件的副本分别存储在每个收件人的邮箱中。相反地， Sun Java System Messaging Server 力求保留一个邮件副本，而不考虑该邮件所在的邮箱数。通过在包含该邮件的邮箱中创建指向该邮件的硬链接即可实现此目的。

在将其他邮件传送系统迁移到 Sun Java Messaging Server 时，可能会在迁移过程中将这些多个邮件副本复制到 Sun Java Messaging Server 中。邮件存储会很大，这意味着不必要地重复了很多邮件。此外，在正常的服务器操作中也可能会积累同一邮

件的多个副本，例如，从 IMAP append 操作或其他来源中。

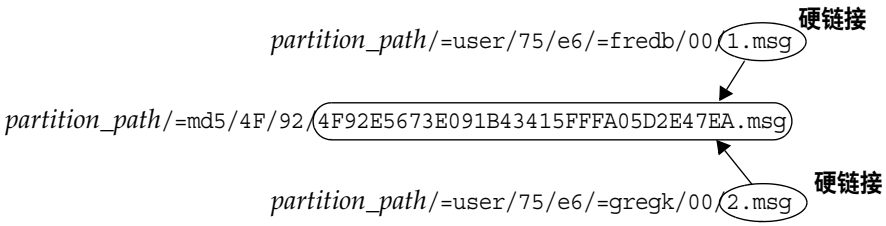
Messaging Server 提供了一个名为 relinker 的新命令，该命令用于删除过量的邮件副本并用指向单个副本的硬链接替换这些邮件副本。

relinker 操作原理

重链接功能可在命令模式或实时模式下运行。当 relinker 命令运行时，它将扫描整个邮件存储分区，创建或更新 MD5 邮件摘要系统信息库 （以硬链接形式），删除过量的邮件文件，并创建必要的硬链接。

摘要系统信息库由指向邮件存储中的邮件的硬链接组成。它存储在目录分层结构 *partition_path*/=md5 中。此目录与用户邮箱分层结构 *partition_path*/=user 并行 （请参见图 18-1 第 494 页）。摘要系统信息库中的邮件可由其 MD5 摘要唯一标识。例如，如果 fredb/00/1.msg 的摘要为 4F92E5673E091B43415FFFA05D2E47，则 *partition*/=user/*hashdir*/*hashdir*/=fredb/00/1.msg 将被链接到 *partition*/=md5/*hashdir*/*hashdir*/4F92E5673E091B43415FFFA05D2E47EA.msg。如果另一个邮箱中也有这封相同邮件 （例如 *partition_path*/=user/*hashdir*/*hashdir*/gregk/00/17.msg），则该邮件也将被硬链接到 *partition_path*/=md5/4F/92/4F92E5673E091B43415FFFA05D2E47EA.msg。如图 18-5 第 540 页所示。

图 18-5 邮件存储摘要系统信息库



对于这封邮件，链接计数为三。如果从 fredb 和 gregk 邮箱中删除了这两封相同邮件，则链接计数为一并且可以清除此邮件。

还可以在实时模式下运行 relinker 进程以实现类似的功能。有关详细信息，请参见第 542 页的 “在实时模式下使用 relinker”。

在命令行模式中使用 relinker

relinker 将扫描整个邮件存储分区，创建或更新 MD5 邮件系统信息库 （以硬链接形式）并删除过量的邮件文件。 relinker 扫描完存储分区后，它将输出唯一邮件数和重链接前后分区大小的统计信息。为了在已散列的存储上更快速地运行，relinker 将只计算尚未存在于 =md5 中的邮件摘要。它还具有可以删除整个摘要系统信息库 （此操作不会影响用户邮箱）的选项。

命令的语法如下所示：

relinker [-p *partitionname*] [-d]

其中 *partitionname* 指定要处理的分区 （默认值：所有分区）， -d 指定将删除摘要系统信息库。以下显示了输出样例：

```
# relinker

Processing partition: primary
Scanning digest repository...
Processing user directories.............................
------------------------------------------------------------
Partition statistics                Before        After
------------------------------------------------------------
Total messages                     4531898      4531898
Unique messages                    4327531      3847029
Message digests in repository            0      3847029
Space used                           99210Mb      90481Mb
Space savings from single-copy        3911Mb      12640Mb
------------------------------------------------------------

# relinker -d

Processing partition: primary
Purging digest repository...
------------------------------------------------------------
Partition statistics                Before        After
------------------------------------------------------------
Message digests in repository      3847029            0
------------------------------------------------------------
```

运行 relinker 可能需要花费很长时间，尤其是在系统信息库中没有邮件的情况下首次运行。这是因为如果将 relinker 条件配置为包含所有邮件，则 relinker 必须计算每封邮件的摘要 （有关配置 relinker 条件的信息，请参见第 543 页的 “配置 relinker”）。例如，处理 100 千兆字节的邮件存储可能需要花费六个小时。但是，如果启用了运行时重链接 （请参见第 542 页的 “在实时模式下使用 relinker”），则无需运行 relinker 命令。

如果单独使用 relinker 命令行模式，而不使用运行时选项，则必须清除摘要系统信息库 (=md5)，否则存储 (=user) 中清除的邮件所占用的空间将不能成为可用磁盘空间，因为在摘要系统信息库中仍有这些邮件的链接 （它们将成为孤立邮件）。如果只执行存储的一次性优化 （例如，在迁移后），您可以运行一次 relinker，然后使用 relinker -d 删除整个系统信息库。对于迁移过程中进行的重复清除，只要重复运行 relinker 命令就可以了，因为每次运行该命令时，还会从系统信息库中清除过期的或孤立的邮件。

并行运行 relinker 的多个实例来使每个实例分别处理不同分区 （使用 -p 选项），这样做是最安全的。仅在同一分区内重链接邮件。

在实时模式下使用 relinker

通过将 configutil 参数 local.store.relinker.enabled 设置为 yes 可以在实时模式下启用 relinker 函数。在实时模式下使用 relinker 将计算符合配置的 relinker 条件（第 543 页的 “配置 relinker”）的每封已传送 （或已恢复、 IMAP 已附加等）邮件的摘要，然后查找系统信息库以查看该摘要是否已存在。如果摘要存在， relinker 将在目标邮箱中创建一个指向该摘要的链接而不创建该邮件的新副本。如果摘要不存在， relinker 将创建该邮件，然后在系统信息库中添加指向该邮件的链接。

stored 将扫描每个分区的摘要系统信息库，并清除链接计数为 1 或不符合 relinker 条件的邮件。在可配置的时间段内，扫描一次将扫描完一个目录。这样可以平均分布 I/O 负载而不会对其他服务器操作造成明显影响。默认情况下，清除周期为 24 小时，这意味着从存储中删除了邮件或者邮件超过了配置的最大生存期后，这些邮件最多还可在磁盘上保存 24 小时。如果启用了 relinker 实时模式，将启用此任务。

配置 relinker

表 18-13 显示了用于设置 relinker 条件的参数。

表 18-13 `relinker configutil` 参数

参数	说明
local.store.relinker.enabled	在附加代码中启用实时重链接邮件并启用 `stored` 清除。即使此选项处于禁用状态，也可以运行 `relinker` 命令行工具，但由于 `stored` 将不清除系统信息库，因此必须将 `relinker -d` 用于此任务。启用此选项将影响邮件传送性能但可以节省磁盘空间。 默认值：否
local.store.relinker.maxage	保存在系统信息库中或由 relinker 命令行考虑的邮件最大生存期 （以小时为单位）。 -1 表示无生存期限制，即仅从系统信息库中清除孤立邮件。对于 `relinker`，它表示处理现有邮件而不考虑生存期。值越小保留的系统信息库也就越小，从而允许 `relinker` 或 `stored` 清除可以更快地运行并更快地收回磁盘空间；而值越大允许重复邮件重链接的时间就越长，例如，用户分几天将同一邮件复制到存储中，或在几天或几星期内运行迁移等情况。 默认值：24
local.store.relinker.minsize	邮件的最小大小 （以千字节为单位），由运行时 relinker 或命令行 relinker 考虑。设置为非零值将失去 relinker 用于较小邮件的优点，但可以获得较小的系统信息库。 默认值：0
local.store.relinker.purgecycle	整个 `stored` 清除周期的近似持续时间 （以小时为单位）。实际持续时间取决于扫描系统信息库中的每个目录所花费的时间。值越小使用的 I/O 就越多；值越大收回磁盘空间的速度就越慢。0 表示连续运行清除而不在目录之间有任何暂停。-1 表示不使用 `stored` 而必须使用 `relinker -d` 命令执行清除。 默认值：24

备份并恢复邮件存储

邮件存储备份和恢复是最常见和最重要的管理任务之一。它由备份邮件存储中的所有邮件和文件夹组成。必须实现邮件存储的备份和恢复策略，以确保发生以下问题时不会丢失数据：

- 系统崩溃
- 硬件故障
- 邮件或邮箱的意外删除
- 重新安装或升级系统时出现问题
- 自然灾难 （例如，地震、火灾、飓风）
- 迁移用户

您可以使用命令行实用程序 `imsbackup` 和 `imsrestore` 或集成解决方案 （使用 Legato Networker®）执行邮件存储备份和恢复。

Messaging Server 将提供单副本备份过程。不管多少用户文件夹包含特定邮件，备份期间仅使用找到的第一封邮件文件备份一次邮件文件。第二封邮件副本将作为第一封邮件文件名称的链接备份，依此类推。 `imsbackup` 将邮件文件的设备和索引节点用作索引来维护所有邮件的散列表。但是，恢复数据时，此方法确实会产生一些影响。有关更多信息，请参见第 549 页的 “部分恢复的注意事项”。

注 还可以通过备份所有邮件文件和目录来执行邮件存储备份和恢复。请参见第 555 页的 “邮件存储灾难备份和恢复”。

本节包含以下小节：

- 第 544 页的 “创建邮箱备份策略”
- 第 545 页的 “创建备份组”
- 第 547 页的 “Messaging Server 备份和恢复实用程序”
- 第 549 页的 “部分恢复的注意事项”
- 第 550 页的 “从已被增量备份的邮箱中恢复邮件”
- 第 551 页的 “使用 Legato Networker”
- 第 554 页的 “使用除 Legato 以外其他的第三方备份软件”
- 第 555 页的 “邮件存储灾难备份和恢复”
- 第 555 页的 “备份和恢复问题的故障排除”
- 第 555 页的 “邮件存储灾难备份和恢复”

创建邮箱备份策略

备份策略将取决于若干因素，例如：

- 高峰业务负载
- 完全备份和增量备份
- 并行备份和串行备份

高峰业务负载

安排系统备份时，需要考虑到高峰业务负载，因为这在高峰时段可以减少系统负载。例如，清晨时段 （例如 2:00 AM）可能是安排备份的最佳时段。

完全备份和增量备份

增量备份 （请参见第 547 页的 “增量备份”）将扫描存储查找更改的数据，并仅备份已经更改的内容。完全备份将备份整个邮件存储。需要确定与增量备份相比系统执行完全备份的频率。您可能需要将增量备份作为每日维护过程执行，而每星期执行一次完全备份。

并行备份和串行备份

用户数据存储在多个磁盘中时，如果需要，可以并行备份用户组。根据系统资源，并行备份可以加速整体备份过程。但是，如果要减少备份对服务器性能的影响，可能需要使用串行备份。使用并行备份还是串行备份可能取决于许多因素，包括系统负载、硬件配置、有多少可用的磁带驱动器等等。

创建备份组

备份组是由正则表达式定义的任意用户邮箱集。通过将用户邮箱组织成备份组，您可以定义更灵活的备份管理。

例如，您可以创建三个备份组，第一个组包含以字母 A 至 L 开始的用户 ID，第二个组包含用户 ID 以 M 至 Z 开始的用户，而第三个组包含用户 ID 以数字开始的用户。管理员可以使用这些备份组以并行方式备份邮箱，也可能一天只备份特定组，另一天备份其他组。

关于备份组有几点事项要记住：

1. 备份组是邮件用户的任意**虚拟**的组。它们不会准确地映射到邮件存储目录 （图 18-1 第 494 页），尽管看上去似乎会这样。
2. 它们由管理员使用 UNIX 正则表达式定义。
3. 正则表达式是在以下配置文件中定义的
   msg_svr_base`/config/backup-groups.conf`
4. `imsbackup` 和 `imsrestore` 中引用备份组时，备份组使用以下路径格式：
   /partition_name/backup_group

backup-groups.conf 格式如下：

```
group_name=definition
group_name=definition
.
.
.
```

使用上述段落中介绍的示例，以下定义将用于创建三个备份组：

```
groupA=[a-l].*
groupB=[m,-z].*
groupC=[0-9].*
```

现在您可以在几个级别中规定 imsbackup 和 imsrestore 的范围。您可以使用以下备份命令备份 / 恢复整个邮件存储：

imsbackup -f *device* /

要备份 groupA 中的所有用户的所有邮箱，请使用以下命令：

imsbackup -f *device* /*partition*/groupA

默认分区称为 primary。

预定义备份组

Messaging Server 包括一个不必创建 backup-groups 配置文件即可用的预定义备份组。此组称为 user ；其中包括所有用户。例如，以下命令将备份 primary 分区上的所有用户：

imsbackup -f backupfile /primary/user

Messaging Server 备份和恢复实用程序

为备份和恢复数据， Messaging Server 提供了 imsbackup 和 imsrestore 实用程序。请注意， imsbackup 和 imsrestore 实用程序不具有在通用工具 （如 Legato Networker）中可以找到的高级功能。例如，实用程序对磁带自动转换器只提供非常有限的支持，并且不能将单个存储写入多个并行设备。综合备份将通过通用工具（如 Legato Networker）的插件来实现。有关使用 Legato Networker 的详细信息，请参见第 551 页的 “使用 Legato Networker”。

imsbackup 实用程序

使用 imsbackup，您可以将邮件存储的选定内容写入任何串行设备，包括磁带、UNIX 管道或纯文本文件。可以在以后使用 imsrestore 实用程序恢复备份或备份的选定部分。可以将 imsbackup 的输出传输到 imsrestore。

以下示例将整个邮件存储备份到 /dev/rmt/0：

```
imsbackup -f /dev/rmt/0 /
```

此示例将用户 ID joe 的邮箱备份到 /dev/rmt/0：

```
imsbackup -f /dev/rmt/0 /primary/user/joe
```

此示例将备份组 groupA 中定义的所有用户的所有邮箱备份到 backupfile （请参见第 545 页的 “创建备份组”）：

```
imsbackup -f- /primary/groupA > backupfile
```

增量备份

以下示例将备份从 2004 年 5 月 1 日下午 1 点 10 分至今所存储的邮件。默认情况下将备份所有邮件而不考虑它们的日期：

```
imsbackup -d 20040501:13100
```

此命令使用默认块因子 20。有关 imsbackup 命令的完整语法说明，请参见 Messaging Server Reference Manual。

imsrestore 实用程序

要从备份设备恢复邮件，请使用 imsrestore 命令。例如，以下命令将从文件 backupfile 中恢复 user1 的邮件。

```
imsrestore -f backupfile /primary/user1
```

有关 imsbackup 命令的完整语法说明，请参见 Messaging Server Reference Manual。

执行备份时排除批量邮件

执行一个备份操作时，您可以指定将从备份中被排除的邮箱。通过排除可以产生大量琐碎邮件的批量邮箱或垃圾邮箱，您可以简化备份会话，减少完成操作的时间，并最小化存储备份数据所需的磁盘空间。

要排除邮箱，请为 configutil 参数 local.store.backup.exclude 指定一个值。

您可以指定单个邮箱或由 % 字符分隔开的邮箱列表。（在邮箱名称中 % 是非法字符。）例如，您可以指定以下值：

```
Trash
```

```
Trash%Bulk Mail%Third Class Mail
```

在第一个示例中，排除了文件夹 Trash。在第二个示例中，排除了文件夹 Trash、Bulk Mail 和 Third Class Mail。

备份实用程序将备份用户邮箱中所有的文件夹，那些以 local.store.backup.exclude 参数指定的文件夹除外。

此功能与 Messaging Server 备份实用程序、Legato Networker 和第三方备份软件一起工作。

您可以覆盖 local.store.backup.exclude 设置，并通过在操作期间指定被排除邮箱的完整逻辑名称以备份此邮箱。假设已排除 “垃圾箱”文件夹。您还可以通过指定以下内容来备份 “垃圾箱”，例如：

```
/primary/user/user1/trash
```

但是，如果指定

```
/primary/user/user1
```

“垃圾箱”文件夹被排除。

部分恢复的注意事项

部分恢复是指仅恢复部分邮件存储。完全恢复是指恢复整个邮件存储。邮件存储使用单副本邮件系统。即，仅将任何邮件的单个副本作为单个文件保存在存储中。该邮件的任何其他实例 （如邮件发送到多个邮箱时）都存储为该副本的链接。由于此原因，恢复邮件时会有一些影响。例如：

- **完全恢复**。完全恢复期间，链接的邮件仍将指向同一个索引节点，将其作为它们要链接到的邮件文件。
- **部分备份 / 恢复**。但是，部分备份和部分恢复期间可能不会保留邮件存储的单副本特征。

以下示例说明了执行部分恢复时，由多个用户使用的邮件发生的变化。假设有三封邮件，同时属于三个用户 A、 B 和 C，如下所示：

```
A/INBOX/1
B/INBOX/1
C/INBOX/1
```

示例 1。在第一个示例中，系统执行部分备份和完全恢复过程步骤，如下所示：

1. 备份用户 B 和 C 的邮箱。
2. 删除用户 B 和 C 的邮箱。
3. 恢复步骤 1 中的备份数据。

在此示例中， `B/INBOX/1` 和 `C/INBOX/1` 被指定了新的索引节点编号，并且邮件数据被写入磁盘上的新位置。仅恢复了一封邮件；第二封邮件是第一封邮件的硬链接。

示例 2。在此示例中，系统执行完全备份和部分恢复，如下所示：

1. 执行完全备份。
2. 删除用户 A 的邮箱。
3. 恢复用户 A 的邮箱。

A/INBOX/1 被指定了新的索引节点编号。

示例 3。在此示例中，部分恢复可能需要多次尝试：

1. 执行完全备份。

   将 `B/INBOX/1` 和 `C/INBOX/1` 备份为 `A/INBOX/1` 的链接。

2. 删除用户 A 和 B 的邮箱。
3. 恢复用户 B 的邮箱。

   恢复实用程序要求管理员首先恢复 A/INBOX。
4. 恢复用户 A 和 B 的邮箱。
5. 删除用户 A 的邮箱 （可选）。

注 如果要确保对所有邮件进行部分恢复，可以运行 imsbackup 命令并使用 -i 选项。如果有必要， -i 选项将多次备份每封邮件。

如果备份设备 （如：驱动器或磁带）可查找， imsrestore 将查找包含 A/INBOX/1 的位置，并将其恢复为 B/INBOX/1。如果备份设备 （如：UNIX 管道）不可查找， imsrestore 将记录对象 ID 和文件的相关 （链接）对象的 ID，并且管理员必须使用 -r 选项再次调用 imsrestore 以恢复缺少的邮件引用。

从已被增量备份的邮箱中恢复邮件

如果您正从已被增量备份的邮箱中恢复邮件，并且该邮箱存在于您要用于恢复邮件的服务器上，那么恢复邮件需要简单而直观的运行 imesrestore。但是，如果您要从已被增量备份的邮箱中恢复邮件，并且该邮箱不再存在，则必须遵循不同的恢复过程。

使用以下过程之一将邮件恢复至不存在于邮件存储服务器上的邮箱中：

- 在恢复操作期间，禁用邮件向用户的传送。通过将 LDAP 属性 mailDeliveryOption 设置为 hold 来实现此操作。
- 在使用 imesrestore 之前，应使用 mboxutil -c 命令创建邮箱。

恢复增量备份必须遵循这些说明的原因如下：在邮箱已被删除或正被迁移时，imsrestore 实用程序将使用存储在备份归档文件中的邮箱唯一标识有效性标志和邮件唯一标识 (UID) 来重新创建邮箱。

以前，当 imsrestore 重新创建已删除或迁移的邮箱时，它将为邮箱分配新的 UID 有效性标志并为邮件分配新的 UID。在这种情况下，带有高速缓存邮件的客户机将必须重新同步邮箱 UID 有效性标志和邮件 UID。客户机将必须再次下载新的数据，增加服务器上的工作负荷。

在新的 imsrestore 行为下，客户机高速缓存将保持同步，并且恢复进程将透明地运行，而不会对性能有负面影响。

如果邮箱存在，imsrestore 将为已恢复的邮件分配新的 UID，从而使新的 UID 与已分配给现有邮件的 UID 保持一致。要确保 UID 的一致性， imsrestore 在恢复操作期间会锁定邮箱。但是，由于 imsrestore 现在使用的是备份归档文件中的邮箱 UID 有效性标志和邮件 UID，而不是分配新的 UID 值，因此如果执行增量备份和恢复，UID 可能会变得不一致。

如果使用 imsbackup 实用程序的 -d 日期选项执行增量备份，则可能需要多次调用 imsrestore 以完成恢复操作。如果执行了增量备份，则必须恢复最新的完全备份和所有后续的增量备份。

新邮件可以在恢复操作期间被传送至邮箱，但在这种情况下，邮件 UID 可能变得不一致。要防止 UID 的不一致，您需要采取以上介绍的操作之一。

使用 Legato Networker

Messaging Server 包括提供了带有第三方备份工具（例如 Legato Networker）的界面的备份 API。物理邮件存储结构和数据格式封装在备份 API 中。备份 API 将直接与邮件存储进行交互式操作。它显示了备份服务的邮件存储的逻辑视图。备份服务使用邮件存储的概念表示法来存储和检索备份对象。

Messaging Server 为备份和恢复邮件存储数据提供了可以由 Legato Networker 的 save 和 recover 命令调用的应用程序特定模块 (ASM)。然后， ASM 将调用 Messaging Server 的 imsbackup 和 imsrestore 实用程序。

注 本节提供有关如何将 Legato Networker 与 Messaging Server 邮件存储一起使用的信息。要了解 Legato Networker 界面，请参见 Legato 文档。

使用 Legato Networker 备份数据

要使用 Legato Networker 执行 Messaging Server 邮件存储的备份，调用 Legato 界面前必须执行以下预备步骤：

1. 创建从 /usr/lib/nsr/imsasm 到 msg_srv_base/lib/msg/imsasm 的符号链接。
2. 从 Sun 或 Legato 获取 nsrfile 二进制的副本并将其复制到以下目录：

   /usr/bin/nsr

   请注意，仅当使用以前版本的 Networker (5.x) 时才需要进行此操作。使用 Networker 6.0 和更高版本时， nsrfile 将自动被安装在 /usr/bin/nsr 下。

3. 如果要按组备份用户，请执行以下步骤：

   a. 创建第 545 页的 “创建备份组”中所述的备份组文件。

   b. 要验证配置，请运行 mkbackupdir.sh。

      查看由 mkbackupdir.sh 创建的目录结构。该结构应与表 18-4 中所示目录结构相似。

      请注意，如果未指定 backup-groups.conf 文件，备份进程将对所有用户使用默认备份组 ALL。

4. 在目录 /nsr/res/ 中，为您的保存组创建 res 文件，以在备份前调用 mkbackupdir.sh 脚本。有关示例，请参见表 18-4。

注 Legato Networker 的早期版本限制保存组的名称为 64 个字符。如果此目录的名称加上邮箱的逻辑名称 （例如 /primary/groupA/fred）超过了 64 个字符，则必须运行 mkbackupdir.sh -p。因此，应该为 mkbackupdir.sh 的 -p 选项使用短路径名。例如，以下命令将在 /backup 下创建备份映像：

```
mkbackupdir.sh -p /backup
```

重要提示：备份目录必须可以由邮件存储所有者 （如：inetuser）。

图 18-6 显示了样例备份组目录结构。

图 18-6 备份组目录结构

```
/backup/primary/groupA/amy
                       /bob
                       /carly
                /groupB/mary
                       /nancy
                       /zelda
                /groupC/123go
                       /1bill
                       /354hut
```

以下示例显示了 /nsr/res 目录中名为 IMS.res 的样例 res 文件：

```
type:savepnpc;
precmd: "echo mkbackupdir started",
   "/usr/siroe/server5/msg-siroe/bin/mkbackupdir.sh -p /backup";
pstcmd: "echo imsbackup Completed";
timeout: "12:00 pm";
```

现在您可以准备运行 Legato Networker 界面，如下所示：

1. 如果有必要，则创建 Messaging Server 保存组。
   a. 运行 nwadmin。
   b. 选择 “自定义” | “组” | “创建”。
2. 使用 savepnpc 作为备份命令创建备份客户机：
   a. 将保存组设置为由 mkbackupdir 创建的目录。

      对于单个会话备份，使用 /backup

      对于并行备份，使用 /backup/*server*/*group*

      确保已经创建如第 545 页的 “创建备份组”中所定义的 *group*。

      还必须设置备份会话数量的并行性。

      请参见第 553 页的 “示例：在 Networker 中创建备份客户机：”。
3. 选择 “组控制” | “启动”以测试备份配置。

示例：在 Networker 中创建备份客户机：

要在 Networker 中创建备份客户机，请从 nwadmin 选择 “客户机” | “客户机设置” | “创建”：

```
Name:siroe
Group: IMS
Savesets:/backup/primary/groupA
   /backup/secondary/groupB
   /backup/tertiary/groupC
         .
         .
Backup Command:savepnpc
Parallelism: 4
```

使用 Legato Networker 恢复数据

要恢复数据，可以使用 Legato Networker `nwrecover` 界面或 `recover` 命令行实用程序。以下示例将恢复用户 a1 的 INBOX：

```
recover -a -f -s siroe /backup/siroe/groupA/a1/INBOX
```

下一示例将恢复整个邮件存储：

```
recover -a -f -s siroe /backup/siroe
```

使用除 Legato 以外其他的第三方备份软件

Messaging Server 提供了两种邮件存储备份解决方案，命令行 `imsbackup` 和 Solstice Backup (Legato Networker)。运行单个 `imbackup` 备份整个邮件存储的大型邮件存储将花费相当长的时间。 Legato 解决方案支持多个备份设备上的并行备份会话。并行备份可以显著缩短备份时间 （可达到每小时可备份 25GB 数据）。

如果使用的是其他第三方并行备份软件 （例如， Netbackup），可以使用以下方法将备份软件与 Messaging Server 集成。

1. 将用户分成组 （请参见第 545 页的 “创建备份组”），并在目录 *msg_svr_base*`/config/` 下创建 `backup-groups.conf` 文件。

注	此备份解决方案需要附加的磁盘空间。要并行备份所有组，磁盘空间要求将是邮件存储大小的两倍。如果没有足够的磁盘空间，请将用户分成较小的组，然后一次备份一个组集。例如 group1 至 group5， group6 至 group10。备份后删除组数据文件。

2. 运行 `imsbackup` 将每个组备份到中转区下的文件中。

   命令是 `imsbackup -f <device> /<instance>/<group>`

   可以同时运行多个 `imsbackup` 进程。例如：

   ```
   # imsbackup -f- /primary/groupA > /bkdata/groupA &
   # imsbackup -f- /primary/groupB > /bkdata/groupB &
   ...
   ```

   `imsbackup` 不支持大型文件，如果备份数据大于 2 GB，则需要使用 `-f-` 选项将数据写入 `stdout` 然后将输出传输到一个文件中。

3. 使用第三方备份软件以备份中转区 （在我们的示例中是 /bkdata）中的组数据文件。

4. 要恢复用户，请标识用户的组文件名，从磁带恢复该文件，然后使用 imsrestore 从数据文件恢复用户。

   请注意， imsrestore 不支持大型文件。如果数据文件大于 2GB，请使用以下命令：

   ```
   # cat /bkdata/groupA | imsrestore -f- /primary/groupA/andy
   ```

备份和恢复问题的故障排除

本节介绍常见的备份和恢复问题及其解决方法。

- **问题**：当使用 imsrestore 或 imsasm 恢复文件夹或 INBOX 时，它会把该文件夹中所有的邮件附加至当前文件夹。这将导致该文件夹中存在这些邮件的多个副本。

  解决方案：确保 imsasm 脚本中未设置 imsrestore 的 -i 标志。

- **问题**：我只想对邮件文件夹中新添加的邮件进行增量备份，但当我进行尝试时，整个文件夹都进行了备份。如何只备份新添加的邮件呢？

  解决方案：在 imsbackup 上设置 -d *datetime* 标志。这将备份从指定日期和时间至今所存储的邮件。默认情况下将备份所有邮件而不考虑它们的日期。

邮件存储灾难备份和恢复

灾难是指整个邮件存储的灾难性故障。即邮件存储服务器上的所有数据全部丢失的情况。完整的邮件存储灾难恢复将包含恢复以下丢失的数据：

- 所有邮件存储数据。可以使用第 543 页的 “备份并恢复邮件存储”中说明的过程备份这些数据。如果使用了文件系统备份方法，请确保备份以下数据：
  - 所有邮件存储分区
  - 位于 msg_svr_base/data/store/mboxlist 的邮件存储数据库文件。
- 位于 msg_svr_base/data/store/dbdata/snapshots 的邮件存储数据库快照 （请注意，可以使用 configutil 参数 local.store.snapshotpath 配置邮件存储数据库快照文件的位置）。（如果使用了文件系统备份，请在恢复这些数据后运行 reconstruct -m。）

- 所有配置数据。包括：
  - 位于 msg_svr_base/data/config 的本地配置文件
  - LDAP Directory Server 中的 Messaging Server 配置数据

监视用户访问

Messaging Server 提供了命令 imsconnutil，允许您监视通过 IMAP、 POP 和 http 进行的用户的邮件存储访问。您还可以确定用户的上次登录和注销时间。此命令在每个邮件存储的基础上运行，不能在多个邮件存储之间运行。

注 使用此功能或其他 Messaging Server 功能对用户的电子邮件进行监视、阅读或其他访问时，如果这些行为与相关法律或法规相违背，或与用户自己的策略或协议相违背，则可能构成潜在的责任源。

此命令需要系统用户 （默认值：inetuser），并且必须将配置变量 local.imap.enableuserlist、 local.http.enableuserlist 和 local.enablelastaccess 设置为 1。

要列出当前通过 IMAP 或任何 Web 邮件客户机登录的用户，请使用以下命令：

```
# imsconnutil -c
```

要列出邮件存储上每个用户的上一次 IMAP、 POP 或 Messenger Express 访问 （登录和注销），请使用：

```
# imsconnutil -a
```

以下命令可以完成两项任务：1) 确定指定用户当前是否已通过 IMAP 或 Messenger Express 或者任何通过 mshttp 连接的客户机登录 （请注意，此项不适用于 POP，因为 POP 用户通常不保持连接）， 2) 列出用户上次登录和注销的时间：

```
# imsconnutil -c -a -u user_ID
```

请注意，使用以下命令可以从文件输入用户列表，每行一个用户：

```
# imsconnutil -c -a -f filename
```

您还可以使用 -s 标志指定特定服务 （imap 或 http）。例如，要列出特定用户 ID 是否已登录 IMAP，使用以下命令：

```
# imsconnutil -c -s imap -u user_ID
```

有关 imsconnutil 语法的完整说明，请参见 Sun Java System Messaging Server Administration Reference。

下面是某个示例的输出：

```
$ ./imsconnutil -a -u soroork
UID IMAP last accessHTTP last accessPOP last access
================================================================================
soroork 08/Jul/2003:10:49:0510/Jul/2003:14:55:52----NOT-RECORDED----

$ ./imsconnutil -c
IMAP
UID TIME AUTH         TO          FROM
================================================================================
ed  17/Jun/2003:11:24:03plain172.58.73.45:193129.157.12.73:2631
bill17/Jun/2003:04:28:43plain172.58.73.45:193129.158.16.34:2340
mia 17/Jun/2003:09:36:54plain172.58.73.45:193192.18.184.103:3744
jay 17/Jun/2003:05:38:46plain172.58.73.45:193129.159.18.123:3687
paul17/Jun/2003:12:23:28plaintext172.58.73.45:193192.18.194.83:2943
tony17/Jun/2003:05:38:46plain172.58.73.45:193129.152.18.123:3688
anil17/Jun/2003:12:26:40plaintext172.58.73.45:193192.18.164.17:1767
anil17/Jun/2003:12:25:17plaintext172.58.73.45:193129.150.17.34:3117
jack17/Jun/2003:12:26:32plaintext172.58.73.45:193129.150.17.34:3119
toni17/Jun/2003:12:25:32plaintext172.58.73.45:193192.18.148.17:1764
================================================================================
10 users were logged in to imap.
Feature is not enabled for http.
--------------------------------------------------------------------------------
```

邮件存储故障排除

本节提供有关活动时维护邮件存储的原则。此外，本节还介绍了当邮件存储被破坏或者意外关闭时，可以使用的其他邮件存储恢复过程。请注意，有关这些附加邮件存储恢复过程的小节是第 563 页的 “修复邮箱和邮箱数据库”的扩展。

阅读本节前，强烈建议您查阅本章以及 Sun Java System Messaging Server Administration Reference 中有关命令行实用程序和 configutil 的章节。本节涉及的主题包括：

- 第 558 页的 “标准邮件存储监视过程”
- 第 567 页的 “常见问题和解决方案”

- 第 560 页的 “邮件存储启动和恢复”
- 第 563 页的 “修复邮箱和邮箱数据库”

标准邮件存储监视过程

本节概述了邮件存储的标准监视过程。这些过程有助于常规邮件存储检查、测试和标准维护。

有关其他信息，请参见第 722 页的 “监视邮件存储”。

检查硬件空间

邮件存储应具有足够的附加磁盘空间和硬件资源。邮件存储接近磁盘空间和硬件空间的最大限度时，邮件存储内部可能会出现问题。

磁盘空间不足是导致邮件服务器问题和故障的最常见的原因之一。如果没有用于写入到邮件存储的空间，邮件服务器将会失败。此外，可用磁盘空间低于特定阈值时，会产生与邮件传送、日志记录等相关的问题。当 `stored` 进程的清除功能失败并且不从邮件存储中擦除已删除的邮件时，磁盘空间会迅速耗尽。

有关监视磁盘空间的信息，请参见第 538 页的 “监视磁盘空间”和第 722 页的 “监视邮件存储”。

检查日志文件

检查日志文件以确保邮件存储进程按配置运行。 Messaging Server 为其支持的以下每个主要协议 （或服务）都创建了一组单独的日志文件：SMTP、 IMAP、 POP 和 HTTP。您可以从 Console 或目录 *msg_svr_base*`/log/` 中查看日志文件。应按例行程序监视日志文件。

请注意日志记录可能会影响服务器性能。在给定的时间内，指定的日志记录越详尽，日志文件所占用的磁盘空间越多。您应当为服务器定义有效且实际的日志旋转、失效和备份策略。有关为服务器定义日志记录策略的信息，请参见第 21 章 “管理日志记录”。

检查用户 IMAP/POP 会话

Messaging Server 提供了一种称为遥测的功能，可以将用户的全部 IMAP 或 POP 会话捕获到文件中。此功能对调试客户机问题很有用。例如，如果用户抱怨他们的邮件访问客户机未按预期那样工作，则此功能可用于跟踪访问客户机和 Messaging Server 之间的交互作用。

要捕获会话，只需创建以下目录：

msg_svr_base/data/telemetry/*pop_or_imap*/*userid*

Messaging Server 将在此目录中为每个会话创建一个文件。下面显示了输出示例：

```
LOGIN redb 2003/11/26 13:03:21
>0.017>1 OK User logged in
<0.047<2 XSERVERINFO MANAGEACCOUNTURL MANAGELISTSURL MANAGEFILTERSURL
>0.003>* XSERVERINFO MANAGEACCOUNTURL {67}
http://redb@cuisine.blue.planet.com:800/bin/user/admin/bin/enduser
MANAGELISTSURL NIL MANAGEFILTERSURL NIL
2 OK Completed
<0.046<3 select "INBOX"
>0.236>* FLAGS (\Answered Élagged áraft áeleted \Seen $MDNSent Junk)
* OK [PERMANENTFLAGS (\Answered Élagged áraft áeleted \Seen $MDNSent Junk \*)]
* 1538 EXISTS
* 0 RECENT
* OK [UNSEEN 23]
* OK [UIDVALIDITY 1046219200]
* OK [UIDNEXT 1968]
3 OK [READ-WRITE] Completed
<0.045<4 UID fetch 1:* (FLAGS)
>0.117>* 1 FETCH (FLAGS (\Seen) UID 330)
* 2 FETCH (FLAGS (\Seen) UID 331)
* 3 FETCH (FLAGS (\Seen) UID 332)
* 4 FETCH (FLAGS (\Seen) UID 333)
* 5 FETCH (FLAGS (\Seen) UID 334)
<etc>
```

检查 stored 进程

stored 功能可执行各种重要任务，例如邮件数据库的死锁和事务操作、强制执行生存期策略以及擦除和删除磁盘上存储的邮件。如果 stored 停止运行， Messaging Server 最终会出现问题。如果 start-msg 运行时 stored 未启动，则其他进程也不会启动。

- 检查 stored 进程是否正在运行。运行 stored -t -v
- 检查在 *store_root*/mboxlist 中生成的日志文件。
- 在默认日志文件 *msg_svr_base*/log/default/default 中检查 stored 邮件
- 检查每当 stored 进程尝试以下功能之一时，以下文件的时间戳（位于目录 *msg_svr_base*/config/ 中）是否已更新：

表 18-14 stored 操作

stored 操作	功能
stored.ckp	初始化数据库检查点时触及到该文件。大约每 1 分钟标记一次。
stored.lcu	每次清除数据库日志时触及该文件。大约每 5 分钟标记一次时间戳。
stored.per	每次产生精读用户数据库写出时触及该文件。每小时标记一次时间戳。

有关 stored 进程的详细信息，请参见第 538 页的 “使用 stored 实用程序”和 Messaging Server Reference Manual 的 "Messaging Server Command-line Utilities" 一章中关于 stored 实用程序的部分。

有关监视 stored 功能的其他信息，请参见第 722 页的 “监视邮件存储”。

检查数据库日志文件

数据库日志文件是指 sleepycat 事务检查点操作日志文件 （位于目录 *store_root*/mboxlist 中）。如果日志文件堆积，则不会出现数据库检查点操作。通常，单个时间段内存在两个或三个数据库日志文件。如果有更多文件，则可能是问题的征兆。

检查用户文件夹

如果要检查用户文件夹，可以运行命令 reconstruct -r -n （递归无修复），此命令将查看所有用户文件夹并报告错误。有关 reconstruct 命令的详细信息，请参见第 563 页的 “修复邮箱和邮箱数据库”。

检查主存文件

仅当进程已经意外终止时才会存在主存文件。查阅这些文件很重要，特别是在邮件存储中发现问题时。在 Solaris 中，使用 coreadm 配置 core 文件位置。

邮件存储启动和恢复

邮件存储数据由邮件、索引数据和邮件存储数据库组成。虽然此数据相当可靠，在极少时候系统中也可能出现邮件存储数据问题。这些问题将在默认日志文件中指出，并且几乎始终透明地被修复。在极少情况下，日志文件中的错误消息可能会指出您需要运行 reconstruct 实用程序。此外，作为最后的手段，邮件将由第 543 页的 “备份并恢复邮件存储”中所述的备份和恢复进程保护。本节将着重说明 stored 的自动启动和恢复进程。

邮件存储自动执行许多恢复操作，这以前是管理员的职责。启动期间，邮件存储守护进程 stored 将执行这些操作，包括数据库快照和必要时的自动快速恢复。 stored 将彻底检查邮件存储的数据库并在检测到问题时自动启动修复。

stored 还通过默认日志的状态消息提供数据库状态的综合分析，报告对邮件存储完成的修复和使其运行的自动尝试。

自动启动和恢复操作原理

stored 守护程序将在其他邮件存储进程之前启动。如果有必要，它将初始化并恢复邮件存储数据库。邮件存储数据库可保存文件夹、配额、订阅和邮件标志信息。数据库可以进行日志记录和处理事务，因此已经内置了恢复。此外，某些数据库信息将在每个文件夹的邮件索引区域中大量地被复制。

尽管数据库相当可靠，但在极少情况下也会中断。在大多数情况下， stored 可以透明地恢复和修复数据库。但是，无论何时重新启动 stored，都应检查默认日志文件以确保不需要其他管理介入。如果数据库需要进一步重建，日志文件中的状态消息将提醒您运行 reconstruct。

打开邮件存储数据库前， stored 将分析其完整性，并将状态消息发送到**警告**类别下的默认日志。某些邮件将对管理员很有用，某些邮件将由用于内部分析的编码数据组成。如果 stored 检测到任何问题，则将尝试修复数据库并尝试再次启动数据库。

打开数据库时， stored 将以信号表明其余服务可以启动。如果自动修复失败，默认日志中的消息将指定要采取的措施。有关详细信息，请参见第 562 页的 “表示需要 reconstruct -m 的错误消息”。

在以前的版本中， stored 可能会花费很长时间启动恢复进程，致使管理员怀疑 stored 是否被 “阻塞” 了。这种长时间的恢复现在已不存在， stored 将在一分钟内确定最终状态。但是，如果 stored 需要使用恢复技术 （例如从快照恢复），则进程可能会花费几分钟时间。

大多数恢复之后，数据库通常会更新，并且不需要进行任何其他操作。但是，某些恢复需要 reconstruct -m 以便与邮件存储中的冗余数据同步。同样，这会在默认日志中说明，因此启动后监视默认日志非常重要。即使邮件存储看起来启动和运行正常，运行任何要求的操作 （例如 reconstruct）都是很重要的。

阅读日志文件的另一个原因是可以首先确定导致数据库损坏的原因。尽管 stored 用于调出邮件存储，而不管系统中的任何问题，但是您仍要尝试确定导致数据库损坏的原因，因为这可能是更大的隐藏问题的征兆。

表示需要 *reconstruct -m* 的错误消息

本节介绍需要运行 reconstruct -m 的错误消息类型。

错误消息指示邮箱错误时，运行 reconstruct <mailbox>。示例：

“邮箱 user/joe/INBOX 中的邮件 102 的高速缓存数据无效。需要重建”

“邮箱已破坏，缺少固定标题 :user/joe/INBOX 之外”

“邮箱已破坏， start_offset 在 EOF:user/joe/INBOX 之外”

当错误消息指示数据库错误时，请运行 reconstruct -m。示例：

“正在删除附加数据库日志。请在启动后立即运行 reconstruct -m 以再同步冗余数据”

“从快照恢复数据。请在启动后立即运行 reconstruct -m 以再同步冗余数据”

数据库快照

快照是数据库的热备份，由 stored 使用以在几分钟内透明地恢复中断的数据库。这比使用 reconstruct 要快得多，后者依赖于其他区域中存储的冗余信息。

邮件存储数据库快照操作原理

默认情况下，每 24 小时自动获取一次数据库 （位于 mboxlist 目录中）的快照。默认情况下，快照被复制到 store 目录的子目录中。默认情况下，在任意给定时间有五个快照：一个实时数据库、三个快照和一个数据库 / 已删除副本。数据库 / 已删除副本比较新，并且是抛入 mboxlist 数据库目录的子目录 removed 中的数据库的紧急副本。

如果恢复进程由于确定数据库已损坏而决定删除当前数据库， stored 会将其移入 removed 目录 （如果可以）。此操作允许在需要时对数据库进行分析。

数据移动一周仅发生一次。如果已存在数据库的副本， stored 将不会在每次进行存储时替换副本。如果 removed 目录中的数据是一星期以前的数据，则仍将替换副本。这是为了防止有问题的原始数据库由于连续启动被替换太快。

指定邮件存储数据库快照的时间间隔和位置

应有五倍的空间用于组合的数据库和快照。强烈建议管理员重新配置快照以在单独的磁盘上运行，并调节快照以满足系统需求。

如果 stored 在启动时检测到数据库的问题，最好的快照将自动被恢复。有三个快照变量，可以设置以下参数：快照文件的位置、获取快照的时间间隔、保存的快照数量。表 18-15 显示了这些 configutil 参数。

获取快照时间间隔太小将会导致给系统带来频繁的负担，并更有可能会将数据库中的问题复制为快照。获取快照时间间隔太大意味着获取快照时数据库要保持过去的状态。

建议采用一天的快照时间间隔，如果问题将在系统中保存若干天并且您希望返回问题存在的时间点以前的时段，则一周或更长的快照时间间隔会很有用。

stored 可以监视数据库并且非常智能，如果检测到数据库不够完好，则拒绝最新快照。而将检索最新、最可靠的快照。尽管快照可能是从一天以前检索的，系统将使用更新的冗余数据并覆盖较早的快照数据 （如果可用）。

因此，快照所起的最终作用是使系统接近最新，并尝试在运行中重建数据来减轻系统剩余部分的负担。

表 18-15 邮件存储数据库快照参数

参数	说明
local.store.snapshotpath	邮件存储数据库快照文件的位置。或者是现有绝对路径，或者是 store 目录的相对路径。 默认值：dbdata/snapshots
local.store.snapshotinterval	快照之间的分钟数。有效值：1 - 46080 默认值：1440 （1440 分钟 = 1 天）
local.store.snapshotdirs	保存的不同快照的数量。有效值：2 - 367 默认值：3

修复邮箱和邮箱数据库

如果一个或多个邮箱已破坏，您可以使用 reconstruct 实用程序重建邮箱或邮箱数据库，并修复所有不一致性。

reconstruct 实用程序将重建一个或多个邮箱或主邮箱文件，并修复所有不一致性。您可以使用此实用程序恢复邮件存储中几乎所有形式的数据破坏。请参见第 562 页的 “表示需要 reconstruct -m 的错误消息”。

注 请注意，低级数据库修复 （例如完成事务和回滚不完全事务）将在启动时自动执行。

表 18-16 列出了 reconstruct 选项。有关详细的语法和使用要求，请参见 Sun Java System Messaging Server Administration Reference (http://docs.sun.com/doc/819-0106)。

表 18-16 reconstruct 选项

选项	说明
-e	在重建之前删除 store.exp 文件。这将消除已删除但未被存储进程清除的邮件的所有内部存储记录。在使用 -i 或 -e 时使用 -f 选项也很有用，因为这些选项仅在文件夹被实际重建的情况下才工作。同样，如果使用 -n 选项 （它执行检查而不是重建），则 -i 和 -e 选项将不工作。 如果 reconstruct 无法检测到损坏，运行 reconstruct -e 将不能恢复已删除的邮件。 -f 将强制执行重建。
-i	用于在重建之前将 store.idx 文件长度设置为零。在使用 -i 或 -e 时使用 -f 选项也很有用，因为这些选项仅在文件夹被实际重建的情况下才工作。同样，如果使用 -n 选项 （它执行检查而不是重建），则 -i 和 -e 选项将不工作。
-f	强制 reconstruct 执行对邮箱的修复。
-l	用于重建 lright.db。
-m	用于执行一致性检查以及修复邮箱数据库 （如果需要）。此选项将检查在假脱机区域中找到的每个邮箱，酌情添加条目或从邮箱数据库删除条目。无论何时添加条目或从数据库删除条目，实用程序都将消息显示到标准输出文件。特别是它修复 folder.db、 quota.db 和 lright.db
-n	仅检查邮件存储，而不对邮箱执行修复。 -n 选项不能单独使用，除非提供了邮箱名称。未提供邮箱名称时， -n 选项必须与 -r 选项一起使用。 -r 选项可以与 -p 选项组合使用。例如，以下任一命令都是有效的： reconstruct -n user/dulcinea/INBOX reconstruct -n -r reconstruct -n -r -p primary reconstruct -n -r user/dulcinea/
-o	作废，请参见 mboxutil -o
-o -d *filename*	作废，请参见 mboxutil -o
-p *partition*	-p 选项用于与 -m 选项一起使用，限制了到指定分区的重建范围。如果未指定 -p 选项，reconstruct 将默认为对所有分区执行操作。特别是它修复 folder.db 和 quota.db，而不是 lright.db。这是因为修复 lright.db 需要对邮件存储中的每个用户进行 acl 扫描。为每个分区执行此操作效率不高。要修复 lright.db，请运行 reconstruct -l。 指定分区名称；不使用全路径名。
-q	修复配额子系统中的所有不一致性，例如带有错误配额根 （其中报告了错误的配额使用情况）的邮箱。其他服务器进程正在运行时，可以运行 -q 选项。
-r [*mailbox*]	修复并对指定邮箱的分区区域执行一致性检查。 -r 选项还将修复指定邮箱内的所有子邮箱。如果不使用任何邮箱参数指定 -r，实用程序将修复用户分区目录内的所有邮箱的假脱机区域。
-u *user*	-u 选项用于与 -m 选项一起使用，限制了到指定用户的重建范围。-u 选项必须与 -p 选项一起使用。如果未指定 -u 选项， reconstruct 默认为对所有分区或由 -p 选项指定的分区进行操作。 指定用户名称；不使用全路径名。

重建邮箱

要重建邮箱，请使用 -r 选项。您应在以下情况使用此选项：

- 访问邮箱时返回以下错误之一：“System I/O 错误”或 “邮箱格式无效”。
- 访问邮箱时导致服务器崩溃。
- 已经向假脱机目录添加文件或从其中删除文件。

reconstruct -r 首先将运行一致性检查。仅在检测到任何问题时报告所有一致性并重建。因此， reconstruct 实用程序的性能在此版本内得到了改进。

您可以使用以下示例中所述的 reconstruct：

要重建属于用户 daphne 的邮箱的假脱机区域，请使用以下命令：

```
reconstruct -r user/daphne
```

要重建邮箱数据库中列出的所有邮箱的假脱机区域，请使用以下命令：

```
reconstruct -r
```

但是，您必须谨慎使用此选项，因为对于大型邮件存储，重建邮箱数据库中列出的所有邮箱的假脱机区域将花费很长时间。（请参见第 566 页的 “reconstruct 性能”。）故障恢复的更好的方法可能是将多个磁盘用于存储。如果一个磁盘出现故障，整个存储不会出现故障。如果一个磁盘破坏，只需使用 -p 选项重建一个存储的分区，如下所示：

```
reconstruct -r -p subpartition
```

要重建命令行参数中列出的邮箱，只要它们位于 primary 分区中，请使用以下命令：

```
reconstruct -p primary mbox1 mbox2 mbox3
```

如果确实需要重建 primary 分区中的所有邮箱，请使用以下命令：

```
reconstruct -r -p primary
```

如果要强制 reconstruct 程序重建文件夹，而不执行一致性检查，请使用 -f 选项。例如，以下命令将强制执行用户文件夹 daphne 的重建：

```
reconstruct -f -r user/daphne
```

要检查所有邮箱而不对其进行修复，请使用 -n 选项，如下所示：

```
reconstruct -r -n
```

检查并修复邮箱

要执行高级别一致性检查和邮箱数据库的修复，请使用以下命令：

```
reconstruct -m
```

要执行主分区的一致性检查和修复，请使用以下命令：

```
reconstruct -p primary -m
```

注 同时运行 reconstruct 与 -p 和 -m 标识将不能修复 lright.db。这是因为修复 lright.db 需要对邮件存储中的每个用户进行 ACL 扫描。为每个分区执行此操作效率不高。要修复 lright.db，请运行 reconstruct -l

要执行名为 john 的单个用户的邮箱的一致性检查和修复，请执行以下命令：

```
reconstruct -p primary -u john -m
```

您应在以下情况下使用 -m 选项：

- 从存储假脱机区域删除了一个或多个目录，因此也需要删除邮箱数据库条目。
- 一个或多个目录被恢复到存储假脱机区域，因此也需要添加邮箱数据库条目。
- stored -d 选项不能使数据库保持一致。

  如果 stored -d 选项不能使数据库保持一致，您应按指示的顺序执行以下步骤：

  - 关闭所有服务器。
  - 删除 *store_root*/mboxlist 中的所有文件。
  - 重新启动服务器进程。
  - 运行 reconstruct -m 以根据假脱机区域的内容建立新邮箱数据库。

reconstruct 性能

reconstruct 执行操作所花费的时间取决于以下因素：

- 要执行的操作和选择的选项的种类
- 磁盘性能
- 运行 reconstruct -m 时文件夹的数量
- 运行 reconstruct -r 时邮件的数量
- 邮件存储的总大小
- 系统运行的其他进程以及系统的繁忙程度

- 是否存在正在进行的 POP、 IMAP、 HTTP 或 SMTP 活动

`reconstruct -r` 选项将执行初始一致性检查；此检查将根据必须重建多少文件夹来改善 `reconstruct` 的性能。

一个具有大约 2400 个用户、85GB 的邮件存储和在服务器上并行的 POP、IMAP 或 SMTP 活动的系统具有如下性能：

- `reconstruct -m` 花费了大约 1 小时
- `reconstruct -r -f` 花费了大约 18 小时

注 如果服务器不执行正在进行的 POP、IMAP、HTTP 或 SMTP 活动，`reconstruct` 操作可能会明显花费较少的时间。

常见问题和解决方案

本节列出了常见的邮件存储问题和解决方案：

- 第 567 页的 “Messenger Express 或 Communications Express 未装入邮件页面”
- 第 567 页的 “使用通配符模式的命令不起作用”
- 第 568 页的 “未知 / 无效分区”
- 第 568 页的 “用户邮箱目录问题”

Messenger Express 或 Communications Express 未装入邮件页面

如果用户无法装入任何 Messenger Express 页面或 Communications Express 邮件页面，则问题可能是数据压缩后被破坏。如果系统部署了过时的代理服务器，则有时可能会出现这种情况。要解决此问题，请尝试将 `local.service.http.gzip.static` 和 `local.service.http.gzip.dynamic` 设置为 0 以禁用数据压缩。如果这样能够解决问题，您可能需要更新代理服务器。

使用通配符模式的命令不起作用

某些 UNIX shell 可能需要用引号引起通配符参数，某些则不需要。例如，C shell 尝试将包含通配符 （*、 ?）的参数扩展为文件，如果找不到匹配项则失败。这些模式匹配参数可能需要包含在引号中，以传递给命令 （如 `mboxutil`）。

例如：

```
mboxutil -l -p user/usr44*
```

将在 Bourne shell 中运行，但在 tsch 和 C shell 中将失败。这些 shell 可能需要以下命令：

```
mboxutil -l -p "user/usr44*"
```

如果使用通配符模式的命令不起作用，请验证是否需要为该 shell 的通配符使用引号。

未知 / 无效分区

如果用户邮箱被移动到刚创建的新分区并且尚未刷新或重新启动 Messaging Server，则用户将会从 Messenger Express 获得消息 “未知 / 无效分区”。此问题仅在新分区中发生。如果现在向此新分区添加其他用户邮箱，则不必刷新 / 重新启动 Messaging Server。

用户邮箱目录问题

当邮件存储的损坏仅限于少数用户且没有对系统造成全局损坏时，将出现用户邮箱问题。以下指导建议了识别、分析和解决用户邮箱目录问题的进程：

1. 查看日志文件、错误消息或用户观察到的任何异常性能。
2. 要保存调试信息和历史记录，请将整个 *store_root*/mboxlist/ 用户目录复制到邮件存储以外的其他位置。
3. 要查找可能导致问题的用户文件夹，请运行命令 `reconstruct -r -n`。如果使用 `reconstruct` 找不到该文件夹，则该文件夹可能不存在于 `folder.db` 中。

   如果使用 `reconstruct -r -n` 命令找不到该文件夹，请使用 `hashdir` 命令以确定位置。有关 `hashdir` 的详细信息，请参见第 536 页的 “hashdir 实用程序”和 Messaging Server Reference Manual 的 "Messaging Server Command-line Utilities" 一章中关于 `hashdir` 实用程序的部分。
4. 找到文件夹后，请检查文件、检查权限并验证正确的文件大小。
5. 使用 `reconstruct -r`（不使用 `-n` 选项）重建邮箱。
6. 如果 `reconstruct` 未检测到您观察到的问题，您可以使用 `reconstruct -r -f` 命令强制执行对邮件文件夹的重建。
7. 如果文件夹不在 `mboxlist` 目录 (*store_root*/mboxlist) 中，而是在 `partition` 目录 (*store_root*/partition) 中，则可能存在全局不一致性。在此情况下，应运行 `reconstruct -m` 命令。
8. 如果前面的步骤不起作用，可以删除 `store.idx` 文件并再次运行 `reconstruct` 命令。

注意 如果确定是在 `reconstruct` 命令无法找到的文件中有问题，则应仅删除 `store.idx` 文件。

9. 如果问题限制为有问题的邮件，则应将邮件文件复制到邮件存储以外的其他位置，并对 mailbox/ 目录运行命令 reconstruct -r。

10. 如果确定文件夹存在于磁盘 （*store_root*/partition/ 目录）上，但是显然不在数据库 （*store_root*/mboxlist/ 目录）中，则运行命令 reconstruct -m 以确保邮件存储的一致性。

有关 reconstruct 命令的详细信息，请参见第 563 页的 “修复邮箱和邮箱数据库”。

store 守护程序不启动

如果 stored 不启动，并显示以下错误消息：

```
# msg_svr_base/sbin/start-msg

msg_svr_base: Starting STORE daemon ...Fatal error:Cannot find group in name
service
```

这表示无法找到 local.servergid 中配置的 UNIX 组。 stored 和其他命令需要将其 gid 设置到该组。有时 local.servergid 定义的组可能会被无意删除。在此情况下，请创建已删除的组，将 inetuser 添加到该组，将 *instance_root* 及其文件的拥有权更改为 inetuser 和该组。

第 19 章

配置安全和访问控制

Messaging Server 支持各种灵活的安全功能，这些功能使您可以防止邮件被截、防止盗窃信息者冒充用户或管理员，并仅允许特定用户访问邮件传送系统的特定部分。

Messaging Server 安全体系结构从整体上看是 Sun Java System 服务器的安全体系结构的一部分。此体系结构依照工业标准和公共协议建立，从而在最大程度上实现了互操作性和一致性。因此，要实现 Messaging Server 安全策略，则您不仅需要参见本章，还需要参见若干其他文档。特别是，设置 Messaging Server 安全性时需要参见 《 Sun ONE Server Console 5.2 Server Management Guide 》中的信息。

本章包含以下各节：

- 第 572 页的 “关于服务器安全性”
- 第 573 页的 “关于 HTTP 安全性”
- 第 573 页的 “配置验证机制”
- 第 577 页的 “用户密码登录”
- 第 578 页的 “配置加密和基于证书的验证”
- 第 589 页的 “配置管理员对 Messaging Server 的访问”
- 第 591 页的 “配置客户机对 POP、 IMAP 和 HTTP 服务的访问”
- 第 601 页的 “启用 POP Before SMTP”
- 第 604 页的 “配置客户机对 SMTP 服务的访问”

关于服务器安全性

服务器安全性包括一系列广泛的主题。在大多数企业中，确保只有授权的用户才能访问服务器、确保密码或标识不被泄漏、确保通信时用户没有不适当地代表其他人，以及确保在必要时可以进行保密通信都是对邮件传送系统的重要要求。

危及服务器安全性的原因很多，因此或许可以通过多种途径来增强这一安全性。本章着重介绍设置加密、验证和访问控制。本章讨论了以下与安全性相关的 Messaging Server 主题：

- **用户 ID 和密码登录**：要求用户在登录到 IMAP、POP、HTTP 或 SMTP 时输入其用户 ID 和密码，并要求用户将发件人验证传送给邮件收件人时使用 SMTP 密码登录。
- **加密和验证**：将服务器设置为使用 TLS 和 SSL 协议，以加密通信和验证客户机。
- **管理员访问控制**：使用控制台的访问控制设备可以委托其他用户访问 Messaging Server 和其中某些单个任务。
- **TCP 客户机访问控制**：使用过滤技术来控制哪些客户机可以连接到服务器的 POP、 IMAP、 HTTP 以及经过验证的 SMTP 服务。

并不是所有与 Messaging Server 相关的安全和访问问题都在本章进行讨论。以下是在其他章节中讨论的安全问题：

- **物理安全性**：如果未采取置备措施以确保服务器计算机的物理安全，软件安全性将毫无意义。
- **邮件存储访问**：您可以定义一系列 Messaging Server 的邮件存储管理员。这些管理员可以查看和监视邮箱，并可以控制对邮箱的访问。有关详细信息，请参见第 18 章 “管理邮件存储”。
- **最终用户帐户配置**：使用 Delegated Administrator 产品主要可以维护最终用户帐户信息 （仅对于 Sun LDAP Schema 1 有效）。还可以使用控制台界面管理最终用户帐户。
- **过滤未经请求的大容量电子邮件 (UBE)**：请参见第 17 章 “邮件过滤和访问控制”。

Web 站点提供了大量相关文档，这些文档包含了各种安全主题。有关此处提及的主题的其他背景信息和与安全相关的其他信息，请访问文档 Web 站点 http://docs.sun.com。

关于 HTTP 安全性

Messaging Server 支持用户 ID/ 密码验证、客户机证书验证和 Access Manager。但是，在协议如何处理客户机和服务器之间的网络连接方面有些区别。

POP、 IMAP 或 SMTP 客户机登录到 Messaging Server 后，即建立了一个连接和一个会话。连接将持续会话的全过程 （即从登录到注销）。建立新连接后，客户机必须到服务器上重新验证。

HTTP 客户机登录到 Messaging Server 后，服务器将为客户机提供唯一的会话 ID。在会话过程中，客户机使用此会话 ID 可以建立多个连接。 HTTP 客户机无需对每个连接都重新验证；如果会话被终止并且客户机想要建立新会话，客户机就需要重新验证。（如果 HTTP 会话持续闲置状态达到一定时间，服务器将自动终止 HTTP 会话，并注销客户机；默认的时间段为 2 小时。）

使用以下技术可以改进 HTTP 会话的安全性：

- 会话 ID 与特定的 IP 地址绑定在一起。
- 每个会话 ID 都有与其相关联的超时值；如果在指定时间段内未使用会话 ID，则会话 ID 将无效。
- 服务器保留了一个所有打开的会话 ID 的数据库，因此客户机无法冒充某个 ID。
- 会话 ID 被存储在 URL 中而并非任何 Cookie 文件中。

有关为改进的连接性能指定配置参数的信息，请参见第 5 章“配置 POP、IMAP 和 HTTP 服务”。

有关 Access Manager 的信息，请参见第 129 页的第 6 章 “启用单点登录 (SSO)”。

配置验证机制

验证机制是客户机向服务器证明其标识的特殊方法。 Messaging Server 支持由简单验证和安全层 (SASL) 协议定义的验证方法并支持基于证书的验证。本节介绍了 SASL 机制。有关基于证书的验证的详细信息，请参见第 578 页的 “配置加密和基于证书的验证”。

Messaging Server 支持以下基于密码验证的 SASL 验证方法。

- **PLAIN** — 此机制通过网络传递用户的纯文本密码，在网络上很容易窃听密码。

  请注意， SSL 可用于缓解窃听问题。有关更多信息，请参见第 578 页的 “配置加密和基于证书的验证”。

- **DIGEST-MD5** — RFC 2831 中定义的询问 / 响应验证机制。（Messaging Multiplexor 尚不支持 DIGEST-MD5。）
- **CRAM-MD5** — 一种询问 / 响应验证机制，类似于 APOP，但也适合与其他协议配合使用。在 RFC 2195 中已定义。
- **APOP** — 仅可与 POP3 协议配合使用的询问 / 响应验证机制。在 RFC 1939 中已定义。
- **LOGIN** — 等效于 PLAIN，只为了与 SMTP 验证的预标准实现相兼容。默认情况下，此机制仅可由 SMTP 使用。

使用询问 / 响应验证机制，服务器将询问字符串发送给客户机。客户机则以该询问的散列和用户密码响应。如果客户机的响应与服务器拥有的散列相匹配，则用户通过验证。由于散列不可逆，所以通过网络发送用户密码时不会泄露此密码。

注 POP、 IMAP 和 SMTP 服务支持所有 SASL 机制。 HTTP 服务仅支持纯文本密码机制。

表 19-1 显示了某些 SASL 参数和与 SASL 相关的 `configutil` 参数。有关 `configutil` 参数的最新和最完整列表，请参见 Sun Java System Messaging Server Administration Reference。

表 19-1 某些 SASL 参数和与 SASL 相关的 `configutil` 参数

参数	说明
`sasl.default.ldap.has_plain_passwords`	该值为布尔值，表示目录存储了可以启用 APOP、 CRAM-MD5 和 DIGEST-MD5 的纯文本密码。 默认值：False
`sasl.default.transition_criteria`	不再支持或使用。请参见 `sasl.default.auto_transition`。
`sasl.default.auto_transition`	布尔值。设置此参数后，当用户提供纯文本密码时，系统将把此密码存储格式转换为目录服务器的默认密码存储格式。此参数可用于从纯文本密码迁移到 APOP、CRAM-MD5 或 DIGEST-MD5。 默认值：False
`service.imap.allowanonymouslogin`	此参数使 IMAP 可以使用 SASL ANONYMOUS 机制。 默认值：False

表 19-1 某些 SASL 参数和与 SASL 相关的 configutil 参数

参数	说明
service.{imap|pop|http}.plaintextmincipher	如果此参数 > 0，则只有激活安全层 （SSL 或 TLS）才能使用纯文本密码。这强制用户必须在要登录的客户机上启用 SSL 或 TLS，以防止在网络中泄露其密码。MMP 具有等效选项 “RestrictPlainPasswords”。 注意：实际上， 5.2 发行版的 Messaging Server 将针对由 SSL 或 TLS 协商的加密算法的程度来检查该值。为了简化此选项并更好地反映一般情况下的使用，已将此功能去除。 默认值：0
sasl.default.mech_list	要启用的以空格分隔的 SASL 机制的列表。如果非空，则此选项将覆盖 sasl.default.ldap.has_plain_passwords 选项以及 service.imap.allowanonymouslogin 选项。此选项应用于所有协议 （IMAP、POP、 SMTP）。 默认值：False
sasl.default.ldap.searchfilter	如果没有在 inetDomainSearchFilter 中为域指定搜索过滤器，则它就是用于查找用户的默认搜索过滤器。语法与 inetDomainSearchFilter 相同 （请参见模式指南）。 默认值：(&(uid=%U)(objectclass=inetmailuser))
sasl.default.ldap.searchfordomain	默认情况下，验证系统将按照域查找规则 （需要引用）在 LDAP 中查找域，然后查找用户。但是，如果该选项被设置为 “0”而不是默认值 “1”，则不会进行域查找并且针对用户的搜索 （使用 sasl.default.ldap.searchfilter）将在由 local.ugldapbasedn 指定的 LDAP 树下直接进行。此参数提供了与传统单域模式的兼容性，但建议不要在新部署中使用此参数，因为即使小公司也可能进行合并或更名，这些都需要多个域的支持。

配置访问纯文本密码的步骤

要运行 CRAM-MD5、 DIGEST-MD5 或 APOP SASL 验证方法，均需要访问用户的纯文本密码。您需要执行以下步骤：

1. 将 Directory Server 配置为以明文存储密码。
2. 配置 Messaging Server，以便其明确 Directory Server 正使用明文密码。

配置 Directory Server 以存储密码的步骤

要启用 CRAM-MD5、 DIGEST-MD5 或 APOP 机制，则必须按以下步骤将 Directory Server 配置为以明文存储密码：

1. 在 “控制台”中，打开您想要配置的 Directory Server。
2. 单击 “配置”选项卡。

3. 打开左窗格中的 “数据”。
4. 单击右窗格中的 “密码”。
5. 从 “密码加密”下拉式列表中选择 “明文”。

注 此更改仅影响以后创建的用户。现有用户则只能在作了此更改后转换或重置其密码。

配置 Messaging Server 的步骤

现在可以配置 Messaging Server，以便其明确 Directory Server 可以检索明文密码。此操作可以使 Messaging Server 安全地公布 APOP、 CRAM-MD5 和 DIGEST-MD5：

```
configutil -o sasl.default.ldap.has_plain_passwords -v 1
```

通过将该值设置为 0，可以禁用这些询问 / 响应 SASL 机制。

注 直到重置或迁移 （请参见 “转换用户的步骤”）用户密码后，现有用户才能使用 APOP、 CRAM-MD5 或 DIGEST-MD5。

请注意， MMP 有一个等效选项：CRAM。

转换用户的步骤

您可以使用 `configutil` 指定有关转换用户的信息。比如，用户密码更改或客户机尝试使用用户不具有正确条目的机制进行验证。

```
configutil -o sasl.default.auto_transition -v value
```

对于其中的值，可以指定以下值之一：

- `no` 或 `0` - 不转换密码。该值为默认值。
- `yes` 或 `1` - 转换密码。

要成功地转换用户，则必须在 Directory Server 中设置 ACI，以允许 Messaging Server 写访问用户密码属性。要完成此操作，请执行以下步骤：

1. 在 “控制台”中，打开您想要配置的 Directory Server。
2. 单击 “目录”选项卡。
3. 选择用户 / 组树的基本后缀。

4. 从 “对象” 菜单中选择 “访问权限”。
5. 选择 （双击）“Messaging Server 最终用户管理员写访问权限” 的 ACI。
6. 单击 “ACI 属性”。
7. 将 `userpassword` 属性添加到现有属性列表中。
8. 单击 “确定”。

`sasl.default.mech_list` 可用于启用 SASL 机制列表。如果非空，则此选项将覆盖 `sasl.default.ldap.has_plain_passwords` 选项以及 `service.imap.allowanonymouslogin` 选项。此选项应用于所有协议 （IMAP、 POP、 SMTP）。

用户密码登录

用户登录到 Messaging Server 以发送或接收邮件时需要提交密码是抵御未授权访问的第一道防线。 Messaging Server 支持对其 IMAP、 POP、 HTTP 和 SMTP 服务的基于密码的登录。

IMAP、 POP 和 HTTP 密码登录

默认情况下，内部用户必须提交密码才能从 Messaging Server 检索用户邮件。您可以单独启用或禁用对 POP、IMAP 和 HTTP 服务的密码登录。有关对 POP、IMAP 和 HTTP 服务进行密码登录的详细信息，请参见第 117 页的 “基于密码的登录”。

用户密码可以以明文或以加密的格式从用户的客户机软件传送到服务器上。如果将客户机和服务器都配置为启用 SSL 并且都支持所需程度的加密 （如第 584 页的 “启用 SSL 并选择加密算法的步骤”中的说明），则进行加密。

用户 ID 和密码都存储在安装的 LDAP 用户目录中。密码安全性标准 （例如最小长度）由目录策略要求确定；这些标准并不是 Messaging Server 管理的一部分。

基于证书的登录是基于密码登录的备用登录。本章讨论了该主题以及 SSL 的其余部分；请参见第 586 页的 “设置基于证书的登录的步骤”。

询问 / 响应 SASL 机制是纯文本密码登录的另一个备用登录。

SMTP 密码登录

默认情况下，用户连接到 Messaging Server 的 SMTP 服务以发送邮件时无需提交密码。但是，您可以启用到 SMTP 的密码登录以便启用经过验证的 SMTP。

经过验证的 *SMTP* 是 SMTP 协议的扩展，它允许客户机验证服务器。此验证附带邮件。经过验证的 SMTP 的主要用途是允许旅行中 （或正在使用主 ISP）的本地用户无需创建其他用户可以滥用的开放中继即可提交邮件 （转发邮件）。客户机使用 "AUTH" 命令可以验证服务器。

有关启用 SMTP 密码登录和因此经过验证的 SMTP 的说明，请参见第 315 页的“SMTP 验证、 SASL 和 TLS”。

您可以使用带 SSL 加密或不带 SSL 加密的经过验证的 SMTP。

配置加密和基于证书的验证

本节包含以下小节：

- 第 580 页的 “通过管理控制台获得证书”
- 第 584 页的 “启用 SSL 并选择加密算法的步骤”
- 第 586 页的 “设置基于证书的登录的步骤”
- 第 587 页的 “如何使用 SMTP 代理服务器优化 SSL 性能”

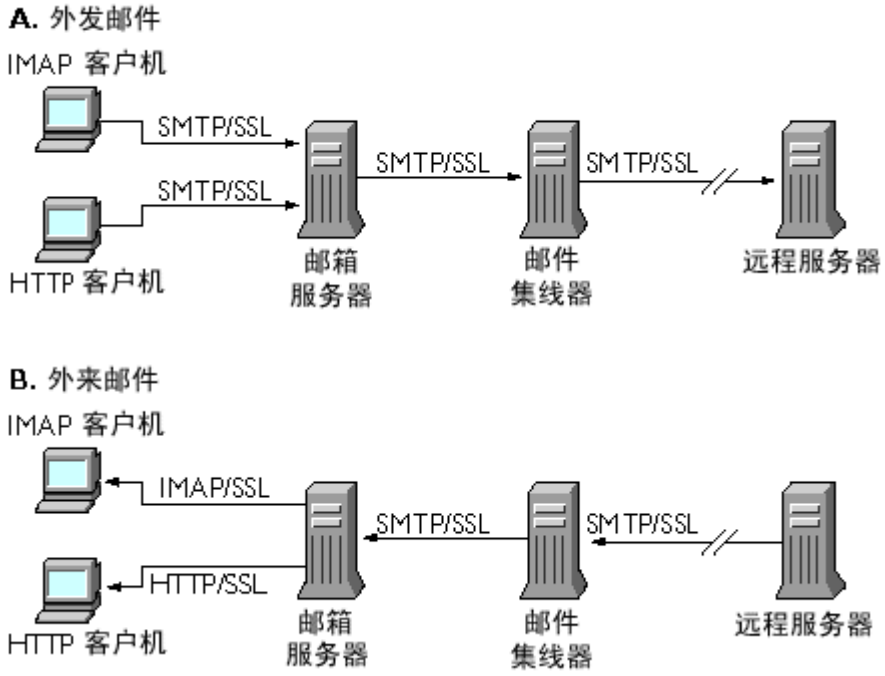
Messaging Server 将传输层安全性 (TLS) 协议 （或称为安全套接字层 [SSL] 协议）用于加密的通信以及用于客户机和服务器的基于证书的验证。 Messaging Server 支持 SSL 版本 3.0 和 3.1。 TLS 与 SSL 完全兼容并包含所有必需的 SSL 功能。

有关 SSL 的背景信息，请参见 "*Introduction to SSL*" （作为 Managing Servers with iPlanet Console 的附录被复制）。 SSL 基于公共密钥密码学的概念，在 **“公共密钥密码学介绍”**中已作了说明 （也作为 Managing Servers with iPlanet Console 的附录被转载）。

如果对 Messaging Server 及其客户机之间以及服务器和其他服务器之间的邮件传送进行加密，则几乎没有机会窃听通信。如果正在连接的客户机已经过验证，则盗窃信息者几乎没有机会冒充 （欺骗）这些客户机。

SSL 起了 IMAP4、HTTP、POP3 和 SMTP 应用层下面的协议层的作用。 SMTP 和 SMTP/SSL 使用同一端口； HTTP 和 HTTP/SSL 要求使用不同的端口； IMAP 和 IMAP/SSL 以及 POP 和 POP/SSL 可以使用同一端口，也可以使用不同的端口。 SSL 在外发和外来邮件的邮件通信的特定阶段进行操作，如图 19-1 中所示。

图 19-1 与 Messaging Server 的加密通信



SSL 提供了逐个加密，但是不能在每个中间服务器上都加密邮件。

注 要启用对外发邮件的加密，则必须将通道定义修改为包含 `tls` 通道关键字，例如 `maytls`、`musttls` 等。有关详细信息，请参见第 *317* 页的 “传输层安全性”和 Messaging Server Reference Manual。

请记住，设置一个 SSL 连接时的附加系统开销可能给服务器带来性能负担。设计邮件传送安装以及分析性能时，您可能需要针对服务器容量来平衡安全需要。

注 因为所有 Sun Java System 服务器都支持 SSL，并且许多服务器上通过控制台来启用和配置 SSL 的界面几乎都相同，所以在 Managing Servers with iPlanet Console 的 SSL 一章中更完整地记录了本节中所述的若干任务。对于那些任务，本章仅给出摘要信息。

通过管理控制台获得证书

无论将 SSL 用于加密还是用于验证，都需要获得服务器证书以用于 Messaging Server。此证书可使您的服务器区别于客户机和其他服务器。如果要通过管理控制台获得证书，请按本节中的步骤执行操作。如果要在命令行模式中创建自签名证书，请参见第 583 页的 “创建自签名证书”。

管理内部模块和外部模块的步骤

服务器证书建立了密钥对的拥有权和有效性，编号则用于加密和解密数据。服务器的证书和密钥对代表了您的服务器的标识。证书和密钥对都存储在证书数据库中，此数据库可以内置于服务器中或位于外部的可移动硬件插卡 （智能卡）上。

Sun Java System 服务器使用遵循公共密钥密码学系统 (PKCS) #11 API 的模块来访问密钥和证书数据库。通常可以从给定硬件设备的供应商那里获得此设备的 PKCS #11 模块，并且必须将此模块安装到 Messaging Server 之后， Messaging Server 才能使用此设备。预先安装的 “Netscape 内部 PKCS # 11 模块”支持使用内置于服务器中的证书数据库的单个内部软件标记。

对证书设置服务器包括为证书创建数据库及其密钥和安装 PKCS #11 模块。如果未使用外部硬件标记，则请在服务器中创建内部数据库并使用作为 Messaging Server 一部分的此内部默认模块。如果使用了外部标记，则请连接硬件智能卡阅读器并安装其 PKCS #11 模块。

您可以通过控制台管理 PKCS #11 模块，无论此模块是内部模块还是外部模块。要安装 PKCS #11 模块，请执行以下操作：

1. 将硬件插卡阅读器连接到 Messaging Server 主机计算机并安装驱动程序。
2. 使用控制台中的 “PKCS #11 管理”界面为已安装的驱动程序安装 PKCS #11 模块。

（有关更完整的说明，请参见 Managing Servers with iPlanet Console 中有关 SSL 的章节。）

安装硬件加密加速器 如果将 SSL 用于加密，则安装硬件加密加速器可能会改进服务器的加密和解密邮件的性能。加密加速器通常由永久地安装在服务器计算机中的硬件板和软件驱动程序组成。 Messaging Server 支持遵循 PKCS #11 API 的加速器模块。（它们是基本的硬件标记，并不存储自己的密钥；而是使用内部数据库来存储。）首次安装由生产商指定的硬件和驱动程序时即安装了加速器，然后通过安装 PKCS #11 模块完成安装 （带有硬件证书标记时）。

请求服务器证书的步骤

在控制台中打开服务器并运行 “证书设置向导”可以请求服务器证书。您可以从 “控制台”菜单或从 “Messaging Server 加密”选项卡访问此向导。使用此向导可以执行以下任务：

1. 生成证书请求。
2. 通过电子邮件将请求发送到要颁发证书的证书授权机构 (CA)。

来自 CA 的电子邮件响应到达后，将此电子邮件保存为文本文件并使用 “证书设置向导”安装此文件。

（有关更完整的说明，请参见 Managing Servers with iPlanet Console 中有关 SSL 的章节。）

安装证书的步骤

安装是一个与请求不同的过程。来自 CA 的响应您的证书请求的电子邮件到达并将其保存为文本文件后，请再次运行 “证书设置向导”以安装作为证书的文件：

1. 指定您已经获得的要安装的证书。
2. 系统提示将证书的文本粘贴到字段中时，执行此操作。
3. 将证书昵称从 `server-cert` 更改为 `Server-Cert`。

   如果您不想更改证书昵称，则可以通过设置 `configutil` 参数 `encryption.rsa.nssslpersonalityssl` 更改系统所需的证书昵称的形式。

（有关更完整的说明，请参见 Managing Servers with iPlanet Console 中有关 SSL 的章节。）

注 这也是安装 CA 证书 （下面将介绍）应遵循的过程，服务器将使用此证书确定是否相信客户机所递交的证书。

安装信任的 CA 证书的步骤

还要使用 “证书设置向导”安装证书授权机构的证书。 CA 证书可验证 CA 自身的标识。您的服务器在验证客户机和其他服务器的过程中使用这些 CA 证书。

例如，如果除了基于密码的验证之外，您将您的企业设置为基于证书的客户机验证（请参见第 157 页中的 “设置基于证书的登录”），则需要安装所有 CA （被信任可以颁发您的客户机可能递交的证书）的 CA 证书。这些 CA 对于您的组织可能是内部 CA 也可能是外部 CA，代表了商业机构或政府机构或其他企业。（有关将 CA 证书用于验证的详细信息，请参见 Managing Servers with iPlanet Console 中的 "*Introduction to Public-Key Cryptography*"。）

安装后， Messaging Server 初始包含了若干商业 CA 的 CA 证书。如果您需要添加其他商业 CA 或者如果您的企业正在开发自己的 CA 用于内部使用 （使用 Sun Java System Certificate Server），则需要获得并安装其他 CA 证书。

注 随 Messaging Server 自动提供的 CA 证书对客户机证书并未初始标记为信任。如果您想要信任由这些 CA 颁发的客户机证书，则需要编辑信任设置。有关说明，请参见第 153 页中的 “管理证书和信任的 CA”。

要请求并安装新的 CA 证书，您需要执行以下操作：

1. 与证书授权机构 （可通过 Web 或电子邮件）联系并下载该机构的 CA 证书。
2. 将已接收的证书文本保存为文本文件。
3. 使用 “证书设置向导”（如前面小节所述）安装此证书。

有关更完整的说明，请参见 Managing Servers with iPlanet Console 中有关 SSL 的章节。

管理证书和信任的 CA

您的服务器可以将信任的 CA 的任何编号的证书用于验证客户机。

通过在控制台中打开您的服务器并在 “控制台”菜单中选择 “证书管理命令”，您可以查看、编辑 Messaging Server 中所安装的证书的信任设置或删除任何证书。有关说明，请参见 Managing Servers with iPlanet Console 中有关 SSL 的章节。

创建密码文件

在所有 Sun Java System 服务器上，当使用 “证书设置向导”请求证书时，向导将创建一个密钥对，并将其存储在内部模块的数据库中或外部数据库 （在智能卡上）中。然后此向导将提示您提供密码，此密码用于加密专用密钥。仅此相同密码以后才可以用于解密密钥。此向导不保留密码也不在任何位置存储此密码。

在大多数为其启用了 SSL 的 Sun Java System 服务器上，在启动时系统都提示管理员提供解密密钥对所需的密码。但是，在 Messaging Server 上，为了缓解必须多次（至少在三个服务器进程中需要）输入密码带来的不便，并方便无人看管的服务器重新启动，可以从密码文件读取密码。

此密码文件被命名为 `sslpassword.conf` 并位于 *msg_svr_base*`/config/` 目录中。文件中的条目是具有以下格式的单独行

`moduleName:password`

其中 *moduleName* 是要使用的内部或外部 PKCS #11 模块的名称， *password* 则是解密此模块的密钥对的密码。此密码以明 （不加密的）文存储。

Messaging Server 提供了默认版本的密码文件，具有以下单个条目 （适用于内部模块和默认密码）：

```
Internal (Software) Token:netscape!
```

如果安装内部认证时指定的不是默认密码，则需要编辑密码文件的上述行以反映您指定的密码。如果安装外部模块，则需要将一个新的行添加到文件中，该行包含模块名称和您为此模块指定的密码。

注意 因为系统未在服务器启动时提示管理员提供模块密码，所以确保管理员控制对服务器的正常访问以及服务器主机及其备份的正常物理安全性是极为重要的。

创建自签名证书

如果要在命令行模式中创建自签名证书，请按照本节中的说明执行操作。要使用证书向导创建证书，请参见第 580 页的 “通过管理控制台获得证书”。

1. 以超级用户身份登录或成为超级用户 (root)。
2. 在 /opt/SUNWmsgsr/config/sslpassword 中为 certutil 指定证书数据库密码。例如：

   ```
   # echo "password" > /opt/SUNWmsgsr/config/sslpassword
   ```

   其中 *password* 是您指定的密码。
3. 移动到 sbin 目录并生成证书数据库 (cert8.db) 和密钥数据库 (key3.db)。例如：

   ```
   # cd /opt/SUNWmsg/sbin
   # ./certutil -N -d /opt/SUNWmsgsr/config -f
   /opt/SUNWmsgsr/config/sslpassword
   ```
4. 生成默认的自签名根证书授权机构证书。示例：

```
# ./certutil -S -n SampleRootCA -x -t "CTu,CTu,CTu"
-s "CN=My Sample Root CA, O=sesta.com" -m 25000
-o /opt/SUNWmsgsr/config/SampleRootCA.crt
-d /opt/SUNWmsgsr/config
-f /opt/SUNWmsgsr/config/sslpassword   -z /etc/passwd
```

5. 为主机生成证书。例如：

```
../certutil -S -n Server-Cert -c SampleRootCA -t "u,u,u"
-s "CN=hostname.sesta.com, o=sesta.com" -m 25001
-o /opt/SUNWmsgsr/config/SampleSSLServer.crt
-d /opt/SUNWmsgsr/config -f /opt/SUNWmsgsr/config/sslpassword
-z /etc/passwd
```

其中 *hostname*.sesta.com 是服务器主机名。

6. 验证证书。例如：

```
# ./certutil -V -u V -n  SampleRootCA -d /opt/SUNWmsgsr/config
# ./certutil -V -u V -n  Server-Cert -d /opt/SUNWmsgsr/config
```

7. 列出证书。例如：

```
# ./certutil -L -d /opt/SUNWmsgsr/config
# ./certutil -L -n Server-Cert -d /opt/SUNWmsgsr/config
```

8. 使用 modutil 列出可用的安全模块 (secmod.db)。例如：

```
# ./modutil -list -dbdir /opt/SUNWmsgsr/config
```

9. 将证书数据库文件的拥有者更改为邮件服务器用户和组，如示例中所示。

```
chown mail:mailserv /opt/SUNWmsgsr/config/cert8.db
chown mail:mailserv /opt/SUNWmsgsr/config/key3.db
```

10. 重新启动邮件传送服务以启用 SSL。

注 以前，证书和密钥文件总是位于 Messaging Server 的配置目录中。现在，可以使用 local.ssldbpath （指定证书和密钥文件的位置）和 local.ssldbprefix （指定证书和密钥文件的前缀）来指定这些文件的位置。

启用 SSL 并选择加密算法的步骤

您可以使用控制台启用 SSL 并选择 Messaging Server 可以在其与客户机的加密通信中使用的加密算法集。

关于加密算法

加密算法是用于在加密进程中加密和解密数据的算法。某些加密算法比其他加密算法强大，这意味着经这些算法保密的邮件更难被未经授权的用户译出。

加密算法通过将密钥 （一个长编号）应用到数据中对数据进行操作。通常，加密过程中加密算法使用的密钥越长，没有正确的解秘密钥来解密数据则越难。

客户机用 Messaging Server 启动 SSL 连接时，客户机会让服务器了解客户机会将何种加密算法和密钥长度用于加密。在所有加密通信中，双方必须使用同一加密算法。因为有很多通用的加密算法和密钥组合，所以，服务器应当能够灵活地支持加密。 Messaging Server 可支持至多 6 种加密算法和密钥长度的组合。

表 6.1 列出了 Messaging Server 支持的可与 SSL 3.0 配合使用的加密算法。此表汇总了可从 Managing Servers with iPlanet Console 中的 "*Introduction to SSL*" 一章中获得的更详细信息。

表 19-2 适用于 Messaging Server 的 SSL 加密算法

加密算法	说明
带有 128 位加密和 MD5 邮件验证的 RC4	最快的加密算法 （通过 RSA 实现）以及强度很高的加密算法和加密密钥的组合。
带有 168 位加密和 SHA 邮件验证的三重 DES	一种较慢的加密算法 （美国政府标准），但却是最强大的加密算法和加密密钥的组合。
带有 56 位加密的 DES 和 SHA 邮件验证	较慢的加密算法 （美国政府标准）以及普通强度的加密算法和加密密钥组合。
带有 40 位加密的 RC4 和 MD5 邮件验证	最快的加密算法 （通过 RSA 实现）和较低强度的加密算法和加密密钥组合。
带有 40 位加密的 RC2 和 MD5 邮件验证	较慢的加密算法 （通过 RSA 实现）和较低强度的加密算法和加密密钥组合。
无加密，只有 MD5 邮件验证	无加密；仅使用用于验证的邮件摘要。

除非您具备不使用某个特定加密算法的令人信服的理由，否则应当支持所有加密算法。但是，请注意出口法律限制在某些国家 / 地区使用某些加密算法。同时，在美国出口控制法放宽之前，所生产的某些客户机软件不能使用较高强度的加密。请注意，虽然 40 位加密算法可以阻止偶尔窃听者，但这些算法并不安全，因此将不会阻止被激发的攻击。

要启用 SSL 并选择加密算法，请遵循以下命令行步骤：

要启用或禁用 SSL：

```
configutil -o nsserversecurity -v [ on | off ]
```

要启用或禁用 RSA 加密算法：

```
configutil -o encryption.rsa.nssslactivation -v [ on | off ]
```

要指定一个标记：

```
configutil -o encryption.rsa.nsssltoken -v tokenname
```

要指定一个证书：

```
configutil -o encryption.rsa.nssslpersonalityssl -v certname
```

请注意，如果启用 RSA 加密算法，还必须指定一个标记和一个证书。

要选择加密算法首选项：

```
configutil -o encryption.nsssl3ciphers -v cipherlist
```

其中 *cipherlist* 是以逗号分隔的加密算法列表。

注 要启用对外发邮件的 SSL 加密，则必须将通道定义修改为包含 `tls` 通道关键字，例如 `maytls`、`musttls` 等。有关详细信息，请参见第 317 页的 “传输层安全性”和 Messaging Server Reference Manual。

设置基于证书的登录的步骤

除了基于密码的验证之外，Sun Java System 服务器还支持通过检查用户的数字证书进行的验证。在基于证书的验证中，客户机建立与服务器之间的 SSL 会话并将用户的证书提交给服务器。然后，服务器将鉴定提交的证书是否真实。如果证书有效，则认为用户经过验证。

要将 Messaging Server 设置为基于证书登录，请执行以下操作：

1. 为您的服务器获取服务器证书。（有关详细信息，请参见第 580 页的 “通过管理控制台获得证书”。）
2. 运行 “证书设置向导”以安装所有信任的证书授权机构的证书，这些证书授权机构将向服务器要验证的用户颁发证书。（有关详细信息，请参见第 581 页的 “安装信任的 CA 证书的步骤”。）

   请注意，只要服务器的数据库中至少要有一个信任的 CA，服务器就会要求每个连接的客户机提供客户机证书。

3. 打开 SSL。（有关详细信息，请参见第 584 页的 “启用 SSL 并选择加密算法的步骤”。）

4. （可选）编辑服务器的 `certmap.conf` 文件以便服务器根据提交的证书中的信息相应搜索 LDAP 用户目录。

   如果用户的证书中的电子邮件地址与用户的目录条目中的电子邮件地址相匹配，则不必编辑 `certmap.conf` 文件，并且无需针对用户条目中的证书优化搜索或验证已提交的证书。

   有关 `certmap.conf` 的格式和可以进行的更改的详细信息，请参见 Managing Servers with iPlanet Console 中的 SSL 一章。

执行这些步骤后，如果客户机建立一个 SSL 会话以便用户可以登录到 IMAP 或 HTTP， Messaging Server 就会要求客户机提供用户证书。如果客户机所提交的证书由服务器建立为信任的 CA 颁发，并且如果证书中的标识与用户目录中的一项相匹配，则用户经过验证并被授予访问权限 （取决于管理该用户的访问控制规则）。

无需禁用基于密码的登录即可启用基于证书的登录。如果允许基于密码的登录 （此为默认状态），并且您已经执行了本节中说明的任务，则同时支持基于密码的和基于证书的登录。在这种情况下，如果客户机建立 SSL 会话并提供证书，则使用基于证书的登录。如果客户机未使用 SSL 或未提供证书，则服务器会要求提供密码。

如何使用 SMTP 代理服务器优化 SSL 性能

由于 SMTP 代理服务器在 SMTP 协议中添加了附加等待时间，大多数站点不应使用 SMTP 代理服务器。但是，对于大量使用 SSL 以保护 SMTP 连接的大规模站点，它可能希望通过对服务器上的所有协议均执行全部 SSL 操作来最大化在 SSL 加速器硬件上的投资，这些操作即 SSL 和代理服务器。邮件队列位于独立的 MTA 计算机上时， SMTP 代理服务器允许前端代理服务器处理 SSL。可以单独配置和购买对每个任务优化硬件的此方法。

有关如何安装 SMTP 代理服务器的说明，请参见第 602 页的 “安装 SMTP 代理的步骤”。

网络安全服务工具

网络安全服务是一组开放源代码库和工具，用于为基于开放标准的 Internet 安全实现和部署应用程序。安全工具可以帮助执行诊断、管理证书、密钥和加密模块，并帮助调试基于 SSL 和 TLS 的应用程序。这些工具位于 `/usr/sfw/bin` 中。

管理证书和密钥

本节介绍的工具可用于存储、检索和保护加密和标识所依赖的密钥和证书。

certutil

证书数据库工具 (certutil) 是命令行实用程序，它可以创建和修改 cert8.db 和 key3.db 数据库文件。密钥和证书管理进程通常以在密钥数据库中创建密钥开始，然后在证书数据库中生成和管理证书。有关 certutil 的更多信息，请访问：

http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html

cmsutil

cmsutil 命令行实用程序使用 S/MIME Toolkit 在 Cryptographic Message Syntax (CMS) 邮件上执行加密和解密等基本操作。此程序执行基本的证书管理操作，例如加密邮件、解密邮件以及为邮件签名。有关 cmsutil 的更多信息，请访问：

http://www.mozilla.org/projects/security/pki/nss/tools/cmsutil.html

modutil

安全模块数据库工具 (modutil) 是用来管理 PKCS #11 模块 （secmod.db 文件）的数据库的命令行实用程序。可以使用该工具添加和删除 PKCS #11 模块、更改密码、设置默认值、列出模块内容、启用或禁用插槽、启用或禁用 FIPS-140-1 规范以及指定加密操作的默认提供者。有关 modutil 的更多信息，请访问：

http://www.mozilla.org/projects/security/pki/nss/tools/modutil.html

pk12util

pk12util 命令行实用程序可以在各自的数据库和文件格式之间导入和导出由 PKCS #12 标准定义的密钥和证书。有关 pk12util 的更多信息，请访问：

http://www.mozilla.org/projects/security/pki/nss/tools/pk12util.html

ssltap

SSL 调试工具 (ssltap) 是识别 SSL 的命令行代理。该工具可代理 SSL 服务器的请求，并显示客户机与服务器之间交换的邮件的内容。它监视 TCP 连接并显示经过的数据。如果连接是 SSL，则显示的信息将包括经过解释的 SSL 记录和握手信息。有关更多信息，请访问：

http://www.mozilla.org/projects/security/pki/nss/tools/ssltap.html

配置管理员对 Messaging Server 的访问

本节大部分与 Sun Java System LDAP Schema v.1 相关。本节包含以下各小节：

- 第 589 页的 “委派的管理的分层结构”
- 第 590 页的 “提供对服务器的整体访问的步骤”
- 第 590 页的 “限制对特定任务的访问权限的步骤”

本节说明了如何控制服务器管理员访问 Messaging Server 的方法。对给定 Messaging Server 和特定 Messaging Server 任务的管理访问发生在委派的服务器管理的环境中。

委派的服务器管理是大多数 Sun Java System 服务器的特性；它是指管理员向其他管理员提供对单个服务器和服务器特性进行有选择地访问的能力。本章简要地汇总了委派的服务器任务。有关更详细的信息，请参见 Managing Servers with iPlanet Console 中有关委派服务器管理的章节。

委派的管理的分层结构

在网络中安装第一个 Sun Java System 服务器时，安装程序将在 LDAP 用户目录中自动创建一个称为配置管理员的组。默认情况下，配置管理员组的成员对网络中的所有主机和服务器具有不受限制的访问权限。

配置管理员组位于访问分层结构的顶层 （例如以下管理员类型），您可以创建配置管理员组以对 Messaging Server 实现委派的管理 （如果使用 Sun Java System LDAP Schema v.1）：

1. **配置管理员**。 Sun Java System 服务器网络的 “超级用户”。具有对所有资源的完全访问权限。
2. **服务器管理员**。域管理员可以创建组以管理每种类型的服务器。例如，可以创建邮件传送管理员组以管理管理域中或整个网络中的所有 Messaging Server。此组成员具有访问该管理域中所有 Messaging Server （但不包括其他服务器）的权限。
3. **任务管理员**。最后，以上任何管理员都可以创建一个组或指派一个单独的用户，该组或该用户具有对单个 Messaging Server 或一组 Messaging Server 的受限访问权限。仅允许此类任务管理员执行特定的、有限的服务器任务 （例如仅启动或停止服务器，或访问给定服务的日志）。

控制台提供了允许管理员执行以下任务的方便的界面：

- 授予一个组或个人对特定 Messaging Server 的访问权限 （如 “提供对服务器的整体访问”中所述 [下一节]）。
- 限制对特定 Messaging Server 中的特定任务的访问 （如第 590 页的 “限制对特定任务的访问权限的步骤”中所述）。

提供对服务器的整体访问的步骤

要授予用户或组访问 Messaging Server 给定实例的权限，请执行以下操作：

1. 以具有您要为其提供的访问 Messaging Server 权限的管理员身份登录到控制台。
2. 在 “控制台”窗口中选择此服务器。

   从 “控制台”菜单中选择 “对象”，然后选择 “设置访问权限”。
3. 添加或编辑对服务器具有访问权限的用户和组的列表。

（有关更完整的说明，请参见 Managing Servers with iPlanet Console 中有关委派服务器管理的章节。）

设置了对特定 Messaging Server 具有访问权限的个人和组的列表后，您即可以使用 ACI （如下节所述）将特定服务器任务委派给此列表上的特定用户或组。

限制对特定任务的访问权限的步骤

通常管理员连接到服务器以执行一项或多项管理任务。通用管理任务列在控制台中的 “Messaging Server 任务”表中。

默认情况下，对特定 Messaging Server 的访问意味着访问其所有任务。但是，任务表中的每项任务都可以有一个附加的访问控制指令 (ACI) 集。服务器在授予已连接用户 （必须已成为对服务器具有整体访问权限的用户）对所有任务的访问权限之前将查阅那些 ACI。实际上，服务器在任务表中仅显示那些用户有权访问的任务。

如果您对 Messaging Server 具有访问权限，则可以在所有任务 （您具有访问权限的所有任务）中创建或编辑 ACI，从而限制其他用户或组对这些任务的访问权限。

要限制已连接用户或组对任务的访问权限，请执行以下操作：

1. 以管理员身份登录到要为其提供限制访问的 Messaging Server 的控制台，该管理员必须具有对此 Messaging Server 的访问权限。

2. 打开服务器并通过在任务文本中单击来选择服务器的任务表中的任务。
3. 从 “编辑” 菜单中选择 “设置访问权限”，并添加或编辑访问规则的列表以授予用户或组您希望其具有的某种访问权限。
4. 根据需要对其他任务重复此过程。

   （有关更完整的说明，请参见 Managing Servers with iPlanet Console 中有关委派服务器管理的章节。）

在 Managing Servers with iPlanet Console 中有关委派服务器管理的章节中更全面地介绍了 ACI 以及如何创建 ACI。

配置客户机对 POP、 IMAP 和 HTTP 服务的访问

本节包含以下小节：

- 第 592 页的 “客户机访问过滤器工作原理”
- 第 592 页的 “过滤器语法”
- 第 597 页的 “过滤器示例”
- 第 599 页的 “为服务创建访问过滤器的步骤”
- 第 600 页的 “为 HTTP 代理验证创建访问过滤器的步骤”

- 第 592 页的 “客户机访问过滤器工作原理”

Messaging Server 支持对其 IMAP、 POP 和 HTTP 服务的基于逐个服务的复杂访问控制，从而，您可以对客户机对服务器的访问权限进行大范围和细分的控制。

如果要为大型企业或 Internet 服务提供商管理邮件传送服务，则这些功能可以帮助您从系统中排除垃圾邮件程序和 DNS 欺骗程序并改进网络的常规安全性。有关对未经请求的大容量电子邮件的特殊控制，请参见第 17 章 “邮件过滤和访问控制”。

注 对于您的企业来说，如果通过 IP 地址控制访问**不是**重大问题，则不必创建本节所述的任何过滤器。如果您只需进行最小访问控制，则有关设置最小访问控制的说明，请参见第 597 页的 “通常允许”一节。

客户机访问过滤器工作原理

Messaging Server 访问控制设备是一种程序，该程序与其服务于的 TCP 守护程序在同一端口上侦听；访问控制设备使用访问过滤器来验证客户机标识，并可授予客户机对此守护程序的访问权限 （如果客户机通过过滤进程）。

作为过滤进程的一部分， Messaging Server TCP 客户机访问控制系统执行 （必要时）套接字端点地址的以下分析：

- 反向查找两个端点的 DNS （以执行基于名称的访问控制）
- 转发两个端点的 DNS 查找 （以检测 DNS 欺骗）
- `Identd` 回叫 （以检查客户端上的用户对于客户机主机是否已知）

系统会将此信息与称为 *filters* 的访问控制语句进行比较以决定是允许还是拒绝访问。对于每种服务，分隔允许过滤器和拒绝过滤器控制访问集。允许过滤器明确允许访问；拒绝过滤器明确禁止访问。

客户机请求访问某项服务时，访问控制系统将使用以下标准按顺序将客户机的地址或名称信息与此项服务的每个过滤器进行比较：

- 搜索将停止在第一个匹配项。因为允许过滤器是在拒绝过滤器之前处理，所以允许过滤器优先。
- 如果客户机信息与此项服务的允许过滤器相匹配，则允许访问。
- 如果客户机信息与此项服务的拒绝过滤器相匹配，则拒绝访问。
- 如果未出现任何与允许或拒绝过滤器匹配的条目，则允许访问 — 只有允许过滤器而没有拒绝过滤器的情况除外，在这种情况下缺少匹配条目意味着拒绝访问。

此处说明的过滤器语法足够灵活，您应该能够以简单而直观的方式实现许多不同种类的访问控制策略。尽管使用几乎排斥的允许或几乎排斥的拒绝可能实现大多数策略，但是还是可以使用允许过滤器和拒绝过滤器的任何组合。

以下各节详细说明了过滤器语法并给出了用法示例。第 599 页的 “为服务创建访问过滤器的步骤”一节介绍了创建访问过滤器的过程。

过滤器语法

过滤器语句包含了服务信息和客户机信息。服务信息可包含服务的名称、主机名和主机地址。客户机信息可包含主机名、主机地址和用户名。服务器信息和客户机信息都可以包含通配符名称或模式。

最简单的过滤器格式是：

service :*hostSpec*

其中 *service* 是服务的名称 （例如 `smtp`、 `pop`、 `imap` 或 `http`），而 *hostSpec* 则是代表客户机请求访问的主机名、 IP 地址或者通配符名称或模式。处理过滤器后，如果客户机查找访问与 *client* 相匹配，则允许还是拒绝 （取决于这是哪种类型的过滤器）对服务的访问由 *service* 来指定。以下是一些示例：

```
imap:roberts.newyork.siroe.com
```

```
pop:ALL
```

```
http:ALL
```

如果是允许过滤器，则第一个语句将授予主机 `roberts.newyork.siroe.com` 对 IMAP 服务的访问权限，而第二个和第三个语句则分别授予所有客户机对 POP 和 HTTP 服务的访问权限。如果是拒绝过滤器，上述语句将拒绝那些客户机对那些服务的访问。（有关通配符名称 [例如 `ALL`] 的说明，请参见第 594 页的 “通配符名称”。）

过滤器中的服务器信息或客户机信息在某种程度上都会比这复杂，在这种情况下过滤器更通用的格式为：

serviceSpec:*clientSpec*

其中 *serviceSpec* 可以是 *service* 或 *service*@*hostSpec*，而 *clientSpec* 可以是 *hostSpec* 或 *user*@*hostSpec*。 *user* 是与客户机主机查找访问相关联的用户名 （或通配符名称）。以下是两个示例：

```
pop@mailServer1.siroe.com:ALL
```

```
imap:srashad@xyz.europe.siroe.com
```

如果是拒绝过滤器，则第一个过滤器拒绝所有客户机访问 `mailServer1.siroe.com` 主机上的 SMTP 服务。第二个过滤器拒绝 `xyz.europe.siroe.com` 主机上的 `srashad` 用户访问 IMAP 服务。（有关何时使用这些扩展的服务器和客户机规范的详细信息，请参见第 596 页的 “服务器主机规范”和第 596 页的 “客户机用户名规范”。）

最后，过滤器具有的最通用的格式为：

serviceList:*clientList*

其中 *serviceList* 由一个或多个 *serviceSpec* 条目组成，而 *clientList* 则由一个或多个 *clientSpec* 条目组成。 *serviceList* 和 *clientList* 内的各个条目以空格和 / 或逗号分隔。

在这种情况下，处理过滤器以后，如果客户机查找访问与 *clientList* 中的任何 *clientSpec* 条目相匹配，则允许或拒绝 （取决于这是哪种类型的过滤器）对所有服务的访问在 *serviceList* 中指定。以下是一个示例：

```
pop, imap, http:.europe.siroe.com .newyork.siroe.com
```

如果是允许过滤器，则将授予 europe.siroe.com 域和 newyork.siroe.com 域任一域中的所有客户机对 POP、 IMAP 和 HTTP 服务的访问权限。有关使用前导点或其他模式来指定域或子网的信息，请参见第 595 页的 “通配符模式”。

您还可以使用以下语法：

“+”或 “-” *serviceList*:*$*next_rule*

+ （允许过滤器）意味着允许客户机列表中的客户机访问守护程序列表服务。

- （拒绝过滤器）意味着拒绝客户机列表中的客户机访问这些服务。

* （通配符过滤器）允许所有客户机使用这些服务。

$ 分隔规则。

以下示例在所有客户机上启用了多项服务。

```
+imap,pop,http:*
```

以下示例显示了多条规则，但每条规则都简化为仅有一个服务名称并将通配符用作客户机列表。（这是在 LDIF 文件中指定访问控制的最通用的方法。）

```
+imap:ALL$+pop:ALL$+http:ALL
```

以下是一个如何对某个用户禁止所有服务的示例：

```
-imap:*$-pop:*$-http:*
```

通配符名称

可以使用以下通配符名称来代表服务名称、主机名或地址或者用户名：

表 19-3 服务过滤器的通配符名称

通配符名称	解释
ALL, *	通用通配符。匹配所有名称。
LOCAL	与所有本地主机 （其名称不包含点字符的主机）相匹配。但是，如果您的安装仅使用规范名称，即使本地主机名将包含点，因而也不会与此通配符相匹配。
UNKNOWN	与名称未知的所有用户或与名称或地址未知的所有主机相匹配。 请小心使用此通配符名称： 由于临时 DNS 服务器问题，主机名可能不可用 — 在这种情况下，使用 UNKNOWN 的所有过滤器将与所有客户机主机都匹配。 软件无法标识与之通信的网络的类型时，网络地址不可用 — 在这种情况下，使用 UNKNOWN 的所有过滤器将与此网络中的所有客户机主机都匹配。

表 19-3 服务过滤器的通配符名称

通配符名称	解释
KNOWN	匹配用户名称已知的所有用户，或匹配主机名称和地址已知的所有主机。 请小心使用此通配符名称： 由于临时 DNS 服务器问题，主机名可能不可用 — 在这种情况下，使用 KNOWN 的所有过滤器都将不适用于所有客户机主机。 软件无法标识与之通信的网络的类型时，网络地址不可用 — 在这种情况下，使用 KNOWN 的所有过滤器都将不适用于此网络中的所有客户机主机。
DNSSPOOFER	与其 DNS 名称不匹配自身 IP 地址的所有主机相匹配。

通配符模式

可以在服务或客户机地址中使用以下模式：

- 以点字符 (.) 开头的字符串。如果主机名的最后组成部分与指定的模式相匹配，则主机名是匹配的。例如，通配符模式 `.siroe.com` 与 `siroe.com` 域中的所有主机都匹配。
- 以点字符 (.) 结尾的字符串。如果主机地址的首批数字字段与指定的模式相匹配，则主机地址是匹配的。例如，通配符模式 `123.45.` 与 `123.45.0.0` 子网中的所有主机的地址都匹配。
- `n.n.n.n/m.m.m.m` 格式的字符串。此通配符模式被解释为一个 *net/mask* 对。如果 *net* 与地址的按位 AND 和 *mask* 相等，则主机地址是匹配的。例如，模式 `123.45.67.0/255.255.255.128` 与范围在 `123.45.67.0` 到 `123.45.67.127` 之间的所有地址都匹配。

EXCEPT 运算符

访问控制系统支持单运算符。在 *serviceList* 或 *clientList* 中有多个条目时，可以使用 EXCEPT 运算符来创建匹配名称或模式的异常情况。例如，以下表达式：

list1 EXCEPT *list2*

表示与 *list1* 相匹配的任何内容都匹配，**除此之外**它还与 *list2* 相匹配。

以下是一个示例：

```
ALL:ALL EXCEPT isserver.siroe.com
```

如果是拒绝过滤器，则除了 `isserver.siroe.com` 主机上的客户机之外，将拒绝所有客户机对所有服务的访问。

可以嵌套 EXCEPT 子句。以下表达式：

list1 EXCEPT *list2* EXCEPT *list3*

被鉴定假设其等价为：

list1 EXCEPT (*list2* EXCEPT *list3*)

服务器主机规范

通过将服务器主机名或地址信息包含在 *serviceSpec* 条目中，您可以进一步标识过滤器中所请求的特定服务。在这种情况下，此条目的格式为：

service@hostSpec

为带有不同 Internet 主机名的多个 Internet 地址设置 Messaging Server 主机计算机时，您可能希望使用此功能。如果您是服务提供商，就可以使用此设备在单个服务器实例中控制具有不同访问控制规则的多个域。

客户机用户名规范

对于支持 RFC 1413 中所述的 identd 服务的客户机主机，您可以通过在过滤器的 *clientSpec* 条目中包含客户机的用户名来进一步标识请求服务的特定客户机。在这种情况下，此条目的格式为：

user@hostSpec

其中 *user* 是由客户机的 identd 服务返回的用户名 （或通配符名称）。

在过滤器中指定客户机用户名会很有用，但请记住以下警告：

- identd 服务未经验证；如果客户机系统已损坏，则不能信任此服务返回的客户机用户名。总的来说，请不要使用具体的用户名；仅使用通配符名称 ALL、KNOWN 或 UNKNOWN。
- 大多数现代客户机计算机都不支持 identd，因此很少在现代部署中提供附加值。我们正考虑在将来的版本中删除 identd 支持，所以如果此功能对您站点有价值，请通知 Sun Java System。
- 用户名查找需要花费时间；对所有用户执行查找可能减慢由不支持 identd 的客户机进行的访问。有选择的用户名查找可以缓解此问题。例如，如下规则：

  serviceList:@xyzcorp.com ALL@ALL

  将匹配 xyzcorp.com 域中的用户而不执行用户名查找，但它将对所有其他系统执行用户名查找。

用户名查找功能在某些情况下可以帮助您防止来自客户机的主机上未经验证用户的攻击。这可以在某些 TCP/IP 中实现，例如，对于盗窃信息者使用 rsh（远程 Shell 服务）来冒充信任的客户机主机，如果客户机主机支持 ident 服务，则可以使用用户名查找来检测这样的攻击。

过滤器示例

本节中的示例显示了控制访问的各种方法。研究这些示例时，请记住允许过滤器在拒绝过滤器之前处理，找到匹配项时搜索即终止，并且找不到任何匹配项时将授权访问。

此处列出的示例使用主机名和域名而不使用 IP 地址。请记住，可以在过滤器中包含地址和网络掩码信息，在名称服务失败时，此过滤器可以改进可靠性。

通常拒绝

在这种情况下，访问都被默认的拒绝。仅允许明确经过验证的主机访问。

默认策略 （无访问）可通过单个普通拒绝文件实现：

```
ALL:ALL
```

此过滤器拒绝允许过滤器没有明显授权的所有客户机访问所有服务。然后，允许过滤器可能类似于以下模式：

```
ALL:LOCAL @netgroup1

ALL:.siroe.com EXCEPT externalserver.siroe.com
```

第一个规则允许来自本地域 （即，主机名中不包含点的所有主机）中的所有主机和来自 `netgroup1` 组的成员的访问。第二个规则使用前导点通配符模式允许来自 `siroe.com` 域的除 `externalserver.siroe.com` 主机之外的所有主机的访问。

通常允许

在这种情况下，访问都被默认的授权。仅拒绝明显指定的主机的访问。

默认策略 （已授权访问）使允许过滤器不必使用。在拒绝过滤器中明显列出的不需要的客户机的示例如下：

```
ALL:externalserver.siroe1.com, .siroe.asia.com

ALL EXCEPT pop:contractor.siroe1.com, .siroe.com
```

第一个过滤器对特殊主机和特定域拒绝所有服务。第二个过滤器仅允许来自特殊主机和特定域的 POP 的访问。

拒绝对被欺骗的域的访问

可以在过滤器中使用 DNSSPOOFER 通配符名称以检测主机名欺骗。指定 DNSSPOOFER 时，访问控制系统执行 DNS 的正向或反向查找以验证客户机所提供的主机名与其实际 IP 地址是否匹配。以下是一个拒绝过滤器的示例：

```
ALL:DNSSPOOFER
```

此过滤器对主机的 IP 地址与其 DNS 主机名不匹配的所有远程主机拒绝所有服务。

控制对虚拟域的访问

如果邮件传送安装使用虚拟域，其中单个服务器实例与多个 IP 地址和多个域名相关联，则您可以通过使用允许过滤器和拒绝过滤器的组合来控制对每个虚拟域的访问。例如，您可以将类似于以下模式的允许过滤器：

```
ALL@msgServer.siroe1.com:@.siroe1.com

ALL@msgServer.siroe2.com:@.siroe2.com

...
```

与类似于以下模式的拒绝过滤器配合使用：

```
ALL:ALL
```

每个允许过滤器仅允许 domain*N* 中的主机连接到其 IP 地址对应于 msgServer.siroe*N*.com 的服务。所有其他连接都被拒绝。

为服务创建访问过滤器的步骤

可以为 IMAP、POP 或 HTTP 服务创建允许过滤器和拒绝过滤器。还可以为 SMTP 服务创建这些过滤器，但这些过滤器几乎没有价值，因为它们仅应用到经过验证的 SMTP 会话中。有关如何控制对未经过验证的 SMTP 会话的访问的信息，请参见第 17 章 “邮件过滤和访问控制”。

Console 要使用控制台创建过滤器，请执行以下步骤：

1. 在 “控制台”中，打开您想要为其创建访问过滤器的 Messaging Server。
2. 单击 “配置”选项卡。
3. 在左窗格中打开 “服务”文件夹并选择 “服务”文件夹下的 “IMAP”、“POP”或 “HTTP”。
4. 在右窗格中单击 “访问”选项卡。

   此选项卡中的 “允许”和 “拒绝”字段显示了用于此服务的现有允许过滤器和访问过滤器。字段中的每行都代表了一个过滤器。对于其中任何一个字段，都可以指定以下操作：

   a. 单击 “添加”以创建新过滤器。系统将打开一个 “允许过滤器”窗口或 “拒绝过滤器”窗口；将新过滤器的文本输入到此窗口中，然后单击 “确定”。

   b. 选择一个过滤器并单击 “编辑”以修改此过滤器。系统将打开一个 “允许过滤器”窗口或 “拒绝过滤器”窗口；编辑此窗口中显示的过滤器文本，然后单击 “确定”。

   c. 选择一个过滤器并单击 “删除”以删除此过滤器。

请注意，如果需要重新安排允许过滤器或拒绝过滤器的顺序，则可以通过执行一系列删除和添加操作来完成此操作。

有关过滤器语法规范和各种示例，请参见第 592 页的 “过滤器语法”。有关其他示例，请参见第 597 页的 “过滤器示例”。

命令行 您还可以通过如下命令行指定访问和拒绝过滤器：

要创建或编辑服务的访问过滤器：

```
configutil -o service.service.domainallowed -v filter
```

其中 *service* 为 `pop`、 `imap` 或 `http`，而 *filter* 遵循第 592 页的 “过滤器语法”中所述的语法规则。

要创建或编辑服务的拒绝过滤器：

```
configutil -o service.service.domainnotallowed -v filter
```

其中 *service* 为 `pop`、 `imap` 或 `http`，而 *filter* 遵循第 592 页的 “过滤器语法”中所述的语法规则。

为 HTTP 代理验证创建访问过滤器的步骤

任何存储管理员都可以代理验证任何服务。（有关存储管理员的详细信息，请参见第 497 页的 “指定管理员对存储的访问权限”。）仅对于 HTTP 服务，如果任何用户的客户机主机都已授权通过代理验证访问过滤器进行访问，则用户可以代理验证服务。

代理验证允许其他服务 （例如一个门户站点）验证用户并将验证证书传递给 HTTP 登录服务。例如，假设一个门户站点提供若干服务，其中之一是 Messenger Express 基于 Web 的电子邮件。通过使用 HTTP 代理验证功能，最终用户仅需要对门户服务进行一次验证；而无需在访问其电子邮件时再次验证。门户站点必须配置作为客户机和服务之间界面的登录服务器。为帮助配置登录服务器以验证 Messenger Express， Sun Java System 提供了一个适用于 Messenger Express 的验证 SDK。

本节说明了如何通过 IP 地址创建允许过滤器以允许 HTTP 代理验证。本节未说明如何设置登录服务器或如何使用 Messenger Express 验证 SDK。有关为 Messenger Express 设置登录服务器和使用验证 SDK 的详细信息，请与您的 Sun Java System 代表联系。

Console 要为 HTTP 服务的代理验证创建访问过滤器，请：

1. 在 “控制台”中，打开您想要为其创建访问过滤器的 Messaging Server。
2. 单击 “配置”选项卡。
3. 在左窗格中打开 “服务”文件夹并选择 “服务”文件夹下的 “HTTP”。
4. 在右窗格中单击 “代理”选项卡。

   此选项卡中的 “允许”字段显示了用于代理验证的现有允许过滤器。
5. 要创建新过滤器，请单击 “添加”。

   系统打开一个 “允许过滤器”窗口。将新过滤器的文本输入到窗口中并单击 “确定”。

6. 要编辑一个现有过滤器，请选择此过滤器并单击 “编辑”。

   系统打开一个 “允许过滤器”窗口。编辑窗口中显示的过滤器文本，然后单击 “确定”。

7. 要删除一个现有过滤器，请从 “允许”字段中选择一个字段，然后单击 “删除”。

8. 完成对 “代理”选项卡所作的更改后，请单击 “保存”。

有关允许过滤器语法的详细信息，请参见第 592 页的 “过滤器语法”。

命令行 您还可以通过如下命令行为 HTTP 服务的代理验证指定访问过滤器：

```
configutil -o service.service.proxydomainallowed -v filter
```

其中 *filter* 遵循第 592 页的 “过滤器语法”中所述的语法规则。

启用 POP Before SMTP

SMTP 验证或 *SMTP Auth* (RFC 2554) 是提供 SMTP 中继服务器安全性的首选方法。SMTP Auth allows only authenticated users to send mail through the MTA. 但是，某些传统客户机仅提供对 *POP before SMTP* 的支持。如果您的系统中出现此情况，您可以按如下所述启用 POP before SMTP。但是，如果可能，请支持您的用户升级 POP 客户机而不是使用 POP before SMTP。在站点中部署了 POP before SMTP 后，用户将依赖于无法遵循 Internet 安全标准的客户机，并使最终用户更容易攻击您的站点和减慢您的站点速度而造成不可避免的性能损耗，因为必须跟踪并整理最近成功的 POP 会话的 IP 地址。

Messaging Server 实现 POP before SMTP 与 SIMS 或 Netscape Messaging Server 是完全不同的。将 Messaging Multiplexor (MMP) 配置为具有 POP 和 SMTP 代理才能支持 POP before SMTP。 SMTP 客户机连接到 SMTP 代理后，此代理将检查最近 POP 验证的内存中高速缓存。如果找到来自同一客户机 IP 地址的 POP 验证，则 SMTP 代理将通知 SMTP 服务器应当允许邮件指向本地和非本地收件人。

安装 SMTP 代理的步骤

1. 安装 Messsaging Multiplexor (MMP) （如 Sun Java Enterprise System Installation Guide 中所述）。
2. 在 MMP 上启用 SMTP 代理。

   将字符串：

   msg_svr_base/lib/SmtpProxyAService@25|587

   添加到 *msg_svr_base*/config/AService.cfg 文件的 ServiceList 选项中。该选项是一个长行并且不能包含换行。

注 升级 MMP 后，将生成对应于 MMP 的四个现有配置文件的四个新文件。 The new files are:

AService-def.cfg、 ImapProxyAService-def.cfg、 PopProxyAService-def.cfg 和 SmtpProxyAService-def.cfg

这些文件是由安装程序创建的，文档中说明的四个配置文件并非由安装过程创建或受其影响。启动 MMP 后，它将查找标准配置文件（如当前所记录的）。如果未查找到标准配置文件，则 MMP 将尝试复制具有相应 *AService.cfg 文件名的各个 *AService-def.cfg 文件。

3. 在每个 SMTP 中继服务器上的 SMTP 通道选项文件 tcp_local_option 中设置 PROXY_PASSWORD 选项。

   SMTP 代理连接到 SMTP 服务器后，此代理必须通知 SMTP 服务器真实的客户机 IP 地址和其他连接信息，以便 SMTP 服务器可以正常应用中继阻塞和其他安全策略 （包括 POP before SMTP 验证）。此为安全敏感操作并且必须经过验证。在 MMP SMTP 代理和 SMTP 服务器上都配置了代理密码，可以确保第三方无法滥用此设备。

   示例：PROXY_PASSWORD=*A_Password*

4. 确保 MMP 用于连接到 SMTP 服务器的 IP 地址没有被 INTERNAL_IP 映射表视为“内部地址”。

   有关 INTERNAL_IP 映射表的信息，请参见第 17 章 “邮件过滤和访问控制”的第 470 页的 “添加 SMTP 中继”。

5. 将 SMTP 代理配置为支持 POP before SMTP。

   a. 编辑 *msg_svr_base*/config/SmtpProxyAService.cfg 配置文件。

      以下 SMTP 代理选项与 IMAP 和 POP 代理的相同选项在操作方面是相同的（请参见第 143 页的第 7 章 “配置和管理多路复用器服务”和 Sun Java System Messaging Server Administration Reference [http://docs.sun.com/doc/819-0106] 的 "Encryption (SSL) Option" 部分中有关这些选项的描述）。

      LdapURL、 LogDir、 LogLevel、 BindDN、 BindPass、 Timeout、 Banner、 SSLEnable、 SSLSecmodFile、 SSLCertFile、 SSLKeyFile、 SSLKeyPasswdFile、 SSLCipherSpecs、 SSLCertNicknames、 SSLCacheDir、 SSLPorts、 CertMapFile、 CertmapDN、 ConnLimits、 TCPAccess

      以上未列出的其他 MMP 选项 （包含 BacksidePort 选项）目前没有应用到 SMTP 代理中。

      添加以下五个选项：

      SmtpRelays 是要用于循环中继的 SMTP 中继服务器主机名 （带有可选端口）的以空格分隔的列表。这些中继必须支持 XPROXYEHLO 扩展。此选项不必有默认设置。**示例：** default:SmtpRelays manatee:485 gonzo mothra

      SmtpProxyPassword 是用于授权在 SMTP 中继服务器上更改源通道的密码。此选项不必有默认设置并且必须与 SMTP 服务器上的 PROXY_PASSWORD 选项相匹配。
      例如： default:SmtpProxyPassword *A_Password*

      除了默认关键字集外， EhloKeywords 选项还为代理提供了可以传递给客户机的 EHLO 扩展关键字列表。 MMP 将从 SMTP 中继所返回的 EHLO 列表中删除所有无法识别的 EHLO 关键字。 EhloKeywords 指定了不应从列表中删除的其他 EHLO 关键字。默认设置为空，但是 SMTP 代理将支持以下关键字，所以无需在此选项中将其列出：8BITMIME、 PIPELINING、 DSN、 ENHANCEDSTATUSCODES、 EXPN、 HELP、 XLOOP、 ETRN、 SIZE、 STARTTLS、 AUTH

      以下是一个可由很少使用 "TURN" 扩展的站点使用的示例：
      示例： default:EhloKeywords TURN

      将 PopBeforeSmtpKludgeChannel 选项设置为 MTA 通道的名称以用于 POP before SMTP 经授权的连接。默认设置为空，对于希望启用 POP before SMTP 的用户，其典型设置是 tcp_intranet。优化 SSL 性能时无需使用此选项 （请参见第 587 页的 “如何使用 SMTP 代理服务器优化 SSL 性能”）。
      示例： default:PopBeforeSmtpKludgeChannel tcp_intranet

ClientLookup 选项默认设置为 no。如果设置为 yes，则系统将无条件地执行对客户机 IP 地址的 DNS 反向查找，因此 SMTP 中继服务器不必做此项工作，可以在每个托管的域基础上设置该选项。
例如： `default:ClientLookup  yes`

b. 在 PopProxyAService.cfg 配置文件中设置 PreAuth 选项和 AuthServiceTTL 选项。优化 SSL 性能时不需要此选项。（请参见第 587 页的“如何使用 SMTP 代理服务器优化 SSL 性能”。）

注 为了使 POP before SMTP 能够运行，**不能**在 IMAP 或 SMTP 代理配置文件中设置 AuthServiceTTL。

这些选项指定了用户经授权在 POP 验证后多少秒之内提交邮件。典型设置是 900 至 1800 秒 （15 至 30 分钟）。

示例：

```
default:PreAuth     yes
default:AuthServiceTTL     900
```

c. 您可以根据需要指定在尝试列表中的下一个中继之前，MMP 将等待 SMTP 中继响应的秒数。

默认设置是 10 （秒）。如果到 SMTP 中继的连接失败， MMP 将避免尝试此中继的分钟数等于故障切换超时时间 （因此如果故障切换超时时间是 10 秒，并且中继失败，则在 10 分钟之内 MMP 将不会再次尝试此中继）。
例如：`default:FailoverTimeout  10`

配置客户机对 SMTP 服务的访问

有关配置客户机对 SMTP 服务的访问的信息，请参见第 17 章 “邮件过滤和访问控制”。

基于 SSL 的用户 / 组目录查找

对于 MTA、MMP 和 IMAP/POP/HTTP 服务，可能会基于 SSL 进行用户 / 组目录查找。前提是必须在 SSL 模式下配置 Messaging Server。设置以下 configutil 参数来启用此功能：local.service.pab.ldapport 设为 636， local.ugldapport 设为 636，local.ugldapusessl 设为 1。

第 20 章

管理 Communications Express Mail 的 S/MIME

可以在 Sun Java System Communications Express Mail 上使用安全 / 通用 Internet 邮件扩展服务 (S/MIME)。已设置为使用 S/MIME 的 Communications Express Mail 用户可以与 Communications Express Mail、 Microsoft Outlook Express 和 Mozilla 邮件系统的其他用户交换签名邮件或加密邮件。

您可以在联机帮助中找到有关在 Communications Express Mail 中使用 S/MIME 的信息。本章说明了管理 S/MIME 的信息。本章由以下各节组成：

- 第 606 页的 “什么是 S/MIME？”
- 第 607 页的 “必需的软件和硬件组件”
- 第 608 页的 “使用 S/MIME 的要求”
- 第 610 页的 “安装 Messaging Server 后开始使用”
- 第 617 页的 “smime.conf 文件的参数”
- 第 623 页的 “Messaging Server 选项”
- 第 624 页的 “使用 SSL 确保 Internet 链路的安全”
- 第 626 页的 “客户机的密钥访问库”
- 第 628 页的 “验证专用密钥和公共密钥”
- 第 634 页的 “授予使用 S/MIME 功能的权限”
- 第 635 页的 “管理证书”
- 第 639 页的 “Communications Express S/MIME 最终用户信息”

什么是 S/MIME?

S/MIME 为 Communications Express Mail 用户提供以下功能：

- 为外发邮件创建数字签名，以确保邮件接收人收到的邮件未被篡改而且是来自发件人
- 对外发邮件进行加密，以防止邮件在到达收件人的邮箱之前被他人查看、更改或以任何方式使用邮件内容
- 使用包含证书撤销列表 (CRL) 的进程来验证收到的签名邮件的数字签名
- 自动对收到的加密邮件进行解密，以便收件人能够阅读邮件内容
- 与 S/MIME 兼容客户机 （例如 Communications Express Mail 和 Mozilla 邮件系统）的其他用户交换签名邮件或加密邮件

用户需要了解的概念

要正确管理 S/MIME，您需要熟悉以下概念：

- 平台的基本管理步骤
- 轻量目录访问协议 (LDAP) 目录的结构和用法
- 在 LDAP 目录中添加或修改条目
- Sun Java System Directory Server 的配置过程
- 以下各项的概念和用途：
  - 安全通信线路的安全套接字层 (SSL)
  - 数字签名电子邮件
  - 加密电子邮件
  - 浏览器的本地密钥库
  - 智能卡及使用智能卡必需的软件和硬件
  - 专用 — 公共密钥对及其证书
  - 证书授权机构 (CA)
  - 验证密钥及其证书
  - 证书撤销列表 (CRL)。（有关 CRL 的介绍，请参见第 629 页的 “何时根据 CRL 检查证书？”。）

必需的软件和硬件组件

本节说明了将 Communications Express Mail 与 S/MIME 结合使用必需的硬件和软件。尝试针对 S/MIME 进行配置之前，请确保已在服务器和客户机上安装了所有正确版本的软件。

表 20-1 列出了在其中访问 Communications Express Mail 的客户机必需的软件和硬件。

表 20-1 客户机必需的硬件和软件

组件	说明
操作系统	• Microsoft Windows 98, 2000 或 XP
浏览器	• Windows 上的 Microsoft Internet Explorer，版本 6 SP2 • Windows 2000 和 Windows 98 上的 Microsoft Internet Explorer，版本 6 SP1（具有 2004 年 12 月 1 日发布的最新修补程序）
Sun 软件	Sun Java 2 Runtime Environment, Standard Edition, 版本 1.4.2_03 或更高版本，但不能是 1.5 版
具有证书的专用 - 公共密钥	一个或多个具有证书的专用 - 公共密钥对。需要使用证书，而且证书必须为标准的 X.509 v3 格式。从 CA 为将要使用 S/MIME 功能的每个 Communications Express Mail 用户获取密钥和证书。密钥及其证书存储在客户机或智能卡中。公共密钥和证书还存储在 Directory Server 可以访问的 LDAP 目录中。 如果要根据证书撤销列表 (CRL) 检查密钥证书以进一步确保密钥是有效的，则由 CA 维护的证书撤销列表必须是系统的一部分。请参见第 629 页的 “何时根据 CRL 检查证书？”。
智能卡软件 （仅当密钥和证书存储在智能卡中时才需要）	• ActivCard Gold，版本 2.1 或 3.0，或 • NetSign，版本 3.1
智能卡阅读器	客户机和智能卡软件支持的任何型号的智能卡阅读设备。

表 20-2 列出了服务器必需的 Sun Microsystems 软件。

表 20-2 服务器必需的软件

Sun 组件	说明
邮件服务器	针对 Solaris 版本 8 或 9 以及 Sun SPARC 计算机发行的 Sun Java System Messaging Server 6 2005Q1
LDAP 服务器	Sun Java System Directory Server 5 2004Q2 或更高版本
Java	Java 2 Runtime Environment， Standard Edition，版本 1.4.2 或更高版本
Access Manager	（如果是在模式 2 下进行部署）— Sun Java System Access Manager 6 2005Q1 和 Communications Express — Sun Java System Communications Express 6 2005Q1

使用 S/MIME 的要求

安装 Messaging Server 后， Communications Express Mail 用户并不能立即使用签名和加密功能。用户必须满足本节所说明的要求才能使用 S/MIME。

专用密钥和公共密钥

必须为将要使用 S/MIME 的每个 Communications Express Mail 用户至少发布一个包括标准 X.509 v3 格式证书的专用和公共密钥对。验证过程所使用的证书可以向其他邮件用户保证密钥确实属于使用密钥的用户。用户可以拥有多个密钥对及相关证书。

密钥及其证书可以由您的组织发布，也可以从第三方供应商处购买。无论密钥和证书是如何发布的，发布组织均被称为证书授权机构 (CA)。

密钥对及其证书以两种方式进行存储：

- 存储在称为智能卡的通用访问卡 (CAC) 中

  这些卡与商业信用卡相似，邮件用户应像使用和保护自己的信用卡那样使用和保护智能卡。智能卡需要使用连接至邮件用户计算机 （客户机）的特殊读卡器才能阅读专用密钥信息。有关更多信息，请参见第 608 页的 “存储在智能卡中的密钥”。

- 存储在邮件用户计算机 （客户机）的本地密钥库中

  邮件用户的浏览器提供密钥库。该浏览器还提供将密钥对和证书下载到密钥库的命令。有关更多信息，请参见第 609 页的 “存储在客户机中的密钥”。

存储在智能卡中的密钥

如果专用 — 公共密钥对及其证书存储在智能卡中，则必须将读卡器正确连接至邮件用户的计算机。读卡设备也需要软件；读卡设备及其软件由出售该设备的供应商提供。

正确安装读卡设备后，如果邮件用户要为外发邮件创建数字签名，则需要将智能卡插入读卡设备中。验证完智能卡密码后， Communications Express Mail 就可以使用专用密钥来对邮件进行签名了。有关支持的智能卡和读卡设备的信息，请参见第 607 页的 “必需的软件和硬件组件”。

用户计算机上应具有来自智能卡供应商的库。有关更多信息，请参见第 626 页的 “客户机的密钥访问库”。

存储在客户机中的密钥

如果未将密钥对和证书存储在智能卡中，则必须将它们保存在邮件用户计算机（客户机）的本地密钥库中。邮件用户计算机的浏览器提供密钥库并提供将密钥对和证书下载到密钥库的命令。密钥库可能受密码保护，这取决于浏览器。

用户计算机上应具有来自浏览器供应商的库以支持本地密钥库。有关更多信息，请参见第 626 页的 “客户机的密钥访问库”。

在 LDAP 目录中发布公共密钥

还必须将所有公共密钥和证书存储到 LDAP 目录中，以便于 Sun Java System Directory Server 访问。这也称为发布公共密钥，从而使其他正在创建 S/MIME 邮件的邮件用户可以使用这些公共密钥。

发件人和收件人的公共密钥用于加密邮件的加密 — 解密过程。公共密钥证书用于验证数字签名所使用的专用密钥。

有关使用 `ldapmodify` 来发布公共密钥和证书的更多信息，请参见第 635 页的 “管理证书”。

授予邮件用户使用 S/MIME 的权限

要创建签名或加密邮件，有效的 Communications Express Mail 用户必须具有相应的权限。这涉及到使用用户的 LDAP 条目的 `mailAllowedServiceAccess` 或 `mailDomainAllowedServiceAccess` LDAP 属性。可以使用这些属性以个人或域为基础允许或不允许邮件用户使用 S/MIME。

有关更多信息，请参见第 634 页的 “授予使用 S/MIME 功能的权限”。

多语言支持

只使用英语作为邮件语言的 Communications Express Mail 用户可能无法阅读包含非拉丁语言字符（例如中文）的 S/MIME 邮件。出现这种情况的原因之一是：安装在用户计算机上的 Java 2 Runtime Environment (JRE) 的 `/lib` 目录中没有 `charsets.jar` 文件。

如果使用默认的 JRE 安装过程下载了英语版本的 JRE，则不会安装 `charsets.jar` 文件。但是，其他语言版本的默认安装过程都会安装 `charsets.jar`。

要确保在 /lib 目录中安装 charsets.jar 文件，请提醒用户使用自定义安装来安装英语版本的 JRE。在安装过程中，用户必须选择 “支持其他语言” 选项。

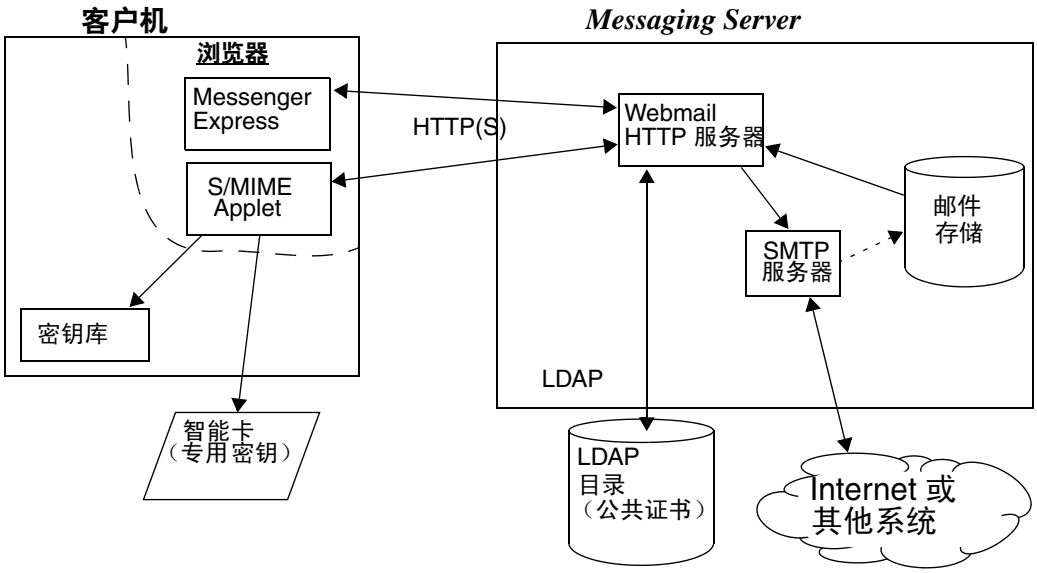
安装 Messaging Server 后开始使用

本节说明了什么是 S/MIME applet，并提供了为 Communications Express Mail 设置 S/MIME 的基本配置过程。该配置过程包括设置 S/MIME applet 的参数及 Messaging Server 的选项。

S/MIME Applet

对邮件进行签名、加密或解密的过程以及验证专用和公共密钥的各个步骤都由一个特殊的 applet 来处理，该 applet 称为 S/MIME applet。可以通过 smime.conf 文件中的参数和 Messaging Server 选项来配置 S/MIME 功能。图 20-1 显示了 S/MIME Applet 与其他系统组件的关系。

图 20-1 S/MIME Applet



首次登录

具有使用 S/MIME 权限的 Communications Express Mail 用户首次登录到 Messaging Server 时，系统将显示有关 S/MIME applet 的一系列特定提示。用“是”或“始终”回答完提示问题后， S/MIME applet 即被下载到计算机中。此 applet 将始终保留在计算机中，直至注销 Communications Express Mail。

有关更多信息，请参阅第 635 页的 “管理证书”。

下载 S/MIME Applet

用户每次登录到 Communications Express Mail 时都将下载 S/MIME applet，除非在用户计算机上为 Java 2 Runtime Environment (JRE) 启用了高速缓存。启用高速缓存后， S/MIME applet 的副本会在首次下载之后保存在用户计算机上，这样，用户就不必在每次登录时都下载此 applet。

高速缓存可以提高性能，因此您可以指导用户执行以下步骤来为 Java 2 Runtime Environment 版本 1.4.*x* 启用高速缓存：

1. 转至 Windows 控制面板。
2. 双击 “Java Plug-in” 图标 (Java 2 Runtime Environment)。
3. 单击 “高速缓存” 选项卡。
4. 选中 “启用高速缓存” 复选框。
5. 单击 “应用”。

下载之后，用户不会感觉到 S/MIME applet 的存在。而看起来似乎是 Communications Express Mail 在对邮件进行签名、加密或解密。如果不弹出错误消息，用户也感觉不到验证专用或公共密钥的过程。有关更多信息，请参阅第 628 页的 “验证专用密钥和公共密钥”。

基本的 S/MIME 配置

S/MIME 的配置文件 `smime.conf` 包含每个 S/MIME 参数的描述性注释和一个示例。 Messaging Server 附带有 `smime.conf` 文件，该文件位于目录 *msg-svr-base*`/config/` 中，其中 *msg-svr-base* 是安装 Messaging Server 的目录。

以下过程包含配置 S/MIME 功能必需的最少步骤：

1. 安装 Messaging Server 之后，验证 Communications Express Mail 的基本功能是否可以正常工作。

2. 如果尚未执行此操作，则请为有权使用 S/MIME 功能的所有邮件用户创建或获取专用 — 公共密钥对和标准 X.509 v3 格式的证书。
3. 如果使用智能卡存储密钥和证书，则请执行以下操作：
   a. 将智能卡分发到邮件用户。
   b. 确保已在从中访问 Communications Express Mail 的每台客户机上正确地安装了智能卡读卡设备和软件。
4. 如果使用浏览器的本地密钥库存储密钥和证书，请指导邮件用户如何将密钥对和证书下载到本地密钥库。
5. 确保客户机上具有正确的库，以支持智能卡或本地密钥库。有关更多信息，请参见第 626 页的 “客户机的密钥访问库”。
6. 设置 LDAP 目录以支持 S/MIME：
   a. 使用证书授权机构的标识名将 CA 的所有证书存储在 Directory Server 可以访问的 LDAP 目录中。这些证书的 LDAP 属性为 `cacertificate;binary`。请记下存储这些内容的目录信息。在后面的步骤中将用到这些信息。

      有关指定 LDAP 目录信息的示例，请参见第 623 页的 “trustedurl”；有关搜索 LDAP 目录的信息，请参见第 635 页的 “管理证书”。
   b. 在 Directory Server 可以访问的 LDAP 目录中存储公共密钥和证书。公共密钥和证书的 LDAP 属性为 `usercertificate;binary`。请记下存储这些内容的目录信息。在后面的步骤中将用到这些信息。

      有关指定 LDAP 目录信息的示例，请参见第 618 页的 “certurl”；有关搜索 LDAP 目录的信息，请参见第 635 页的 “管理证书”。
   c. 确保发送或接收 S/MIME 邮件的所有用户都可以通过其用户条目中的 LDAP 过滤器使用 S/MIME。过滤器是通过 `mailAllowedServiceAccess` 或 `mailDomainAllowedServiceAccess` LDAP 属性来定义的。

      注意：默认情况下，如果未使用 `mailAllowedServiceAccess` 或 `mailDomainAllowedServiceAccess`，则将允许所有包括 `smime` 的服务。如果要使用这些属性明确指定服务，则必须指定服务 `http`、`smtp` 和 `smime`，以授予邮件用户使用 S/MIME 功能的权限。

      有关更多信息，请参见第 634 页的 “授予使用 S/MIME 功能的权限”。

7. 用任何可用的文本编辑器来编辑 smime.conf 文件。有关参数的语法，请参见文件开头的注释。

   smime.conf 中的所有文本和示例参数前面都带有注释字符 (#)。可以将所需参数添加到 smime.conf 中，或将参数示例复制到文件的其他部分并更改参数示例的值。如果要复制并编辑示例，请确保删除示例行开头的 # 字符。

   将这些参数添加到文件中各自对应的行中：

   a. trustedurl — 设置为 LDAP 目录信息，以查找 CA 的证书。使用在 6a 中保存的信息。

   b. certurl — 设置为 LDAP 目录信息，以查找公共密钥和证书。使用在 6b 中保存的信息。

   c. usercertfilter — 设置为 smime.conf 文件中的示例的值。该示例值通常都是指必需的过滤器。**复制**示例并删除示例行开头的 # 字符。

      该参数指定 Communications Express Mail 用户的主、备用和等效电子邮件地址的过滤器定义，以确保在将用户的专用 — 公共密钥对分配给其他邮件地址时可以找到这些密钥对。

   d. sslrootcacertsurl — 如果要将 SSL 用作 S/MIME applet 和 Messaging Server 之间的通信链路，则应使用 LDAP 目录信息设置 sslrootcacertsurl 以查找 CA 的证书（这些证书用于验证 Messaging Server 的 SSL 证书）。有关更多信息，请参见第 624 页的 “使用 SSL 确保 Internet 链路的安全”。

      checkoverssl — 如果不将 SSL 用作 S/MIME applet 和 Messaging Server 之间的通信链路，则设置为 0。

   e. crlenable — 设置为 0 将立即禁用 CRL 检查，因为执行 CRL 检查可能会要求向 smime.conf 文件添加其他参数。

   f. logindn 和 loginpw — 如果需要进行验证才能访问包含公共密钥和 CA 证书的 LDAP 目录，则请将这些参数设置为具有读权限的 LDAP 条目的标识名和密码。

      注意：无论何时使用由 certurl、crlmappingurl、sslrootcacertsurl 或 trustedurl 参数指定的 LDAP 信息访问 LDAP 目录，都要使用 logindn 和 loginpw 的值。有关更多信息，请参见第 615 页的 “使用证书访问 LDAP 中的公共密钥、 CA 证书和 CRL”。

      如果访问 LDAP 目录时不需要进行验证，则请勿设置 logindn 和 loginpw。

8. 使用 configutil 设置 Messaging Server 选项：

   a. local.webmail.smime.enable — 设置为 1。

b. `local.webmail.cert.enable` — 如果要根据 CRL 验证证书，则设置为 `1`。

有关更多信息，请参见第 623 页的 “Messaging Server 选项”。

9. 现在已将 Communications Express Mail 配置为可以使用 S/MIME 功能。请执行以下步骤验证 S/MIME 功能是否可以正常工作：

a. 重新启动 Messaging Server。

b. 检查 Messaging Server 日志文件 *msg-svr-base*`/log/http`，以了解与 S/MIME 相关的诊断消息。

c. 如果检测到任何有关 S/MIME 的问题，则诊断消息将帮助您确定如何使用配置参数来解决这些问题。

d. 更正必要的配置参数。

e. 重复步骤 a. 到 d.，直至 Messaging Server 的日志文件中不再出现任何有关 S/MIME 的诊断消息。

f. 执行以下步骤检查 S/MIME 功能是否可以正常工作：

I. 从客户机上登录到 Messaging Server。用 “是”或 “始终”回答 S/MIME applet 的特定提示问题。有关更多信息，请参见第 635 页的 “管理证书”。

II. 撰写一条发送给您自己的短消息。

III. 通过选中 “撰写”窗口底部的 “加密”复选框 （如果尚未选中）来对消息进行加密。

IV. 单击 “发送”以将加密消息发送给您自己。这将检验密钥和证书的大多数机制。

V. 如果发现加密消息存在问题，则问题最有可能出在 `smime.conf` 文件中用于 LDAP 目录信息的值和 / 或在 LDAP 目录中存储密钥和证书的方式上。请检查 Messaging Server 日志以获得更多诊断消息。

表 20-3 中总结的其他 S/MIME 参数提供了许多选项，您可以使用这些选项进一步配置 S/MIME 环境。有关这些参数的更多信息，请参见第 617 页的 “smime.conf 文件的参数”。

表 20-3 smime.conf 参数摘要

S/MIME 必需的参数	用于智能卡和本地密钥库的参数	用于 CRL 检查的参数	用于初始设置和安全链路的参数
`certurl*`	`platformwin`	`checkoverssl`	`alwaysencrypt`
`logindn`		`crlaccessfail`	`alwayssign`

表 20-3 smime.conf 参数摘要

S/MIME 必需的参数	用于智能卡和本地密钥库的参数	用于 CRL 检查的参数	用于初始设置和安全链路的参数
loginpw		crldir	sslrootcacertsurl
trustedurl*		crlenable	
usercertfilter*		crlmappingurl	
		crlurllogindn	
		crlurlloginpw	
		crlusepastnextupdate	
		readsigncert	
		revocationunknown	
		sendencryptcert	
		sendencryptcertrevoked	
		readsigncert	
		sendsigncertrevoked	
		timestampdelta	

* 必须为这些参数指定值，因为它们都没有默认值。

使用证书访问 LDAP 中的公共密钥、 CA 证书和 CRL

S/MIME 必需的公共密钥、 CA 证书和 CRL 可能存储在 LDAP 目录中 （请参见上一节）。可以通过单个 URL 或多个 URL 访问 LDAP 中的密钥、证书和 CRL。例如， CRL 可能存储在某个 URL 中，而公共密钥和证书则存储在另一个 URL 中。Messaging Server 允许您指定哪个 URL 包含必需的 CRL 或证书信息，以及有权访问这些 URL 的条目的 DN 和密码。这些 DN/ 密码证书都是可选的；如果未指定任何一个证书，将首先尝试使用 HTTP 服务器证书访问 LDAP ；如果失败，将尝试以 anonymous 访问 LDAP。

要访问必需的 URL，需要设置两对 smime.conf 证书参数：logindn 和 loginpw，以及 crlurllogindn 和 crlurlloginpw。

在 smime.conf 中， logindn 和 loginpw 是用于所有 URL 的证书。它们指定对公共密钥、公共密钥的证书和 CA 证书具有读权限的 LDAP 条目的 DN 和密码。这些密钥、密钥证书和 CA 证书由 certurl 和 trustedurl 参数指定。

crlurllogindn 和 crlurlloginpw 指定对映射表中的结果 URL 具有读权限的 LDAP 条目的 DN 和密码 （有关更多信息，请参见第 629 页的 “访问 CRL”）。如果这些证书未被接受，将拒绝 LDAP 访问并且不再尝试其他证书。要么同时指定这两个参数，要么两者都保留为空。这些参数不适用于直接来自证书的 URL。

设置特定 URL 的密码

Messaging Server 允许对 DN/ 密码对进行专门定义，以访问以下 smime.conf URL：certUrl、 trustedUrl、 crlmappingUrl 和 sslrootcacertsUrl。

语法如下：

url_type　　*URL* **[** | *URL_DN* | *URL_password***]**

示例：

```
trustedurl==ldap://mail.siroe.com:389/cn=Directory Manager, ou=people,
o=siroe.com,o=ugroot?cacertificate?sub?(objectclass=certificationauthority) |
cn=Directory manager | boomshakalaka
```

LDAP 证书用法总结

本节总结了 LDAP 证书的用法。

- 所有 LDAP 证书都是可选的；如果未指定任何一个证书，将首先尝试使用 HTTP 服务器证书访问 LDAP ；如果失败，将尝试以 anonymous 访问 LDAP。

  可以将以下两对 smime.conf 参数用作指定的两组 URL 的证书：

  `logindn` 和 `loginpw` - `smime.conf` 中的所有 URL

  `crlurllogindn` 和 `crlurlloginpw` — 映射表中的所有 URL

  它们都是默认的 LDAP 证书对。

- 可以为 `smime.conf` 中指定的或通过映射 CRL URL 而得到的任何 URL 指定可选的本地 LDAP 证书对。
- 将按照指定证书时的顺序来检查每个证书：

  1) 本地 LDAP 证书对 — 如果指定，则只进行一次尝试

  2) 默认 LDAP 证书对 — 如果指定并且没有本地 LDAP 证书对，则只进行一次尝试

  3) 服务器 — 如果既没有指定本地 LDAP 证书对也没有指定默认 LDAP 证书对，则首先尝试服务器

  4) anonymous — 仅在服务器失败或没有指定任何证书的情况下才尝试 anonymous

- 如果为 URL 指定了本地 LDAP 证书对，则首先使用该证书对；如果访问失败，将拒绝访问。
- 如果没有为 URL 指定本地 LDAP 证书对，则使用对应的默认 LDAP 证书对；如果访问失败，将拒绝访问。

smime.conf 文件的参数

Messaging Server 附带有 `smime.conf` 文件，该文件位于目录 *msg-svr-base*`/config/` 中，其中 *msg-svr-base* 是安装 Messaging Server 的目录。该文件中的所有文本和参数示例前面都带有注释字符 (#)。

您可以将保护您设置的值的参数添加到 `smime.conf` 文件中，也可以编辑参数示例。如果要使用示例，请将示例复制到该文件的其他部分，编辑参数的值并删除示例行开头的 # 字符。

安装 Messaging Server 后，用任何可用的文本编辑器编辑 smime.conf。表 20-4 中所描述的参数不区分大小写，而且如果没有特殊说明，不需要进行设置。

表 20-4 smime.conf 文件中的 S/MIME 配置参数

参数	用途
alwaysencrypt	控制初始设置，以决定是否为有权使用 S/MIME 的所有 Communications Express Mail 用户自动加密所有外发邮件。每个 Communications Express Mail 用户都可以通过使用表 20-6 第 642 页 中所描述的复选框来覆盖用于邮件的这一参数值。 选择以下值之一： 0 — 不对邮件进行加密。 Communications Express Mail 中的加密复选框显示为未选中状态。该值为默认值。 1 — 始终对邮件进行加密。 Communications Express Mail 中的加密复选框显示为选中状态。 示例： alwaysencrypt==1
alwayssign	控制初始设置，以决定是否为有权使用 S/MIME 的所有 Communications Express Mail 用户自动签名所有外发邮件。每个 Communications Express Mail 用户都可以通过使用表 20-6 第 642 页 中所描述的复选框来覆盖用于邮件的这一参数值。 选择以下值之一： 0 — 不对消息进行签名。 Communications Express Mail 中的签名复选框显示为未选中状态。该值为默认值。 1 — 始终对消息进行签名。 Communications Express Mail 中的签名复选框显示为选中状态。 示例： alwaysensign==1
certurl	指定 LDAP 目录信息，以查找 Communications Express Mail 用户的公共密钥和证书 （公共密钥的 LDAP 属性为 usercertificate;binary）。有关证书的更多信息，请参见第 635 页的 “管理证书”。 该参数必须指向 LDAP 目录信息树 (DIT) 的用户 / 组中的最高节点， DIT 包括 Messaging Server 正在服务的所有用户。这对具有多个域的站点来说尤其重要；对于单域来说，标识名必须是用户 / 组树的根标识名而不是包含用户的子树的标识名。 您必须设置该参数。 示例： certurl==ldap://mail.siroe.com:389/ou=people, o=siroe.com, o=ugroot

表 20-4 smime.conf 文件中的 S/MIME 配置参数

参数	用途
checkoverssl	控制根据 CRL 检查密钥的证书时是否使用 SSL 通信链路。有关更多信息，请参见第 624 页的 “使用 SSL 确保 Internet 链路的安全”。 选择以下值之一： 0 — 不使用 SSL 通信链路。 1 — 使用 SSL 通信链路。该值为默认值。 如果将代理服务器与正在进行的 CRL 检查结合使用，则可能会出现问题。有关更多信息，请参见第 631 页的 “代理服务器和 CRL 检查”。
crlaccessfail	指定 Messaging Server 多次尝试访问 CRL 失败后等待下一次尝试访问 CRL 的时间。该参数没有默认值。 语法： crlaccessfail==*number_of_failures*:*time_period_for_failures*:*wait_time_before_retry* 其中： *number_of_failures* 是在 *time_period_for_failures* 指定的时间间隔中，允许 Messaging Server 访问 CRL 失败的次数。该值必须大于零。 *time_period_for_failures* 是 Messaging Server 对尝试访问 CRL 失败进行计数的秒数。该值必须大于零。 *wait_time_before_retry* 是 Messaging Server 在指定时间间隔内达到尝试访问失败次数的限制而要再次尝试访问 CRL 所需等待的秒数。该值必须大于零。 示例： crlaccessfail==10:60:300 在该示例中， Messaging Server 在 1 分钟内访问 CRL 时出现了 10 次失败。 Messaging Server 在等待 5 分钟后再次尝试访问 CRL。有关更多信息，请参见第 633 页的 “访问 CRL 时出现问题”。
crldir	指定 Messaging Server 将 CRL 下载到磁盘的目录信息。默认值为 *msg-svr-base*/data/store/mboxlist，其中 *msg-svr-base* 是安装 Messaging Server 的目录。有关更多信息，请参见第 631 页的 “使用过时 CRL”。
crlenable	控制是否根据 CRL 检查证书。如果存在匹配项，则证书将被视为已撤销。 smime.conf 文件中的 send*revoked 参数的值确定 Communications Express Mail 是拒绝还是使用具有已撤销证书的密钥。有关更多信息，请参见第 628 页的 “验证专用密钥和公共密钥”。 选择以下值之一： 0 — 不根据 CRL 检查每个证书。 1 — 根据 CRL 检查每个证书。该值为默认值。请确保将 Messaging Server 的 local.webmail.cert.enable 选项设置为 1，否则即使将 crlenable 设置为 1 也不会进行 CRL 检查。

表 20-4 smime.conf 文件中的 S/MIME 配置参数

参数	用途
crlmappingurl	指定 LDAP 目录信息以查找 CRL 映射定义。仅在具有映射定义时才需要该参数。有关更多信息，请参见第 629 页的 “访问 CRL”。该参数没有默认值。您也可以选择添加能够访问该 URL 的 DN 和密码。 语法： crlmappingurl *URL*[|*URL_DN*	*URL_password*] 示例： crlmappingurl==ldap://mail.siroe.com:389/cn=XYZ Messaging, ou=people, o=mail.siroe.com,o=isp?msgCRLMappingRecord?sub?(objectclass=msgCRLMappingTable)|cn=Directory Manager	pAsSwOrD
crlurllogindn	指定对 CRL 映射定义具有读权限的 LDAP 条目的标识名 （如果条目直接来自证书，则没有标识名。有关更多信息，请参见第 904 页中的 “访问 CRL”）。 如果未指定 crllogindn 和 crlloginpw 的值，则 Messaging Server 将使用 HTTP 服务器的登录值来访问 LDAP 目录。如果失败，Messaging Server 将尝试匿名访问 LDAP 目录。 示例： crllogindn==cn=Directory Manager
crlurlloginpw	为 crllogindn 参数的标识名指定 ASCII 文本格式的密码。 如果未指定 crllogindn 和 crlloginpw 的值，则 Messaging Server 将使用 HTTP 服务器的登录值来访问 LDAP 目录。如果失败，Messaging Server 将尝试匿名访问 LDAP 目录。 示例： crlloginpw==zippy
crlusepastnextupdate	控制在当前日期超过了 CRL 的 “下一次更新”字段中指定的日期时是否使用 CRL。有关更多信息，请参见第 631 页的 “使用过时 CRL”。 选择以下值之一： 0 — 不使用过时的 CRL。 1 — 使用过时的 CRL。该值为默认值。
logindn	指定对 LDAP 目录中的公共密钥、公共密钥的证书和 CA 证书具有读权限的 LDAP 条目的标识名。这些密钥、密钥证书和 CA 证书位于由 certurl 和 trustedurl 参数指定的 LDAP 目录中。 如果未指定 logindn 和 loginpw 的值，则 Messaging Server 将使用 HTTP 服务器的登录值来访问 LDAP 目录。如果失败， Messaging Server 将尝试匿名访问 LDAP 目录。 示例： logindn==cn=Directory Manager

表 20-4 smime.conf 文件中的 S/MIME 配置参数

参数	用途
loginpw	为 logindn 参数的标识名指定 ASCII 文本格式的密码。 如果未指定 logindn 和 loginpw 的值，则 Messaging Server 将使用 HTTP 服务器的登录值来访问 LDAP 目录。如果失败， Messaging Server 将尝试匿名访问 LDAP 目录。 示例： loginpw==SkyKing
platformwin	指定在 Windows 平台上使用智能卡或本地密钥库时必需的一个或多个库名称。仅在默认值不适用于您的客户机时才更改该参数。默认值为： platformwin==CAPI:library=capibridge.dll; 有关更多信息，请参见第 626 页的 “客户机的密钥访问库”。
readsigncert	控制在阅读消息时是否根据 CRL 检查公共密钥的证书以验证 S/MIME 数字签名。（专用密钥用于创建邮件的数字签名，但是不能根据 CRL 对其进行检查，因而要根据 CRL 检查与专用密钥相关联的公共密钥的证书。）有关更多信息，请参见第 628 页的 “验证专用密钥和公共密钥”。 选择以下值之一： 0 — 不根据 CRL 检查证书。 1 — 根据 CRL 检查证书。该值为默认值。
revocationunknown	确定在根据 CRL 检查证书时返回模糊状态的情况下应采取的措施。在这种情况下，无法确定证书的状态为有效还是已撤销。有关更多信息，请参见第 628 页的 “验证专用密钥和公共密钥”。 选择以下值之一： ok — 将证书视为有效证书。 revoked — 将证书视为撤销证书。该值为默认值。
sendencryptcert	控制用于加密外发邮件的公共密钥的证书在使用之前是否根据 CRL 进行检查。有关更多信息，请参见第 628 页的 “验证专用密钥和公共密钥”。 选择以下值之一： 0 — 不根据 CRL 检查证书。 1 — 根据 CRL 检查证书。该值为默认值。
sendencryptcertrevoked	确定当用于加密外发邮件的公共密钥证书已撤销时应采取的措施。有关更多信息，请参见第 628 页的 “验证专用密钥和公共密钥”。 选择以下值之一： allow — 使用公共密钥。 disallow — 不使用公共密钥。该值为默认值。

表 20-4 smime.conf 文件中的 S/MIME 配置参数

参数	用途
sendsigncert	控制是否根据 CRL 检查公共密钥证书，从而确定是否可以将专用密钥用于为外发邮件创建数字签名。（专用密钥用于数字签名，但是不能根据 CRL 对其进行检查，因而要根据 CRL 检查与专用密钥相关联的公共密钥的证书。）有关更多信息，请参见第 628 页的“验证专用密钥和公共密钥”。 选择以下值之一： 0 — 不根据 CRL 检查证书。 1 — 根据 CRL 检查证书。该值为默认值。
sendsigncertrevoked	确定专用密钥已撤销时应采取的措施。（专用密钥用于创建邮件的数字签名，但是不能根据 CRL 对其进行检查，因而要根据 CRL 检查与专用密钥相关的公共密钥的证书。如果公共密钥证书已撤销，则其对应的专用密钥也将撤销。）有关更多信息，请参见第 628 页的“验证专用密钥和公共密钥”。 选择以下值之一： allow — 使用撤销的专用密钥。 disallow — 不使用撤销的专用密钥。该值为默认值。
sslrootcacertsurl	指定标识名和 LDAP 目录信息以查找有效 CA 的证书，这些证书用于验证 Messaging Server 的 SSL 证书。如果在 Messaging Server 中启用了 SSL，则该参数为必需参数。有关更多信息，请参见第 624 页的 “使用 SSL 确保 Internet 链路的安全”。 如果具有接收来自客户机应用程序的所有请求的代理服务器的 SSL 证书，则这些 SSL 证书的 CA 证书也必须位于该参数所指向的 LDAP 目录中。 您也可以选择添加能够访问该 URL 的 DN 和密码。 语法： crlmappingurl *URL*[|*URL_DN* | *URL_password*] 示例： sslrootcacertsurl==ldap://mail.siroe.com:389/cn=SSL Root CA Certs, ou=people, o=siroe.com, o=isp? cacertificate;binary?base? (objectclass=certificationauthority)|cn=Directory Manager | pAsSwOrD
timestampdelta	以秒为单位指定时间间隔，该时间间隔用于确定根据 CRL 检查公共密钥的证书时是使用消息的发送时间还是接收时间。 该参数的默认值为零，这将使 Communications Express Mail 始终使用接收时间。有关更多信息，请参见第 632 页的 “确定要使用的邮件发送时间”。 示例： timestampdelta==360

表 20-4 smime.conf 文件中的 S/MIME 配置参数

参数	用途
trustedurl	指定标识名和 LDAP 目录信息以查找有效 CA 的证书。该参数为必需参数。 您也可以选择添加能够访问该 URL 的 DN 和密码。 语法： crlmappingurl *URL*[|*URL_DN*	*URL_password*] 示例： trustedurl==ldap://mail.siroe.com:389/cn=Directory Manager, ou=people, o=siroe.com,o=ugroot?cacertificate?sub?(objectclass=certificationauthority)|cn=Directory Manager	pAsSwOrD
usercertfilter	指定 Communications Express Mail 用户的主、备用和等效电子邮件地址的过滤器定义，以确保将用户的专用 - 公共密钥对分配给其他邮件地址时可以找到这些密钥对。 该参数为必需参数，并且没有默认值。

Messaging Server 选项

要设置适用于 S/MIME 的三个 Messaging Server 选项，请在安装 Messaging Server 的计算机上执行以下操作：

1. 以超级用户身份登录。然后输入：

   ```
   # cd msg-svr-base/sbin
   ```

   其中， *msg-svr-base* 是安装 Messaging Server 的目录。

2. 按照下表所述并根据系统需要来设置 Messaging Server 选项。使用 configutil 实用程序设置选项。如果没有特殊说明，则不需要对选项进行设置。

参数	用途
local.webmail.cert.enable	控制处理 CRL 检查的进程是否应执行 CRL 检查。 0 — 进程不根据 CRL 检查证书。该值为默认值。 1 — 进程根据 CRL 检查证书。如果设置为 1，请确保将 smime.conf 文件中的 crlenable 参数也设置为 1。
local.webmail.cert.port	指定运行 Messaging Server 的计算机上的端口号，以用于 CRL 通信。只能在该计算机本地使用该端口。该值必须大于 1024。默认值为 55443。 如果默认端口号已被占用，则必须设置该选项。

参数	用途
local.webmail.smime.enable	控制 Communications Express Mail 用户是否可以使用 S/MIME 功能。选择以下值之一： 0 — 即使为系统配置了正确的软件和硬件，Communications Express Mail 用户也无法使用 S/MIME 功能。该值为默认值。 1 — 有权使用 S/MIME 功能的 Communications Express Mail 用户可以使用 S/MIME 功能。 示例： configutil -o local.webmail.smime.enable -v 1

使用 SSL 确保 Internet 链路的安全

Messaging Server 支持使用用于 Internet 链路的安全套接字层 (SSL)（Internet 链路会影响 Communications Express Mail），如下表所示。

链接对象：	说明
Messaging Server 和 Communications Express Mail	要使用 SSL 确保该链路的安全，需要进行有关 Messaging Server 的管理工作。 Communications Express Mail 用户在其浏览器中输入 Messaging Server 的 URL 信息时，必须使用 HTTPS 协议，而不是 HTTP 协议。 有关更多信息，请参见第 625 页的 “确保 Messaging Server 和 Communications Express Mail 之间的链路的安全”。
Messaging Server 和 S/MIME applet	根据 CRL 检查公共密钥证书时，S/MIME applet 必须直接与 Messaging Server 进行通信。要使用 SSL 确保该链路的安全，除了设置 smime.conf 文件中的 sslrootcacertsurl 和 checkoverssl 之外，还需要进行有关 Messaging Server 的管理工作。 有关更多信息，请参见第 625 页的 “确保 Messaging Server 和 S/MIME Applet 之间的链路的安全”。

确保 Messaging Server 和 Communications Express Mail 之间的链路的安全

Messaging Server 支持使用用于 Messaging Server 和 Communications Express Mail 之间的 Internet 链路的安全套接字层 (SSL)。在为 SSL 设置了 Messaging Server 之后，请为 SSL 配置 Communications Express。请参见 Communications Express 管理指南 (http://docs.sun.com/doc/819-1067)。 Communications Express Mail 用户在其浏览器中使用 HTTPS 协议

HTTPS://*hostname*.*domain*:*secured_port*

而不是 HTTP 协议 （HTTP://*hostname*.*domain*:*unsecure_port*）来指定 Communications Express URL。显示 Communications Express 登录窗口时，如果用户看到窗口底部的锁定位置有锁形图标，则说明系统具有安全链路。

有关适用于 Messaging Server 的 SSL 配置信息，请参见第 578 页的 “配置加密和基于证书的验证”或 Communications Express Administration Guide (http://docs.sun.com/doc/819-0115)。

确保 Messaging Server 和 S/MIME Applet 之间的链路的安全

根据 CRL 检查公共密钥的证书时， S/MIME applet 必须直接与 Messaging Server 进行通信。要使用 SSL 确保该通信链路的安全，请执行以下步骤：

1. 执行管理任务来为 Messaging Server 配置 SSL。请参见第 578 页的 “配置加密和基于证书的验证”。
2. 设置 smime.conf 文件中的 sslrootcacertsurl 参数，以指定查找根 SSL CA 证书的信息。如果在 Messaging Server 和 S/MIME applet 之间建立了链路，则将使用这些 CA 证书来验证 Messaging Server 的 SSL 证书。
3. 将 smime.conf 文件中的 checkoverssl 参数设置为 1。该 Messaging Server 选项用于确定是否将 SSL 用于 Messaging Server 和 S/MIME applet 之间的链路。无论 Communications Express Mail 用户以何种方式指定 Messenger Server 的 URL （HTTP 或 HTTPS），只要将 checkoverssl 设置为 1， SSL 就可以确保 Messaging Server 和 S/MIME applet 之间的链路的安全。

注 在 Messaging Server 和客户机应用程序（例如 Communications Express Mail）之间可以使用代理服务器。有关使用具有或不具有安全通信链路的代理服务器的更多信息，请参见第 631 页的 “代理服务器和 CRL 检查”。

客户机的密钥访问库

无论邮件用户将专用 — 公共密钥对和证书保存在智能卡上还是保存在其浏览器的本地密钥库中，客户机上都必须具有密钥访问库才能支持存储方法。

这些库由智能卡和浏览器的供应商提供。您必须确保客户机上具有正确的库，并用 `smime.conf` 文件中适当的平台参数指定库名称。参数选项包括：

- `platformwin`，适用于 PC 上运行的 Microsoft Windows。

如果您知道客户机上安装了哪些库，则可以只指定这些库；如果不确定客户机上安装了哪些库，则可以指定用于给定平台和供应商的所有库名称。如果 S/MIME applet 在您指定的库名称中找不到必需的库，则将无法使用 S/MIME 功能。

指定一个或多个库文件名的语法如下：

platform_parameter==*vendor*:library=*library_name*;...

其中：

platorm_parameter 是访问 Communications Express Mail 的客户机平台的参数名称。选择以下名称之一：`platformwin`

vendor 指定智能卡或浏览器的供应商。选择以下文字之一：

`cac`（适用于 ActivCard 或 NetSign 智能卡）
`capi`（适用于具有 CAPI 的 Internet Explorer）
`mozilla`（适用于具有网络安全服务的 Mozilla）

library_name 指定库文件名。有关供应商和操作系统的库名称，请参见表 20-5。

表 20-5 客户机的特殊库

智能卡或浏览器供应商	操作系统	库文件名
	Windows	`acpkcs211.dll`
具有加密应用程序编程接口 (CAPI) 的 Internet Explorer	Windows	`capibridge.dll`
	Windows	`softokn3.dll`
	Windows	`core32.dll`

示例

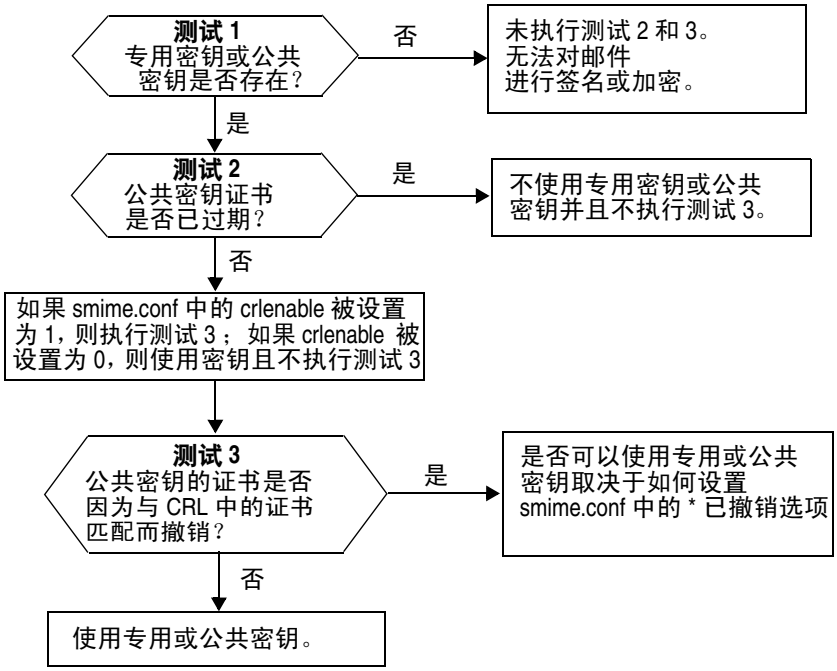
以下示例为 Windows 平台指定了一个智能卡库、一个 Internet Explorer 库和一个 Mozilla 库：

```
platformwin==CAC:library=acpkcs211.dll;CAPI:library=capibridge.dll;
MOZILLA:library=softokn3.dll;
```

验证专用密钥和公共密钥

在 Communications Express Mail 使用专用密钥或公共密钥之前，必须先通过图 20-2 所示的验证测试。本节其余部分将介绍根据 CRL 检查公共密钥的证书的详细信息。

图 20-2 验证专用密钥和公共密钥。



查找用户的专用或公共密钥

当 Communications Express Mail 用户具有多个专用 — 公共密钥对和多个电子邮件地址（主电子邮件地址、备用电子邮件地址或别名电子邮件地址）时，这些密钥可能会与多个地址相关联。在这种情况下， S/MIME applet 必须找到所有密钥以进行验证。使用 `smime.conf` 文件中的 `usercertfilter` 参数来定义过滤器，该过滤器将在根据 CRL 检查公共密钥的证书时为密钥的拥有者创建一个邮件地址列表。有关更多信息，请参见第 623 页的 “usercertfilter”。

何时根据 CRL 检查证书？

证书撤销列表 （即 CRL）是发布密钥对和证书的 CA 所维护的已撤销证书的列表。启用 CRL 检查时，只要发出了查看证书是否已撤销的证书请求，就会使系统检查 CRL。

当将 `smime.conf` 文件中的 `crlenable` 设置为 `1` 时，将在找到未过期密钥后执行 CRL 测试。将根据 CRL 检查公共密钥的证书。每个 CA 只能有一个 CRL，但是同一个 CRL 可以放在多个不同的位置上。

当 S/MIME applet 向 Messaging Server 发送检查证书的请求后，Messaging Server 将根据 CRL 检查证书。公共密钥证书用于验证公共密钥。由于专用密钥是保密的，只能由拥有该密钥的人员使用，因此不能根据 CRL 直接检查专用密钥。要确定专用密钥是否有效，需要使用密钥对的公共密钥证书。当公共密钥的证书通过 CRL 测试时，关联的专用密钥也就通过了该测试。

导致证书撤销的原因有很多，例如，证书的拥有者已离开您的工作单位或丢失了智能卡。

在下列三种情况下需要根据 CRL 检查证书：

- 对外发邮件进行签名时

  S/MIME applet 将始终执行此检查，除非您将 `sendsigncert` 设置为 `0` 或将 `crlenable` 设置为 `0`。

- 阅读收到的签名邮件时

  S/MIME applet 将始终执行此检查，除非您将 `readsigncert` 设置为 `0` 或将 `crlenable` 设置为 `0`。

- 对外发邮件进行加密时

  S/MIME applet 将始终执行此检查，除非您将 `sendencryptcert` 设置为 `0` 或将 `crlenable` 设置为 `0`。

访问 CRL

一个证书包含零个或多个 URL （称为分发点）， Messaging Server 使用这些 URL 来查找 CRL。如果证书没有 CRL URL，则不能根据 CRL 检查该证书，并且会在不知道密钥真实状态的情况下使用专用或公共密钥对邮件进行签名或加密。

如果 Messaging Server 在尝试所有可用的 URL 后都无法查找 CRL 或无法获得对 CRL 的访问权，证书的状态将被视为未知。将由 `revocationunknown` 的设置来确定是否使用处于未知状态的专用或公共密钥。

尽管每个 CA 只能有一个 CRL，但可以在多个位置保存同一个 CRL 的多个副本，体现在用户的公共密钥证书的多个 URL 中。 Messaging Server 将尝试证书的所有 URL 位置，直到获得对 CRL 的访问权。

通过定期从 CA 将最新的 CRL 下载到所需位置，您可以管理 CRL 的多个副本从而优化访问。尽管您无法更改证书中嵌入的 URL，但您可以通过将证书中的 URL 映射到包含 CRL 信息的新 URL，来重新定位 Messaging Server 以使用新的 CRL 位置。请使用下面的语法在 LDAP 目录 （请参见 `crlmappingurl`）中创建一个或多个映射定义的列表：

`msgCRLMappingRecord=`*url_in_certificate*`==`*new_url*`[|`*url_login_DN*`|`*url_login_password*`]`

url_in_certificate 是证书中包含用来查找 CRL 的旧信息的 URL。 *new_url* 是包含新 CRL 信息的新 URL。 *url_login_DN* 和 *url_login_password* 是允许访问 *new_url* 的条目的 DN 和密码。这两个选项都是可选项，如果指定了这两个选项，将仅用于访问新的 URL。

如果 DN 和密码验证失败，将拒绝 LDAP 访问并且不再尝试其他证书。这些登录证书仅对 LDAP URL 有效。如果使用了 `smmime.conf` 的 `crlurllogindn` 和 `crlurlloginpw`，则无需在映射记录中指定登录 DN 和密码。请参见第 615 页的 “使用证书访问 LDAP 中的公共密钥、 CA 证书和 CRL”。

仅允许使用一层映射。可以将证书中各个不同的 URL 映射到同一个新 URL，但您不能将证书 URL 分配给多个新 URL。例如，以下映射列表就是一个无效映射列表：

```
msgCRLMappingRecord=URL12==URL45
msgCRLMappingRecord=URL12==URL66
msgCRLMappingRecord=URL12==URL88
msgCRLMappingRecord=URL20==URL90
msgCRLMappingRecord=URL20==URL93
```

以下示例是正确的映射列表：

```
msgCRLMappingRecord=URL12==URL45
msgCRLMappingRecord=URL14==URL66
msgCRLMappingRecord=URL88==URL66
msgCRLMappingRecord=URL201==URL90
msgCRLMappingRecord=URL202==URL93
```

在 LDAP 目录中创建映射定义后，请使用 `smime.conf` 文件中的 `crlmappingurl` 来指定查找这些映射定义的目录信息。请参见第 620 页的 “crlmappingurl”。

代理服务器和 CRL 检查

如果您的系统在客户机应用程序和 Messaging Server 之间使用了代理服务器，那么，尽管您已正确配置了 S/MIME applet 来执行 CRL 检查，系统仍可能会阻止 CRL 检查。遇到此问题时， Communications Express Mail 用户会收到错误消息，警告他们有效密钥证书已撤销或其状态未知。

造成此问题的原因包括：

- 使用以下配置值请求 CRL 检查：
  - `smime.conf` 文件中的 `crlenable` 参数设置为 `1`
  - Messaging Server 的 `local.webmail.cert.enable` 选项设置为 `1`
- S/MIME applet 和代理服务器之间的通信链路未使用 SSL 进行安全保护，但 S/MIME applet 需要安全链路，因为已将 `smime.conf` 文件中的 `checkoverssl` 参数设置为 `1`

要解决此问题，您可以：

1. 使用 SSL 将客户机和代理服务器之间的通信链路设置为安全链路，并将所有配置值保留为原来的值。

   或者，

2. 保留通信链路不受安全保护的状态，并将 `checkoverssl` 设置为 `0`。

有关更多信息，请参见第 624 页的 “使用 SSL 确保 Internet 链路的安全”。

使用过时 CRL

当 S/MIME applet 向 Messaging Server 发送检查证书的请求后，Messaging Server 将根据 CRL 检查证书。 Messaging Server 并不是在每次检查证书时都将 CRL 下载到内存中，而是将 CRL 的副本下载到磁盘中并使用该副本进行证书检查。每个 CRL 都有一个下次更新字段，该字段指定在哪个日期后应该使用更新的 CRL 版本。下次更新日期可被视为使用 CRL 的截止日期或时间限制。超过下次更新日期的 CRL 将被视为旧的或过时的 CRL，并促使 Messaging Server 在下次检查证书时下载最新版本的 CRL。

每次 S/MIME applet 请求根据 CRL 检查证书时， Messaging Server 都将执行以下操作：

1. 将 CRL 的当前日期与下次更新日期相比较。

2. 如果 CRL 已过时， Messaging Server 将下载最新版本的 CRL 以替换磁盘上过时的 CRL，然后进行检查。但是，如果找不到或无法下载最新的 CRL，将使用 `smime.conf` 文件中的 `crlusepastnextupdate` 的值来确定要执行的操作。

3. 如果 `crlusepastnextupdate` 被设置为 `0`，则不使用过时的 CRL，并且有问题的证书将处于一种模糊状态。 S/MIME applet 使用 `smime.conf` 中的 `revocationunknown` 的值来确定下一步操作：

   a. 如果 `revocationunknown` 被设置为 `ok`，证书将被视为有效，并将使用专用或公共密钥对邮件进行签名或加密。

   b. 如果 `revocationunknown` 被设置为 `revoked`，证书将被视为无效，且不使用专用或公共密钥对邮件进行签名或加密，系统将显示一条弹出式错误消息，警告邮件用户无法使用密钥。

   如果 `crlusepastnextupdate` 被设置为 `1`， S/MIME applet 将继续使用过时的 CRL，这样会使 Communications Express Mail 中的处理不会出现任何中断，但系统会向 Messaging Server 日志文件写入一条消息，警告您出现了这种情况。

这一系列事件将根据 CRL 检查证书的顺序继续发生。只要 Messaging Server 能够及时下载最新版本的 CRL，邮件处理就会根据 `smime.conf` 文件中的设置继续进行而不会中断。定期检查 Messaging Server 日志以查看是否存在指明正在使用过时 CRL 的重复消息。如果无法下载更新的 CRL，您需要调查无法访问此 CRL 的原因。

确定要使用的邮件发送时间

`timestampdelta` 参数主要用于以下目的：

1. 用于处理需要花费很长时间才能到达目的地的邮件的情况。对于这种情况，发件人的密钥可能会被视为无效密钥，尽管事实上该密钥在发送邮件时是有效的。

2. 用于限制对邮件发送时间的信任，因为发送时间可以伪造。

与每封邮件相关的时间有两个：

- 发送邮件的时间，可以在邮件标题详细信息的 “日期”行找到
- 邮件到达目的地的时间，可以在邮件标题详细信息的上一个 “已收到”行找到

注 单击邮件的 “发件人”字段右侧的三角形图标可以查看邮件标题的详细信息。

发送邮件时有效的证书可能在邮件到达目的地时已撤销或过期。遇到此情况时，检查证书有效性时应使用哪个时间呢？是发送时间还是收到时间？使用发送时间将验证发送邮件时证书是否有效。但如果始终使用发送时间，就会忽略一个事实：邮件可能需要很长时间才能到达目的地。在这种情况下最好使用收到的时间。

您可以使用 smime.conf 文件中的 timestampdelta 参数来影响进行 CRL 检查时使用的时间。请将此参数设置为表示秒数的正整数。如果收到时间减去 timestampdelta 的值为发送时间前的某个时间，则使用发送时间。否则，使用收到时间。timestampdelta 的值越小，使用收到时间的频率就越高。如果未设置 timestampdelta，将始终使用收到时间。请参见第 622 页的 “timestampdelta”。

访问 CRL 时出现问题

由于网络或服务器问题等各种原因，当 Messaging Server 尝试根据 CRL 检查证书时， CRL 可能会不可用。您可以使用 smime.conf 文件中的 crlaccessfail 参数来管理 Messaging Server 尝试访问 CRL 的频率，从而使 Messaging Server 可以执行其他任务，而不是一直把时间花在尝试获得对 CRL 的访问上。

使用 crlaccessfail 定义以下内容：

- 尝试失败的次数 （每次尝试失败后，就会将一条错误消息写入 Messaging Server 日志）
- 失败尝试计数发生在哪个时间段
- 进行新一轮的 CRL 访问尝试之前所等待的时间

有关此参数的语法和示例，请参见第 614 页的 “crlaccessfail”。

当证书撤销时

当公共密钥的证书与 CRL 上的任何条目都不匹配时，将使用该专用或公共密钥对外发邮件进行签名或加密。当证书与 CRL 上的某个条目匹配或证书的状态为未知时，该专用或公共密钥将被视为已撤销。默认情况下，Communications Express Mail 不使用具有已撤销证书的密钥对外发邮件进行签名或加密。如果在收件人读取邮件时签名邮件的专用密钥已撤销，收件人将收到一条警告消息，指示不应相信该签名。

如果需要，您可以使用 smime.conf 文件中的下列参数来更改所有已撤销证书的各种默认策略：

- 将 sendsigncertrevoked 设置为 allow，以使用被视为已撤销的专用密钥 （因为其公共密钥的证书已撤销）对外发邮件进行签名

- 将 sendencryptcertrevoked 设置为 allow，以使用具有已撤销证书的公共密钥对外发邮件进行加密
- 将 revocationunknown 设置为 ok，以将状态为未知的证书视为有效证书；将使用该专用或公共密钥对外发邮件进行签名或加密

授予使用 S/MIME 功能的权限

可以使用 LDAP 过滤器来授予或拒绝可通过 Communications Express Mail 使用的各种邮件服务的权限。过滤器是通过 mailAllowedServiceAccess 或 mailDomainAllowedServiceAccess LDAP 属性来定义的。一般来说，过滤器通过以下三种方式之一运行：

- 如果不使用过滤器，则所有用户都有权访问所有服务
- 明确授权一列用户可以访问指定的服务名称 （服务名称列表前带加号 [+]）
- 明确拒绝一列用户访问指定的服务名称 （服务名称列表前带减号 [-]）

S/MIME 必需的邮件服务名称包括 http、 smime 和 smtp。如果需要限制 Communications Express Mail 用户对 S/MIME 的使用，请使用相应的 LDAP 属性语法和服务名称来创建过滤器。使用 LDAP 命令来创建或修改属性。

S/MIME 权限示例

1. 以下示例阻止了一个 Communications Express Mail 用户对 S/MIME 功能的访问：

```
mailAllowedServiceAccess:-smime:*$+imap,pop,http,smtp:*
```

或

```
mailAllowedServiceAccess:+imap,pop,http,smtp:*
```

2. 以下示例阻止了某个域中的所有 Communications Express Mail 用户对 S/MIME 功能的访问：

```
mailDomainAllowedServiceAccess:-smime:*$+imap:*$+pop:*$+smtp:*$+http:*
```

或

```
mailDomainAllowedServiceAccess:+imap:*$+pop:*$+smtp:*$+http:*
```

有关更多信息，请参见第 592 页的 “过滤器语法”。

管理证书

下面的大多数示例都使用了 ldapsearch 和 ldapmodify 命令来搜索 LDAP 目录以查找用户密钥和证书。这些命令由 Directory Server 提供。有关这些命令的更多信息，请参见 Sun ONE Directory Server Resource Kit Tools Reference Release 5.2。

LDAP 目录中的 CA 证书

以下示例将某个证书授权机构的证书添加到 LDAP 目录中。这些证书的目录结构已经存在。证书及其所属的 LDAP 条目将被输入到名为 add-root-CA-cert.ldif 的 .ldif 文件中。除了证书信息必须以 Base64 编码文本形式输入外，所有文本都将以 ASCII 文本形式输入到文件中：

```
dn:cn=SMIME Admin,ou=people,o=demo.siroe.com,o=demo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: certificationAuthority
cn: RootCACerts
sn: CA
authorityRevocationList: novalue
certificateRevocationList: novalue
cacertificate;binary:: MFU01JTUUEjAQBgNVBAsTCU1zZ1NlcnZlcjcMBoGA1UEAxMTydG
QGEwJVUzEOMAwGA1UEMFUJTUUxEjAQBgNVBAsTCU1zZ1NlcnZlcjEMBoGA1UEAxMTQ2VydG
aFw0wNjAxMwODAwMDBaM267hgbX9FExCzAJByrjgNVBAk9STklBMQwCgYDVQQVHR8EgaQwg
YTAlVMRMQYDVQQIEwpDQUxJRk9STklBMQwwCgYDVQQKEwww3ltgYz11lzAdBgNVBpYSE9Vc
5yZWQaddWlm899XBsYW5ldC5jb20wgZ8wDQYJoGBAK1mUTy8vvnOFg4mlHjkghytQUR1k8l
5mvWRf77ntm5mGXRD3XMU4OciUq6zUfIg3ngvxlLyERTIqjUS8HQU4R5pvj+rrVgsAGjggE
+FNAJmtOV2A3wMyghqkVPNDP3Aqq2fkcn4va3C5nRNAYxNNVE84JJ0H3jyPDXhMBlQU6vQn
weMBAAjggEXMIIBEzARBglghkgBhCAQEEBApqlSai4mfuvjh02SQkoPMNDAgTwMB8GA1UdI
QYMBaAEd38IK05AHreiU9OYc6vNMOwZMIGsBgNVHR8EgaQwgaEwb6BtoGuGaWxkYXA6Lyht
bmcucmVkLmlbGFuZXQuY29tL1VJD1DXJ0aWZpY2F0ZSBNYW5hZ2VyLE9VPVBlb3BsZSxPPW
aWxxYT9jZXJ0aZpY2jdu2medXRllkghytQURYFNrkuoCygKoYoaHR0cDovL3Bla2kghytQU
Zy5yZWQuaXBsYW5lC5jb20vcGVranLmNybDAeBgNVHREEFzAVgRNwb3J0aWEuc2hhb0BzdW
4uY29tMA0GCxLm78freCxS3Pp078jyTaDci1AudBL8+RrRUQvxsMJfZeFED+Uuf10Ilt6kw
Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==
```

使用 ldapmodify 命令将 CA 的证书添加到 LDAP 目录中：

```
# ldapmodify -a -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd -v
-f add-root-CA-cert.ldif
```

smime.conf 中 trustedurl 参数的值指定了 CA 证书在 LDAP 目录中的位置。对于示例 1， trustedurl 被设置为：

```
trustedurl==ldap://demo.siroe.com:389/cn=SMIME Admin, ou=people,
o=demo.siroe.com,o=demo?cacertificate;binary?sub?(objectclass=certificatio
nAuthority)
```

LDAP 目录中的公共密钥和证书

以下示例演示了如何将邮件用户的公共密钥和证书添加到 LDAP 目录中。该示例假定 LDAP 目录中已存在该邮件用户。密钥和证书及其所属的 LDAP 条目将被输入到名为 add-public-cert.ldif 的 .ldif 文件中。除了密钥和证书信息必须以 Base64 编码文本形式输入外，所有文本都将以 ASCII 文本形式输入到文件中。

```
dn:uid=JohnDoe,ou=People, o=demo.siroe.com,o=demo
changetype: modify
replace: usercertificate
usercertificate;binary:: MFU01JTUUxEjAQBgNVBAsT1zZ1NlcnZlcjMBoGA1UEAxMTydG
QGEwJVUzEAwGA1hMFU01JTUUxEjAQBgNVBAsTCU1zZ1NlcnZlcjEcMBoGA1UEAxMTQ2VydG
aFw0wNjAxMTODAwaM267hgbX9FExCzAJBgwyrjgNVBAk9STklBMQwwCgYDVQQVHR8EgaQwg
AlVzMRMwEQYDVQQIDQUxJRk9STklBMQwwCgYDVQQKEwww3ltgoOYz11lzAdBgNVBpYSE9Vc
5yZWaddiiWlm899XBsYW5ldb20wgZ8wDQYJoGBAK1mUTy8vvO2nOFg4mlHjkghytQUR1k8l
5mvgcWL77ntm5mGXRD3XMU4OcizUfIg3ngvxlLKLyERTIqjUS8HQU4R5pvj+rrVgsAGjggE
+FG9NAqtOV2A3wMyghqkVPNDP3Aqq2BYfkcn4va3RNAYxNNVE84JJ0H3jyPDXhMBlQU6vQn
1NAgMBGjggEXMIIBEzARBglghkgBhvhCAQEEBApqlSai4mfuvjh02SQMNDAgTwMB8GA1UdI
QYMBaEd38IK05AHreiU9OYc6v+ENMOwZMIGsBgNVHR8EgaQwgaEwb6BuGaWxkYXA6Lyht74
tpbmcmVkLmlwbGFuZXQuY29tL1VJRD1DZXJ0aWZpY2F0ZSBNYW5hZ2V9VPVBlb3BsZSxPPW
1haWxT9jZXJ0aWZpY2jdu2medXRllHjkghytQURYFNrkuoCygKoYoaHDovL3Bla2kghytQU
luZy5WQuaXBsYW5ldC5jb20vcGVraW5nLmNybDAeBgNVHREEFzAVgRNw0aWEuc2hhb0BzdW
4uY29A0GCxLm78UfreCxS3Pp078jyTaDv2ci1AudBL8+RrRUQvxsMJfZD+Uuf10Ilt6kwhm
Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==
```

ldapmodify 命令用于将公共密钥和证书添加到 LDAP 目录中：

```
# ldapmodify -a -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd -v
-f add-public-cert.ldif
```

smime.conf 中 certurl 参数的值指定了公共密钥及其证书在 LDAP 目录中的位置。对于示例 2， certurl 被设置为：

```
certurl==ldap://demo.siroe.com:389/ou=people, o=demo.siroe.com,
o=demo?userCertificate;binary?sub?
```

验证 LDAP 目录中是否存在密钥和证书

以下示例演示了搜索 LDAP 目录以查找 CA 证书和公共密钥及其证书。

搜索一个 CA 证书

在以下示例中，由 -b 选项定义的基本 DN cn=SMIME admin, ou=people,o=demo.siroe.com,o=demo objectclass=* 描述了 LDAP 目录中的一个 CA 证书。如果在目录中找到该证书， ldapsearch 将把关于该证书的信息返回到 ca-cert.lidf 文件中。

```
# ldapsearch -L -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-b "cn=SMIME admin, ou=people,o=demo.siroe.com,o=demo"
"objectclass=*" > ca-cert.ldif
```

以下示例显示了 ca-cert.ldif 文件中的搜索结果。文件内容的格式是使用 ldapsearch 的 -L 选项的结果。

```
# more ca-cert.ldif
dn: cn=SMIME admin,ou=people,o=demo.siroe.com,o=demo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: certificationAuthority
cn: RootCACerts
cn: SMIME admin
sn: CA
authorityRevocationList: novalue
certificateRevocationList: novalue
cacertificate;binary:: MFU01JTUUxEjAQBgNVBAsTCU1zZNlcnZlcjcMBoGA1UEAxMTydG
 QGEwJVEOMAwGA1UEChMFU0UUxEjAQBgNVBAsTCU1zZ1NlcnZlcjEcMBoGA1UEAxMTQ2VydG
 aFw0jAxMTIwODAwMDBaM267X9FExCzAJBgwyrjgNVBAk9STklBMQwwCgYDVQQVHR8EgaQwg
 YlVzMRMwEQYDVQQIEwpDQUx9STklBMQwwCgYDVQQKEwww3ltgoOYz11lzAdBgNVBpYSE9Vc
 5yQuaddiiWlm899XBsYW5ljb20wgZ8wDQYJoGBAK1mUTy8vvO2nOFg4mlHjkghytQUR1k8l
 5mcWRfL77ntm5mGXRD3XMciUq6zUfIg3ngvxlLKLyERTIqjUS8HQU4R5pvj+rrVgsAGjggE
 +FNAJmqtOV2A3wMyghqkDP3Aqq2BYfkcn4va3C5nRNAYxNNVE84JJ0H3jyPDXhMBlQU6vQn
 1NABAAGjggEXMIIBEzglghkgBhvhCAQEEBApqlSai4mfuvjh02SQkoPMNDAgTwMB8GA1UdI
 QYMAFEd38IK05AHreOYc6v+ENMOwZMIGsBgNVHR8EgaQwgaEwb6BtoGuGaWxkYXA6Lyht74
 tpbucmVkLmlwbGFuZY29tL1VJRD1DZXJ0aWZpY2F0ZSBNYW5hZ2VyLE9VPVBlb3BsZSxPPW
 1haWYT9jZXJ0aWZpdu2medXRllHjkghytQURYFNrkuoCygKoYoaHR0cDovL3Bla2kghytQU
 luZyZWQuaXBsYW5ldb20vcGVraW5nLmNybDAeBgNVHREEFzAVgRNwb3J0aWEuc2hhb0BzdW
 4uYtMA0GCxLm78Ufre3Pp078jyTaDv2ci1AudBL8+RrRUQvxsMJfZeFED+Uuf10Ilt6kwhm
 Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==
```

搜索多个公共密钥

在以下示例中，由 -b 选项定义的基本 DN o=demo.siroe.com,o=demo objectclass=* 将把在 LDAP 目录中找到的、位于此基本 DN 上以及此基本 DN 下面的所有公共密钥和证书返回到 usergroup.ldif 文件中：

```
#ldapsearch -L -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-b "o=demo.siroe.com,o=demo" "objectclass=*" > usergroup.ldif
```

搜索一个公共密钥

在以下示例中，由 -b 选项定义的基本 DN uid=JohnDoe, ou=people,o=demo.siroe.com,o=demo objectclass=* 描述了 LDAP 目录中的一个公共密钥及其证书：

```
# ldapsearch -L -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-b "uid=JohnDoe, ou=people,o=demo.siroe.com,o=demo" "objectclass=*" >
public-key.ldif
```

以下示例显示了 public-key.ldif 文件中的搜索结果。文件内容的格式是使用 ldapsearch 的 -L 选项的结果。

```
# more public-key.ldif
dn: uid=sdemo1, ou=people, o=demo.siroe.com, o=demo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: siroe-am-managed-person
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: userPresenceProfile
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: icsCalendarUser
objectClass: sunUCPreferences
mail: JohnDoe@demo.siroe.com
mailHost: demo.siroe.com
.
.
uid: JohnDoe
.
.
```

```
mailUserStatus: active
inetUserStatus: active
.
.
usercertificate;binary:: MFU01JTUUxEjAQBgNBAsTCU1zZ1NlcnZjcMBoGA1UEAxMTydG
QGEwJEOwGA1UEChMFU01JTUUxEjAQBgNVBAsTCU1zZ1NlcnZlcjEcMBoGA1UEAxMTQ2VydG
aFw0MTIwODAwMDBaM267hgbX9FExCzAJBgwyrjgNVBAk9STklBMQwwCgYDVQQVHR8EgaQwg
YTAlVEQYDVQQIEwpDQUxJRk9STklBMQwwCgYDVQQKEwww3ltgoOYz11lzAdBgNVBpYSE9Vc
5yZWQdWlm899XBsYW5ldC5jb20wgZ8wDQYJoGBAK1mUTy8vvO2nOFg4mlHjkghytQUR1k8l
5mvgc7ntm5mGXRD3XMU4OciUq6zUfIg3ngvxlLKLyERTIqjUS8HQU4R5pvj+rrVgsAGjggE
+FG9NmV2A3wMyghqkVPNDP3Aqq2BYfkcn4va3C5nRNAYxNNVE84JJ0H3jyPDXhMBlQU6vQn
1NAgMAgEXMIIBEzARBglghkgBhvhCAQEEBApqlSai4mfuvjh02SQkoPMNDAgTwMB8GA1UdI
QYMBaEdK05AHreiU9OYc6v+ENMOwZMIGsBgNVHR8EgaQwgaEwb6BtoGuGaWxkYXA6Lyht74
tpbucmVkwbGFuZXQuY29tL1VJRD1DZXJ0aWZpY2F0ZSBNYW5hZ2VyLE9VPVBlb3BsZSxPPW
1haxYT9jZaWZpY2jdu2medXRllHjkghytQURYFNrkuoCygKoYoaHR0cDovL3Bla2kghytQU
luZyZWQuaYW5ldC5jb20vcGVraW5nLmNybDAeBgNVHREEFzAVgRNwb3J0aWEuc2hhb0BzdW
4u9tMA0GC78UfreCxS3Pp078jyTaDv2ci1AudBL8+RrRUQvxsMJfZeFED+Uuf10Ilt6kwhm
Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==
.
.
```

网络安全服务证书

用于网络安全服务 (NSS) 的各种证书存储在其各自的数据库中，而不是存储在 LDAP 数据库中。 Messaging Server 提供了两个实用程序 `certutil` 和 `crlutil`，用于将证书及相关 CRL 存储到数据库中。您还可以使用这些实用程序来搜索数据库。

有关 `certutil` 的更多信息，请参见 Sun Java System Directory Server 管理指南 (http://docs.sun.com/doc/819-2013)。有关该实用程序的更多信息，请使用 `crlutil` 附带的帮助文本 （要查看这两个实用程序的联机帮助，请在不使用参数的情况下执行这两个实用程序）。

Communications Express S/MIME 最终用户信息

本节包含适用于最终用户的信息。它包含以下几个小节：

- 第 640 页的 “首次登录”
- 第 641 页的 “签名和加密设置”
- 第 642 页的 “启用 Java 控制台”

首次登录

邮件用户首次登录 Communications Express Mail 时，用户将会收到与 S/MIME applet 相关的特殊提示。

Windows 的提示

在 Windows 98、 2000 或 XP 上首次登录到 Communications Express Mail 时，系统将显示以下提示：

1. 如果您的计算机 （客户机）中未安装 Java 2 Runtime Environment (JRE)，您将收到类似下面内容的提示：

   ```
   Do you want to install and run "Java Plug-in 1.4.2_03 signed on 11/20/03
   and distributed by Sun Microsystems, Inc."?
   Publisher authenticity verified by: VeriSign Class 3 Code Signing 2001
   CA
   ```

   单击 “是”，然后按照后续提示安装 JRE。

注 如果需要英文语言支持并且还需要阅读包含非拉丁字符 （例如中文）的外来 S/MIME 邮件，则您的计算机的 `/lib` 目录中必须包含 `charsets.jar` 文件。

为确保已将 `charsets.jar` 文件安装到 `/lib` 目录中，请使用自定义安装来安装英语版的 JRE。在安装过程中，请选择 “支持其他语言”选项。

有关更多信息，请参见第 609 页的 “多语言支持”。

   在出现最后一个安装提示时单击 “完成”。重新启动计算机，然后再次登录 Communications Express Mail。

2. 系统将显示一则提示，询问您：

   ```
   Do you want to trust the signed applet distributed by "Sun Microsystems,
   Inc."?
   Publisher authenticity verified by: Thawte Consulting cc
   ```

   单击以下回答之一：

   - “是”，接受 S/MIME applet，以用于此 Communications Express Mail 会话。每次登录时都会显示此提示。
   - “否”，拒绝 S/MIME applet。您将不能使用 S/MIME 功能。

- “始终”，接受 S/MIME applet，以将其用于此 Communications Express Mail 会话及所有后续 Communications Express Mail 会话。您将不会再看到此提示。

3. 系统将显示一则提示，询问您：

```
Do you want to trust the signed applet distributed by "sun microsystems,
inc."?
Publisher authenticity verified by: VeriSign, Inc.
```

单击以下回答之一：

- “是”，接受 S/MIME applet，以用于此 Communications Express Mail 会话。每次登录时都会显示此提示。
- “否”，拒绝 S/MIME applet。您将不能使用 S/MIME 功能。
- “始终”，接受 S/MIME applet，以将其用于此 Communications Express Mail 会话及所有后续 Communications Express Mail 会话。您将不会再看到此提示。

签名和加密设置

您可以设置初始签名和加密设置，以控制是否所有用户的外发邮件都：

- 自动签名，或
- 自动加密，或
- 自动签名并加密

初始设置还可以控制位于 Communications Express Mail 窗口底部以及 “选项 — 设置”窗口中的签名和加密复选框是显示为选中 （功能已启用）状态，还是显示为未选中 （功能已禁用）状态。为未选中 （功能已禁用）状态。使用 `smime.conf` 文件中的 `alwaysencrypt` 和 `alwayssign` 参数可以指定初始设置。

让您的邮件用户知道他们可以更改其邮件的初始设置。登录到 Communications Express Mail 后，用户可以暂时覆盖一个邮件的设置，或在持续进行的基础上覆盖所有邮件的设置。

表 20-6 概括了各个复选框的用法。

表 20-6 Communications Express Mail 的签名和加密复选框

复选框文本	位置	Communications Express Mail 用户执行的操作
在邮件中签名	位于 Communications Express Mail 窗口的底部，用于撰写、转发或回复邮件。	• 选中此框将对当前邮件进行签名。 • 取消选中此框将不对当前邮件进行签名。
对邮件进行加密	位于 Communications Express Mail 窗口的底部，用于撰写、转发或回复邮件。	• 选中此框将对当前邮件进行加密。 • 取消选中此框将不对当前邮件进行加密。
在所有外发邮件中签名	位于 Communications Express Mail 的“选项 — 设置”窗口中的“安全传送邮件”选项下。	• 选中此框将自动对所有邮件进行签名。 • 取消选中此框则不会自动对所有邮件进行签名。 注意：您可以使用“在邮件中签名”复选框在逐个处理邮件的基础上覆盖“在所有外发邮件中签名”的设置。
对所有外发邮件加密	位于 Communications Express Mail 的“选项 — 设置”窗口中的“安全传送邮件”选项下。	• 选中此框将自动对所有邮件进行加密。 • 取消选中此框则不会自动对所有邮件进行加密。 注意：您可以使用“对邮件进行加密”复选框在逐个处理邮件的基础上覆盖“对所有外发邮件加密”的设置。

启用 Java 控制台

当 Communications Express Mail 用户处理签名和加密邮件时， S/MIME applet 可以将各种操作消息写入 Java 控制台。在对邮件用户报告的问题进行错误诊断时，Java 控制台消息可能会很有用。但是，仅当通过将 `nswmExtendedUserPrefs` 属性添加到 LDAP 条目的 `inetMailUser` 对象类中从而为用户启用 Java 控制台时，才会生成操作消息。例如：

```
nswmExtendedUserPrefs:meSMIMEDebug=on
```

请不要始终对所有邮件用户都启用 Java 控制台，因为这样做会明显降低 Communications Express Mail 的性能。

第 21 章

管理日志记录

本章提供了用于 Messaging Server MTA、邮件存储和服务的日志记录工具的概述信息。本章还提供了管理这些日志记录工具的过程。

本章包含以下各节：

- 日志记录概述
- 管理日志记录的工具
- 管理 MTA 邮件和连接日志
- 管理服务日志

日志记录概述

日志记录是使系统提供有关系统服务的时间戳和标记信息的一种方法。日志记录提供了系统的当前快照和历史视图。

通过了解和使用 Messaging Server 日志文件，您可以：

- 收集邮件统计信息，例如，邮件大小、邮件传送速率和通过 MTA 的邮件数量
- 执行趋势确定
- 关联到容量规划
- 对问题进行错误诊断

例如，如果您的站点由于用户数量的增加需要添加更多的磁盘存储空间，您可以使用 Messaging Server 日志文件来查看系统需求已增加的百分比，然后规划所需的新磁盘存储量。

您还可以使用 Messaging Server 日志来了解一天的邮件传送模式情况。了解每日高峰负载出现的时间将有助于您进行容量规划。

日志记录还有助于对用户问题进行错误诊断。例如，如果某用户没有收到预期的邮件，您可以使用 Messaging Server 日志记录工具来跟踪该用户的邮件。执行此操作时，您可能会发现这些邮件没有到达是因为它们被自动过滤并发送到 SPAM 文件夹中。

日志记录数据的类型

一般情况下，日志记录提供两种类型的信息：

- 操作数据
- 错误情形，也称作事件日志记录

通常， Messaging Server 日志记录提供操作数据。此操作数据包含的信息有：邮件进入系统的日期和时间；邮件的发件人和收件人；邮件写入磁盘的时间；以后，邮件从磁盘删除的时间和插入用户邮箱的时间。

但是， Messaging Server 日志记录还提供某些事件日志记录数据。要获得事件日志记录数据，您需要将来自不同日志文件的多个项目组合到一起。然后，您可以使用一个特殊的常数 （例如，邮件 ID）来搜索并关联邮件在系统中所经历的生命周期。

Messaging Server 日志文件的类型

Messaging Server 日志记录包含三种类型的日志文件：

1. **MTA 日志**。这些日志为邮件传输代理提供上述操作数据。
2. **错误日志**。这些日志是 MTA 调试日志和 MTA 子组件日志 （即作业控制器、分发程序等）。
3. **邮件存储和服务日志**。这些日志提供来自 HTTP 服务器、 mshttpd、 imap、pop 和 Admin 服务的邮件。这些日志的格式与前两种类型日志的格式不同。

下表列出了日志文件的不同类型。默认情况下，日志文件位于 *msg_svr_base*/data/log 目录中。您可以分别自定义和查看每种日志文件类型。

表 21-1 Messaging Server 日志文件

日志文件的类型	日志文件说明	默认名称
邮件传输代理	显示有关通过 MTA 的邮件通信的信息，其中包括日期和时间信息、入队和出队信息等等。	mail.log、 mail.log_current 或 mail.log_yesterday
连接	包含连接至此系统以发送电子邮件的远程计算机 (MTA)。	connection.log

表 21-1 Messaging Server 日志文件

日志文件的类型	日志文件说明	默认名称
计数器	包含依据在每个通道基础上发送和接收的邮件的邮件趋势。	counters
作业控制器	包含主程序、作业控制器程序、发送器程序和出队列通道程序上的数据。	job_controller.log
分发程序	包含与分发程序相关的错误。打开分发程序调试将增加信息。	dispatcher.log
通道	记录与通道相关的错误。关键字 master_debug 和 slave_debug 可以打开通道调试，这将增加通道日志文件的详细程度。信息的级别和类型由 option.dat 中的各种 *_DEBUG MTA 选项进行控制。	*channelname*_master.log*（示例：tcp_local_master.log*） *channelname*_slave.log*（示例：tcp_local_slave.log*）
Admin	包含与 Console 和 Messaging Server 之间通信 （大多数通过几个 CGI 进程）相关的日志事件，通过其 Administration Server 进行	admin、admin.*sequenceNum.timeStamp*
IMAP	包含与此服务器的 IMAP4 活动相关的日志事件	imap、 imap.*sequenceNum.timeStamp*
POP	包含与此服务器的 POP3 活动相关的日志事件	pop、 pop.*sequenceNum.timeStamp*
HTTP	包含与此服务器的 HTTP 活动相关的日志事件	http、 http.*sequenceNum.timeStamp*
默认值	包含与此服务器的其他活动相关的日志事件，例如命令行实用程序和其他进程	default、default.*sequenceNum.timeStamp*
msgtrace	包含邮件存储的跟踪信息。文件可以快速地增长到非常大，并进行相应监视。	msgtrace
watcher	监视进程故障和未响应服务 （请参见表 4-4 第 101 页），并记录错误消息以表明特定的故障。	watcher

其中：

sequenceNum — 指定一个整数，该整数指定了此日志文件相对于日志文件目录中的其他日志文件的创建顺序。具有较高序列号的日志文件相对于具有较低编号的日志文件而言，属于较新的文件。序列号无法翻滚，而只能在服务器的生命期 （从安装服务器开始）内单调增加。

timeStamp — 指定一个较大整数，它指定了文件创建的日期和时间。（其值以标准 UNIX 时间表示：自 1970 年 1 月 1 日午夜开始的秒数。）

例如，名为 `imap.63.915107696` 的日志文件是指 IMAP 日志文件目录中创建的第 63 个日志文件，创建于 1998 年 12 月 31 日中午 12:34:56。

开放式的序列号与时间戳的组合让您在旋转、终止和选择用于分析的文件时具有了更大的灵活性。有关更为具体的建议，请参见第 672 页的 “定义和设置服务日志记录选项”。

跟踪分布在各种日志文件中的邮件

以下介绍了邮件是如何流经系统的以及在哪些位置将信息写入各种日志文件。此说明有助于您了解如何使用 Message Server 的日志文件来进行错误诊断和解决问题。请参见第 170 页的表 8-2 以跟进。

1. 远程主机与邮件传送主机上的 TCP 插槽建立连接，请求 SMTP 服务。
2. MTA 分发程序将响应该请求，并将连接传递至邮件传送主机的 SMTP 服务。

   MTA 采用模块化设计，它由一组进程组成，其中包括作业控制器和 SMTP 服务分发程序。分发程序接受外来 TCP 连接并将其发送至 SMTP 服务。 SMTP 服务将邮件写入磁盘的通道区。 SMTP 服务了解邮件的信封参数，例如，发件人和收件人。系统中的配置条目将通知它属于哪个目标通道。
3. 分发程序写入 `dispatcher.log` 文件，它分叉了一个线程并使此线程可用于来自某一 IP 地址的外来连接。
4. SMTP 服务器写入其 `tcp_smtp_server.log` 文件，它将记录当远程主机与其建立连接并发送邮件时所发生的情况的对话。分发程序传递至主机 IP 上的 SMTP 服务器时，将创建此日志文件。
5. SMTP 服务器为通道程序 （例如， `tcp_intranet`）将邮件写入磁盘的队列区，并通知作业控制器。
6. 作业控制器联系通道程序。
7. 通道程序传送邮件。

   每个通道均有自己的日志文件。但是，这些日志通常显示通道的开始和停止。要获得更多信息，您需要为通道启用调试级别。但是，由于这会放慢系统速度，而且如果保持打开状态，实际上会使问题更加隐蔽，因此，您应仅当实际问题发生时才启用调试级别。

注 为了高效工作，如果已经为现有进程运行某通道，并且又进入了一个新邮件，系统将不会产生新的通道进程。当前运行的进程将选取该新邮件。

8. 邮件被传送到它的下一个中继站，它可以是另一个主机、另一个 TCP 连接等。在 `connection.log` 文件中写入了此信息。

同时， SMTP 服务器将邮件写入磁盘的队列区，负责该邮件的通道将在 `mail.log_current` 或 `mail.log` 文件中写入记录。此记录显示了诸如邮件入队的日期和时间、发件人和收件人等信息。有关更多信息，请参见第 653 页的“MTA 邮件日志记录示例”。对跟踪邮件来说，最有用的文件是 `mail.log_current` 文件。

管理日志记录的工具

您可以通过使用 Console 和 `configutil` 命令为创建和管理 Messaging Server 日志文件自定义策略。

对于邮件存储日志，您可以使用 Console 来指定日志设置和查看日志。您指定的设置将影响所记录的事件以及事件的数目。分析日志文件时，您可以使用这些设置和其他特性来完善日志事件的搜索。

由于 MTA 使用了独立的日志记录工具，所以您无法使用 Console 来配置 MTA 日志记录服务以及查看日志。而是通过指定配置文件中的信息来配置 MTA 日志记录。

对于超出 Messaging Server 功能范围的日志分析和报告生成，您需要使用其他工具。您可以自行使用文本编辑器或标准系统工具处理日志文件。

使用支持正则表达式分析的可编写文本编辑器，您可以搜索和提取基于本章中讨论的任何标准的日志条目，并可以对结果进行排序，甚至还可以生成总数或其他统计信息。

在 UNIX 环境中，您还可以修改和使用现有报告生成工具，这些工具是为处理 UNIX `syslog` 文件而开发的。如果您希望使用公共域 `syslog` 处理工具，请记住您可能需要修改此工具以解释不同的日期 / 时间格式，以及出现在 Messaging Server 日志条目中但未出现在 `syslog` 条目中的两个附加的组件 （*facility* 和 *logLevel*）。

管理 MTA 邮件和连接日志

MTA 提供了记录每个入队和出队的邮件的功能。还提供了分发程序错误和调试输出。

您可以控制每个通道上的日志记录，也可以指定要记录的所有通道上的邮件活动。在初始配置中，所有通道上均禁用日志记录。

有关更多信息，请参见第 651 页的 “启用 MTA 日志记录”。

启用日志记录使得 MTA 在邮件每次通过 MTA 通道时，都将一个条目写入 *msg_svr_base*/data/log/mail* 文件。这类日志条目对收集有关通过 MTA （或通过特定通道）的邮件数量的统计信息将很有用。您还可以使用这些日志条目来调查其他问题，例如，是否发送或传送了邮件，以及发送或传送邮件的时间。

邮件将返回作业 （每晚午夜时分运行），将所有现有 mail.log_yesterday 都附加到累积日志文件 mail.log，将当前 mail.log_current 文件重命名为 mail.log_yesterday，然后开始一个新的 mail.log_current 文件。邮件返回作业还对所有 connection.log* 文件执行相似的操作。

MTA 执行自动翻滚以保持当前的文件时，您必须通过确定任务 （例如备份文件、截断文件、删除文件等）的策略来管理累积 mail.log 文件。

考虑如何管理日志文件时，请注意 MTA 定期返回作业将执行站点提供的 *msg_svr_base*/bin/daily_cleanup 程序 （如果存在）。因此，某些站点可能选择提供他们自己的清除程序，例如每周重命名一次 （或每月一次）旧的 mail.log 文件等。

注意 启用日志记录后， mail.log 文件将稳定地增长，同时如果不进行检查，将消耗所有可用磁盘空间。监视此文件的大小并定期地删除不必要的内容。按照要求将创建此文件的另一版本时，还可以删除整个文件。

了解 MTA 日志条目格式

MTA 日志文件以 ASCII 文本书写。默认情况下，每个日志文件条目都包含八个或九个字段，如下面示例中所示。

```
19-Jan-1998 19:16:57.64 l tcp_local E 1 adam@sesta.com
 rfc822;marlowe@siroe.com marlowe@siroe.com
```

日志条目显示：

1. 创建条目的日期和时间 （在此示例中为 19-Jan-1998 19:16:57.64）。
2. 源通道的通道名称 （在此示例中为 l）。
3. 目标通道的通道名称 （在此示例中为 tcp_local）。（对于 SMTP 通道，当启用 LOG_CONNECTION 时，加号 (+) 表示入站到 SMTP 服务器；减号 (-) 表示通过 SMTP 客户机出站。）
4. 条目的类型 （在此示例中为 E）；请参见表 21-2 第 649 页。
5. 邮件的大小 （在此示例中为 1）。默认表示为千字节 （使用 MTA 选项文件中的 BLOCK_SIZE 关键字可以更改此默认值）。

6. 信封 From: 地址 （在此示例中为 adam@sesta.com）。请注意带有空信封 From: 地址的邮件 （例如通知邮件），此字段为空白。
7. 信封 To: 地址 （在此示例中为 marlowe@siroe.com）。
8. 信封 To: 地址 （在此示例中为 marlowe@siroe.com）。
9. 传送状态 （仅适用于 SMTP 通道）。

下表说明了日志记录条目代码。

表 21-2 日志记录条目代码

条目	说明
B	发送至 SMTP 服务器的错误命令。收件人地址字段将包含被拒绝的命令，而诊断字段将包含 SMTP 服务器所给出的响应。 MTA 通道选项 (MAX_B_ENTRIES) 用于控制将记录到给定会话中的错误命令的数量。默认值为 10。
BA	验证成功执行后事务中较早的错误命令。
BS	TLS 成功启动后的错误命令。
BSA	TLS 和 AUTH 的错误命令。
D	成功出队列
DA	使用 SASL （验证）成功出队列
DS	使用 TLS （安全）成功出队列
DSA	使用 TLS 和 SASL （安全和验证）成功出队列
E	入队列
EA	使用 SASL （验证）成功入队列
ES	使用 TLS （安全）成功入队列
ESA	使用 TLS 和 SASL （安全和验证）成功入队列
J	拒绝尝试入队列 （被从通道程序拒绝）
K	拒绝收件人邮件。如果发件人请求 NOTIFY=NEVER DSN 标志设置、如果邮件超时或者如果手动返回邮件 （例如， imsimta qm "delete" 命令往往为每个收件人生成 "K" 记录，而 qm "return" 命令则生成 "K" 记录而非 "R" 记录），系统均将拒绝收件人邮件。这表示不会根据发件人自己的请求向发件人发送通知。 与 “K” 记录相比，“R” 记录也为相同的拒绝 / 超时类型，但在 “R” 记录中系统会根据失败邮件产生一封新的通知邮件 （返回给初始发件人）。
Q	出队列临时故障
R	尝试出队列时收件人地址被拒绝 （被主通道程序拒绝），或生成故障 / 弹回邮件
W	发送的警告消息以通知原发件人邮件尚未发送，但仍在重试的队列中。

表 21-2 日志记录条目代码

条目	说明
Z	已成功发送给一些收件人，但临时未成功发送给此收件人；所有收件人的原邮件文件已出队，并在该位置排入此收件人和其他未成功发送的收件人的新邮件文件
SMTP 通道的 LOG_CONNECTION + 或 - 条目	
C	已关闭连接。将出现诊断字段。写入 connection.log_current （或者如果使用了单个日志文件，则写入 mail.log_current）。用于记录关闭连接的原因。尤其是，如果关闭连接是由于达到了某些会话断开连接限制，则诊断字段中将显示此事实。
O	已打开连接
U	记录 SMTP 验证的成功信息和失败信息。格式与其他 O 和 C 条目相同。尤其是，相同的应用程序和传输信息字段以相同的顺序显示。如果已知用户名，则它将记录在用户名字段中。 LOG_CONNECTION MTA 选项的位 7 （值 128）将控制此过程。
X	已拒绝连接
Y	建立连接之前尝试连接失败
I	已收到 ETRN 命令

LOG_CONNECTION、 LOG_FILENAME、 LOG_MESSAGE_ID、 LOG_NOTARY、 LOG_PROCESS 和 LOG_USERNAME 在 MTA 选项文件中全部启用后，格式将发生变化，如下面示例中所示。（此样例日志条目行已因版式原因而换行；实际日志条目将显示在一个物理行。）

```
19-Jan-1998 13:13:27.10 HOSTA   2e2d.2.1 tcp_local   l
 E 1 service@siroe.com rfc822;adam@sesta.com
 adam 276 /imta/queue/l/ZZ01IWFY9ELGWM00094D.00
 <01IWFVYLGTS499EC9Y@siroe.com> inetmail
 siroe.com (siroe.com [192.160.253.66])
```

除了上面已讨论的那些字段外，其中的附加字段是：

1. 运行通道进程的节点的名称 （在本示例中为 HOSTA）。
2. 进程 ID （以十六进制表示），其后是句号 （点）字符和计数。如果这是多线程通道条目 （即， tcp_* 通道条目），则在进程 ID 和计数之间还会显示线程 ID。在本示例中，进程 ID 是 2e2d.2.1。

3. 邮件的 NOTARY （传送收件人请求）标志，表示为整数 （在本示例中为 276）。
4. MTA 队列区域中的文件名 （在本示例中为 /imta/queue/l/ZZ01IWFY9ELGWM00094D.00）。
5. 邮件 ID （在本示例中为 <01IWFVYLGTS499EC9Y@siroe.com>）。
6. 正在执行的进程的名称 （在本示例中为 inetmail）。在 UNIX 上，对于分发程序进程 （例如 SMTP 服务器），此名称通常为 inetmail （除非已使用 SASL）。
7. 连接信息 （在本示例中为 siroe.com (siroe.com [192.160.253.66])）。连接信息由发送系统或通道名称组成，例如由 HELO/EHLO 线路上的发送系统表示的名称 （对于外来 SMTP 邮件），或入队通道的官方主机名 （对于其他类型的通道）。对于 TCP/IP 通道，发送系统的 “真实” 名称 （即由 DNS 反向查找和 / 或 IP 地址报告的符号名称）也可被报告在由 ident* 通道关键字控制的括号内；请参见第 311 页的 “IDENT 查找”。此样例假定使用这些关键字的其中一个，例如使用默认的 identnone 关键字 （用于选择显示在 DNS 和 IP 地址中找到的两个名称）。

启用 MTA 日志记录

要仅收集几个特定 MTA 通道的统计信息，请仅启用感兴趣的那些 MTA 通道上的日志记录通道关键字。许多站点倾向于启用所有 MTA 通道上的日志记录。特别是，如果您要尝试跟踪问题，诊断某些问题的第一步是注意到邮件未进入您期望或想要的通道，启用所有通道的日志记录将有助于您调查此类问题。

➤ 在特定通道上启用 MTA 日志记录

1. 编辑 imta.cnf 文件。

   该文件位于 /opt/SUNWmsgsr/config 目录中。

2. 要为特定通道启用日志记录，请将 logging 关键字添加到通道定义中。例如：

   channel-name keyword1 keyword2 **logging**

此外，您还可以设置一些配置参数，例如日志文件的目录路径、日志级别等等。请参见第 669 页的 “管理服务日志”。

➤ **在所有通道上启用 MTA 日志记录**

1. 编辑 `imta.cnf` 文件。

   该文件位于 `/opt/SUNWmsgsr/config` 目录中。

2. 将 `logging` 关键字添加到 MTA 配置文件的通道块区域的 `defaults` 通道 （请参见第 298 页的 “配置通道默认值”）中。例如：

```
defaults logging notices 1 2 4 7 copywarnpost copysendpost postheadonly
noswitchchannel immnonurgent maxjobs 7 defaulthost siroe.com


l defragment charset7 us-ascii charset8 iso-8859-01
siroe.com
```

指定附加 MTA 日志记录选项

除了启用日志记录时通常提供的基本信息之外，您还可以通过设置 MTA 选项文件中的各种 `LOG_*` MTA 选项来指定要包含的附加、可选信息字段。用 IMTA 调整文件 (*msg_svr_base*`/config/imta_tailor`) 中的 `IMTA_OPTION_FILE` 选项指定的文件将指定 MTA 选项文件。默认情况下，它是 *msg_svr_base*`/config/option.dat` 文件。

有关 MTA 选项文件的完整详细信息，请参见位于 `http://docs.sun.com/doc/819-0106` 的 Sun Java System Messaging Server Reference

➤ **向系统日志发送 MTA 日志**

1. 编辑 MTA 选项文件。
2. 将 `LOG_MESSAGES_SYSLOG` 选项设置为 1。

   0 值为默认值并表示未执行系统日志 （事件日志）记录。

➤ **与日志邮件条目相关联**

1. 编辑 MTA 选项文件。
2. 将 `LOG_MESSAGE_ID` 选项设置为 1。

   0 值为默认值并表示邮件 ID 未保存在 `mail.log` 文件中。

➤ **标识邮件传送重试**

1. 编辑 MTA 选项文件。

2. 将 LOG_FILENAME 选项设置为 1。

   此选项便于立即发现特定邮件文件传送的重试次数。此选项在了解 MTA 是否将传送给多个收件人的邮件分割为磁盘上独立的邮件文件副本时也会很有用。

➤ **记录 TCP/IP 连接**

1. 编辑 MTA 选项文件。
2. 设置 LOG_CONNECTION 选项。

   此选项可使 MTA 记录 TCP/IP 连接以及邮件通信流量。默认情况下，系统将连接日志条目写入 mail.log* 文件。可选地，连接日志条目可以被写入 connection.log* 文件。有关更多信息，请参见 SEPARATE_CONNECTION_LOG 选项。

➤ **将条目写入 connection.log 文件**

1. 编辑 MTA 选项文件。
2. 将 SEPARATE_CONNECTION_LOG 选项设置为 1。

   使用此选项来指定将连接日志条目写入 connection.log 文件中。默认值 0 将导致连接日志记录存储在 MTA 日志文件中。

➤ **通过进程 ID 与日志邮件相关联**

1. 编辑 MTA 选项文件。
2. 设置 LOG_PROCESS 选项。

   与 LOG_CONNECTION 结合使用时，此选项启用连接条目与对应的邮件条目通过进程 ID 相关联。

➤ **将与使邮件入队的进程关联的用户名保存在 mail.log 文件中**

1. 编辑 MTA 选项文件。
2. 设置 LOG_USERNAME 选项。

   此选项控制是否将与使邮件入队的进程关联的用户名保存在 mail.log 文件中。对于使用了 SASL (SMTP AUTH) 的 SMTP 提交，用户名字段将是经过验证的用户名 （带有星号字符前缀）。

MTA 邮件日志记录示例

记录在 MTA 邮件文件中的确切字段格式和字段列表将根据设置的日志记录选项而有所不同。本节将描述一些解释典型日志条目类别的示例。有关附加、可选字段的说明，请参见第 652 页的 “指定附加 MTA 日志记录选项”。

注 由于版式原因，日志文件条目被折叠成多行显示 — 实际日志文件条目是每个条目一行。

查看日志文件时，请记住在典型系统上会一次处理多封邮件。通常，与特定邮件相关的条目将散布在与其他同时正在处理的邮件相关的条目中。基本日志记录信息适用于收集通过 MTA 移动的邮件总体数目。

如果您希望将与同一邮件相关的特定条目和相同的收件人相关联，则启用 LOG_MESSAGE_ID。要将特定邮件与 MTA 队列区域中的特定文件相关联，或从条目查看已尝试传送特定的尚未成功出队列的邮件的次数，请启用 LOG_FILENAME。对于 SMTP 邮件 （通过 TCP/IP 通道处理），如果将 TCP 连接与已发送邮件的远程系统相互关联，则启用 LOG_PROCESS 和 LOG_CONNECTION 的某一级别。

MTA 日志记录示例：用户发送外发邮件

下面的示例显示了如果本地用户通过外发 TCP/IP 通道发送邮件 （例如发送到 Internet），而可能看到的日志条目类别的相当基本的示例。在本示例中，启用了 LOG_CONNECTION。标有 (1) 和 (2) 的行是一个条目 — 它们在实际日志文件中将显示为一个物理行。类似地，标有 (3) - (7) 的行是一个条目并将显示为一个物理行。

代码示例 21-1 日志记录：本地用户发送外发邮件

```
19-Jan-1998 19:16:57.64 l            tcp_local    E 1 (1)
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com (2)

19-Jan-1998 19:17:01.16 tcp_local                  D 1 (3)
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com (4)
 dns;thor.siroe.com
 (TCP|206.184.139.12|2788|192.160.253.66|25) (5)
 (THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694]) (6)
 smtp;250 2.1.5 marlowe@siroe.com and options OK. (7)
```

1. 此行显示了一 (1) 块邮件从 l 通道到 tcp_local 通道入队列 (E) 的日期和时间。
2. 这是与 (1) 位于同一日志文件物理行的一部分，因排版方便而在此处分行显示。显示了信封 From: 地址 （在本例中为 adam@sesta.com）以及原始版本和当前版本的信封 To: 地址 （在本例中为 marlowe@siroe.com）。
3. 显示了一 (1) 块邮件从 tcp_local 通道出队列 (D) 的日期和时间 — 即，由 tcp_local 通道成功发送到某一远程 SMTP 服务器。

4. 显示了信封 From: 地址、原始信封 To: 地址和信封 To: 地址。
5. 显示了连接到 DNS 中的名为 thor.siroe.com 的实际系统，本地发送系统具有 IP 地址 206.184.139.12 并从端口 2788 发送，远程目标系统具有 IP 地址 192.160.253.66 并且远程目标系统的连接端口是端口 25。
6. 显示了远程 SMTP 服务器的 SMTP 标志行。
7. 显示了返回的此地址的 SMTP 状态代码； 250 是基本的 SMTP 成功代码，而此远程 SMTP 服务器使用扩展的 SMTP 状态代码和某一附加文本进行响应。

MTA 日志记录示例：可选日志记录字段

代码示例 21-2 显示了类似于代码示例 21-3 中所示的日志记录条目，但通过设置 LOG_FILENAME=1 和显示文件名和邮件 ID 的 LOG_MESSAGE_ID=1 记录了附加信息；请参见 (1) 和 (2)。特别是邮件 ID 可用于将条目与邮件相关联。

代码示例 21-2 日志记录：包括可选日志记录字段

```
19-Jan-1998 19:16:57.64 l            tcp_local    E 1
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
 /imta/queue/tcp_local/ZZ01ISKLSKLZLI90N15M.00
   <01ISKLSKC2QC90N15M@sesta.com> (1)

19-Jan-1998 19:17:01.16 tcp_local                 D 1
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
 /imta/queue/tcp_local/Z01ISKLSKLZLI90N15M.00
   <01ISKLSKC2QC90N15M@sesta.com> (2)
 dns;thor.siroe.com (TCP|206.184.139.12|2788|192.160.253.66|25)
 (THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694])
 smtp;250 2.1.5 marlowe@siroe.com and options OK.
```

MTA 日志记录示例：发送到列表

代码示例 21-3 第 656 页 对启用 LOG_FILENAME=1、 LOG_MESSAGE_ID=1 和 LOG_CONNECTION=1 将邮件发送给多个收件人进行了说明。此处已将用户 adam@sesta.com 发送给 MTA 邮递列表 test-list@sesta.com，此邮递列表已扩展到 bob@sesta.com、 carol@varrius.com 和 david@varrius.com。请注意每个收件人的原始信封 To: 地址是 test-list@sesta.com，尽管当前信封 To: 地址是每个收件人各自的地址。请注意邮件 ID 是如何一致的，尽管涉及了两个单独的文件 （一个用于 l 通道而另一个用于出 tcp_local 通道）。

代码示例 21-3 日志记录：发送到列表

```
19-Jan-1998 20:01:44.10 l    l            E 1
 adam@sesta.com rfc822;test-list@sesta.com bob
 imta/queue/l/ZZ01ISKND3DE1K90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:44.81 l            tcp_local    E 1
 adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:44.81 l            tcp_local    E 1
 adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:50.69 l                         D 1
 adam@sesta.com rfc822;test-list@sesta.com bob
 imta/queue/l/ZZ01ISKND3DE1K90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:57.36 tcp_local                  D 1
 adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>
 dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
 (gw.varrius.com -- SMTP Sendmail)
 smtp;250 OK.

19-Jan-1998 20:02:06.14 tcp_local                  D 1
 adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>
 dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
 (gw.varrius.com -- SMTP Sendmail)
 smtp;250 OK.
```

MTA 日志记录示例：发送至不存在的域

代码示例 21-4 第 658 页 对尝试发送到不存在的域（此处为 `very.bogus.com`）进行了说明；即，发送到未由 MTA 的重写规则发现其不存在的，并且 MTA 与外发 TCP/IP 通道相匹配的域名。此示例假定了 MTA 选项设置 `LOG_FILENAME=1` 和 `LOG_MESSAGE_ID=1`。

TCP/IP 通道在 DNS 中运行并检查域名时， DNS 返回一个错误，指示该名称不存在。请注意 “拒绝”条目 (R) （如 [5] 中所示），同时 DNS 返回错误，指示该域名是非法域名 （如 [6] 中所示）。

由于提交邮件后地址被拒绝， MTA 将生成弹回信息给原发送人。 MTA 将新拒绝邮件入队给原发送人 (1)，并在删除原出站邮件 （(5) 中所示的 R 条目）之前，将一份副本发送给邮寄主管 (4)。

通知邮件 （例如弹回邮件）具有空信封 From: 地址 — 例如，如 (2) 和 (8) 中所示 — 其中信封 From: 字段显示为空白。由 MTA 生成的弹回邮件的初始排队显示了新通知邮件的邮件 ID 和紧随其后的原始邮件的邮件 ID (3)。（此类信息对于 MTA 不是总可以使用，但可用于记录时，它允许对应于出站失败的邮件的日志条目与对应于结果通知邮件的日志条目相关联。）此类通知邮件入队到进程通道，该通道转而又将这些邮件排队到相应的目标通道 (7)。

代码示例 21-4 日志记录：发送到不存在的域

```
19-JAN-1998 20:49:04 l            tcp_local    E 1
 adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
 imta/queue/tcp_local/ZZ01ISKP0S0LVQ94DU0K.00
 <01ISKP0RYMAS94DU0K@SESTA.COM>

19-JAN-1998 20:49:33 tcp_local    process      E 1              (1)
 rfc822;adam@sesta.com adam@sesta.com                          (2)
 imta/queue/process/ZZ01ISKP0S0LVQ94DTZB.00
 <01ISKP22MW8894DTAS@SESTA.COM>,<01ISKP0RYMAS94DU0K@SESTA.COM>  (3)

19-JAN-1998 20:49:33 tcp_local    process      E 1              (4)
 rfc822;postmaster@sesta.com postmaster@sesta.com
 imta/queue/process/ZZ01ISKP0S0LVQ94DTZB.00
 <01ISKP22MW8894DTAS@SESTA.COM>,<01ISKP0RYMAS94DU0K@SESTA.COM>

19-JAN-1998 20:50:07 tcp_local                  R 1              (5)
 adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
 imta/queue/tcp_local/ZZ01ISKP0S0LVQ94DU0K.00
 <01ISKP0RYMAS94DU0K@SESTA.COM>
 Illegal host/domain name found                                (6)

19-JAN-1998 20:50:08 process      l            E 3              (7)
 rfc822;adam@sesta.com adam                                    (8)
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:08 process      l            E 3
 rfc822;postmaster@sesta.com postmaster
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:12 l                         D 3
 rfc822;adam@sesta.com adam
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:12 l                         D 3
 rfc822;postmaster@sesta.com postmaster
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SIROE.COM>
```

MTA 日志记录示例：发送至不存在的远程用户

代码示例 21-5 第 660 页对尝试发送到远程系统上的错误地址进行了说明。此示例假设 MTA 选项设置为 LOG_FILENAME=1 和 LOG_MESSAGE_ID=1，通道选项设置为 LOG_BANNER=1 和 LOG_TRANSPORTINFO=1。请注意拒绝条目 (R)，如 (1) 中所示。但与代码示例 21-4 第 658 页中的拒绝条目不同，请注意此处的拒绝条目显示了已建立到远程系统的连接，并显示了远程 SMTP 服务器发布的 SMTP 错误代码，(2) 和 (3)。(2) 中所示的信息是设置通道选项 LOG_BANNER=1 和 LOG_TRANSPORTINFO=1 的结果。

代码示例 21-5 日志记录：发送给不存在的远程用户

```
20-JAN-1998 13:11:05 l            tcp_local    E 1
 adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
 imta/queue/tcp_local/ZZ01ISLNBB1JOE94DUWH.00
 <01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:08 tcp_local    process      E 1
 rfc822;adam@sesta.com adam@sesta.com
 imta/queue/process/ZZ01ISLNBB1JOE94DSGB.00
 <01ISLNBFKIDS94DUJ8@sesta.com>,<01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:08 tcp_local    process      E 1
 rfc822;postmaster@sesta.com postmaster@sesta.com
 imta/queue/process/ZZ01ISLNBB1JOE94DSGB.00
 <01ISLNBFKIDS94DUJ8@sesta.com>,<01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:11 tcp_local                 R 1      (1)
 adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
 imta/queue/tcp_local/ZZ01ISLNBB1JOE94DUWH.00
 <01ISLNBAWV3094DUWH@sesta.com>
 dns;thor.siroe.com
 (TCP|206.184.139.12|2788|192.160.253.66|25)            (2)
 (THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694])
 smtp; 553 unknown or illegal user:nonesuch@siroe.com   (3)

20-JAN-1998 13:11:12 process      l            E 3
 rfc822;adam@sesta.com adam
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:12 process      l            E 3
 rfc822;postmaster@sesta.com postmaster
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:13 l                         D 3
 rfc822;adam@sesta.com adam@sesta.com
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:13 l                         D 3
 rfc822;postmaster@sesta.com postmaster@sesta.com
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>
```

MTA 日志记录示例：拒绝远程端提交邮件的尝试

代码示例 21-6 对当 MTA 拒绝远程端提交邮件的尝试时所产生的日志文件条目进行了说明。（本示例假设未启用 LOG_* 可选项，因此条目中仅记录了基本字段。请特别注意，启用 LOG_CONNECTION 选项将导致在此类 J 条目中产生附加信息字段。）在此例中，示例是对已设置 SMTP 中继阻塞 （请参见第 472 页的 “配置 SMTP 中继阻止”）的 MTA 而言的，带有 ORIG_SEND_ACCESS 映射，该映射包括：

```
ORIG_SEND_ACCESS

!...numerous entries omitted...
!
   tcp_local|*|tcp_local|*   $NRelaying$ not$ permitted
```

其中 alan@very.bogus.com 不是内部地址。因此远程用户 harold@varrius.com 尝试通过 MTA 系统中继到远程用户 alan@very.bogus.com 遭到拒绝。

代码示例 21-6 日志记录：拒绝远程端提交邮件的尝试

```
28-May-1998 12:02:23 tcp_local                J 0          (1)
 harold@varrius.com rfc822; alan@very.bogus.com             (2)
 550 5.7.1 Relaying not permitted:alan@very.bogus.com       (3)
```

1. 此日志显示了 MTA 拒绝远程端提交邮件的尝试的日期和时间。拒绝由 J 记录表示。（MTA 通道尝试发送邮件而被拒绝的例子以 R 记录表示，如代码示例 21-4 和代码示例 21-5 所示）。

注 写入日志的最后一个 J 记录将有一个指示，用于声明它是给定会话的最后一个 J 记录。此外， Messaging Server 的当前版本没有对 J 记录的数量做出限制。

2. 显示了尝试的信封 From: 和 To: 地址，地址。在此示例中，无可用的原始信封 To: 信息，因此该字段为空。
3. 此条目包括 MTA 发给远程端 （尝试的发件人）的 SMTP 错误消息。

MTA 日志记录示例：多次传送尝试

代码示例 21-7 对在第一次尝试时不能发送邮件所产生的日志文件条目进行了说明，因此 MTA 将多次尝试发送该邮件。本示例假设选项设置为 LOG_FILENAME=1 和 LOG_MESSAGE_ID=1。

代码示例 21-7 日志记录：多次传送尝试

```
15-Jan-1998 10:31:05.18 tcp_internal   tcp_local   E 3     (1)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZZ01IS3D2ZP7FQ9UN54R.00
 <01IRUD7SVA3Q9UN2D4@sesta.com>

15-Jan-1998 10:31:10.37 tcp_local                 Q 3     (2)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZZ01IS3D2ZP7FQ9UN54R.00             (3)
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 TCP active open:Failed connect()    Error:no route to host (4)

 ...several hours worth of entries...

15-Jan-1998 12:45:39.48 tcp_local                 Q 3     (5)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZY01IS3D2ZP7FQ9UN54R.00              (6)
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 TCP active open:Failed connect()    Error:no route to host

 ...several hours worth of entries...

15-Jan-1998 16:45:24.72 tcp_local                 Q 3
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZX01IS67NY4RRK9UN7GP.00               (7)
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 TCP active open:Failed connect() Error:connection refused (8)

 ...several hours worth of entries...

15-Jan-1998 20:45:51.55 tcp_local                 D 3     (9)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZX01IS67NY4RRK9UN7GP.00
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 dns;host.some.org (TCP|206.184.139.12|2788|192.1.1.1|25)
 (All set, fire away)
 smtp; 250 Ok
```

1. 邮件进入 `tcp_internal` 通道 — 可能来自 POP 或 IMAP 客户机，或可能来自使用 MTA 作为 SMTP 中继的组织中的其他主机； MTA 将其排队到 `tcp_local` 外发通道。
2. 第一次传送尝试失败，由 Q 条目表示。
3. 从 `ZZ*` 文件名可以看出这是第一次传送尝试。

4. TCP/IP 软件包找不到至远程端的路由时，此传送尝试将失败。与代码示例 21-4 第 658 页 不同，DNS 并非针对目标域名 some.org；相反，"no route to host" 错误表示在发送端和接收端之间存在网络问题。
5. 下一次 MTA 定期作业运行时，它重新尝试传送，再次不成功。
6. 此文件名现在是 ZY*，表示这是第二次尝试。
7. 第三次未成功的尝试的文件名是 ZX*。
8. 下一次周期性作业重新尝试传送，传送失败，尽管这一次 TCP/IP 软件包未对无法进入远程 SMTP 服务器表示不满，但其实是远程 SMTP 服务器不接受连接。（可能远程端修复了其网络问题，但尚未备份其 SMTP 服务器 — 或其 SMTP 服务器正忙于处理其他消息而无法在 MTA 尝试连接时接受连接。）
9. 最终邮件出了队列。

MTA 日志记录示例：通过转换通道路由外来 SMTP 邮件

代码示例 21-8 第 663 页 对通过转换通道路由邮件的例子进行了说明。假设此站点具有 CONVERSIONS 映射表，例如：

```
CONVERSIONS

  IN-CHAN=tcp_local;OUT-CHAN=l;CONVERT    Yes
```

本示例假设选项设置为 LOG_FILENAME=1 和 LOG_MESSAGE_ID=1。

代码示例 21-8 日志记录：通过转换通道路由外来 SMTP 邮件

```
04-Feb-1998 00:06:26.72 tcp_local     conversion    E 9 (1)
 amy@siroe.edu rfc822;bert@sesta.com bert@sesta.com
 imta/queue/conversion/ZZ01IT5UAMZ4QW98518O.00
 <01IT5UALL14498518O@siroe.edu>

04-Feb-1998 00:06:29.06 conversion    l             E 9 (2)
 amy@siroe.edu rfc822;bert@sesta.com bert
 imta/queue/l/ZZ01IT5UAOXLDW98509E.00  <01IT5STUMUFO984Z8L@siroe.edu>

04-Feb-1998 00:06:29.31 conversion                  D 9 (3)
 amy@siroe.edu rfc822;bert@sesta.com bert
 imta/queue/conversion/ZZ01IT5UAMZ4QW98518O.00
 <01IT5UALL14498518O@siroe.edu>

04-Feb-1998 00:06:32.62 l                           D 9 (4)
 amy@siroe.edu rfc822;bert@siroe.com bert
 imta/queue/l/ZZ01IT5UAOXLDW98509E.00
 <01IT5STUMUFO984Z8L@siroe.edu>
```

1. 进入的来自外部用户 amy@siroe.edu 的邮件发送到 l 通道收件人 bert@sesta.com。但是， CONVERSIONS 映射条目使邮件初始时排到转换通道 （而不是直接进入 l 通道）。
2. 转换通道运行并将邮件排到 l 通道。
3. 然后转换通道可以使邮件出队 （删除旧邮件文件）。
4. 最后， l 通道使邮件出队 （传送）。

MTA 日志记录示例：出站连接日志记录

代码示例 21-9 第 664 页 说明了通过 LOG_CONNECTION=3 启用连接日志记录后外发邮件的日志输出。在本示例中还假设了 LOG_PROCESS=1、 LOG_MESSAGE_ID=1 和 LOG_FILENAME=1。本示例介绍了用户 adam@sesta.com 将同一邮件发送给 （请注意每个邮件副本的邮件 ID 都相同）三个收件人 bobby@hosta.sesta.com、carl@hosta.sesta.com 和 dave@hostb.sesta.com 的例子。本示例假设邮件从标有 （如此类通道通常的那样） single_sys 通道关键字的 tcp_local 通道发出。因此，如 (1)、(2) 和 (3) 中所示，系统将在磁盘上为属于独立主机名的每组收件人创建独立的邮件文件，其中 bobby@hosta.sesta.com 和 carl@hosta.sesta.com 收件人被存储在同一邮件文件中，而 dave@hostb.sesta.com 收件人被存储在另一邮件文件中。

代码示例 21-9 日志记录：出站连接日志记录

```
19-Feb-1998 10:52:05.41 1e488.0 l            tcp_local    E 1
 adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00                (1)
  <01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:05.41 1e488.0 l            tcp_local    E 1
 adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00                (2)
  <01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:05.74 1e488.1 l            tcp_local    E 1
 adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7C11FU000FCN.00                (3)
  <01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:10.79 1f625.2.0 tcp_local    -           O (4)
 TCP|206.184.139.12|5900|206.184.139.66|25
 SMTP/hostb.sesta.com/mailhub.sesta.com                      (5)

19-Feb-1998 10:52:10.87 1f625.3.0 tcp_local    -           O (6)
 TCP|206.184.139.12|5901|206.184.139.70|25
 SMTP/hosta.sesta.com/hosta.sesta.com                        (7)

19-Feb-1998 10:52:12.28 1f625.3.1 tcp_local                D 1
 adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
```

```
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00
  <01ITRF7BDHS6000FCN@SESTA.COM>
 hosta.sesta.com dns;hosta.sesta.com                              (8)
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 (hosta.sesta.com -- Server ESMTP [iMS V5.0 #8790])
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 smtp;250 2.1.5 bobby@hosta.sesta.com and options OK.

19-Feb-1998 10:52:12.28 1f625.3.1 tcp_local                  D 1
 adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00
  <01ITRF7BDHS6000FCN@SESTA.COM>
 hosta.sesta.com dns;hosta.sesta.com
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 (hosta.sesta.com -- Server ESMTP [iMS V5.0 #8790])
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 smtp;250 2.1.5 carl@hosta.sesta.com and options OK.

19-Feb-1998 10:52:12.40 1f625.3.2 tcp_local      -           C (9)
 TCP|206.184.139.12|5901|206.184.139.70|25
 SMTP/hosta.sesta.com/hosta.sesta.com

19-Feb-1998 10:52:13.01 1f625.2.1 tcp_local                  D 1
 adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7C11FU000FCN.00
  <01ITRF7BDHS6000FCN@SESTA.COM>
 mailhub.sesta.com dns;mailhub.sesta.com
 (TCP|206.184.139.12|5900|206.184.139.66|25)
 (MAILHUB.SESTA.COM -- Server ESMTP [iMS V5.0 #8694])
 (TCP|206.184.139.12|5900|206.184.139.66|25)
 smtp;250 2.1.5 dave@hostb.sesta.com and options OK.

19-Feb-1998 10:52:13.05 1f625.2.2 tcp_local      -           C (10)
 TCP|206.184.139.12|5900|206.184.139.66|25
 SMTP/hostb.sesta.com/mailhub.sesta.com
```

1. 邮件已排入队列，准备发给第一个收件人 ...
2. .... 准备发给第二个收件人 ...
3. .... 准备发给第三个收件人。
4. 设置 LOG_CONNECTION=3 将使 MTA 写入此条目。减号 (-) 表示此条目指外发连接。O 表示此条目对应于连接的开口。同时请注意尽管此开口由线程 2 和线程 3 来执行，但由于多线程的 TCP/IP 通道使用同一进程来处理这些不同的连接开口，因此此处的进程 ID 相同 （均为 1f625）。

5. 由于要连接到两个单独的远程系统，独立线程中的多线程 SMTP 客户机将打开与每个系统的连接 — 第一个显示在本条目中，第二个显示在 7 中。条目的此部分显示了发送和目标 IP 号以及端口号，并显示了初始主机名和通过 DNS 查找到的主机名。在 SMTP/*initial-host*/*dns-host* 子句中，请注意初始主机名和在初始主机名上执行 DNS MX 记录查找后所使用的主机名的显示：mailhub.sesta.com 显然是 hostb.sesta.com 的 MX 服务器。
6. 多线程的 SMTP 客户机在单独的线程中 （尽管进程相同）打开到第二系统的连接。
7. 由于要连接到两个单独的远程系统，独立线程中的多线程 SMTP 客户机将打开与每个系统的连接 — 第二个显示在本条目中，第一个显示在上面的 5 中。条目的此部分显示了发送和目标 IP 号以及端口号，并显示了初始主机名和通过 DNS 查找到的主机名。在本示例中，系统 hosta.sesta.com 显然自己直接接收邮件。
8. 除了产生特定的连接条目外，LOG_CONNECTION=3 还可将与连接相关的信息包含进常规邮件条目中，如此处所示。
9. 设置 LOG_CONNECTION=3 将使 MTA 写入此条目。所有邮件 （本示例中的 bobby 和 carl 邮件）出队列后，系统将关闭连接，如此条目中的 C 所表示。
10. 设置 LOG_CONNECTION=3 将使 MTA 写入此条目。所有邮件 （本示例中的 dave 邮件）出队列后，系统将关闭连接，如此条目中的 C 所表示。

MTA 日志记录示例：入站连接日志记录

代码示例 21-10 说明了通过 LOG_CONNECTION=3 启用连接日志记录后外来 SMTP 邮件的日志输出。

代码示例 21-10 日志记录：入站连接日志记录

```
19-Feb-1998 17:02:08.70 tcp_local    +            O    (1)
 TCP|206.184.139.12|25|192.160.253.66|1244 SMTP       (2)

19-Feb-1998 17:02:26.65 tcp_local    l             E 1
 service@siroe.com rfc822;adam@sesta.com adam
 THOR.SIROE.COM (THOR.SIROE.COM [192.160.253.66])      (3)

19-Feb-1998 17:02:27.05 tcp_local    +             C    (4)
 TCP|206.184.139.12|25|192.160.253.66|1244 SMTP

19-Feb-1998 17:02:31.73 l                          D 1
 service@siroe.com rfc822;adam@sesta.com adam
```

1. 远程系统打开一个连接。字符 O 表示此条目与连接开口有关；字符 + 表示此条目与外来连接有关。
2. 显示用于连接的 IP 号和端口。在此条目中，接收系统 （创建日志文件条目的系统）具有 IP 地址 206.184.139.12 并且将连接指向端口 25 ；发送系统具有 IP 地址 192.160.253.66 并从端口 1244 发送。
3. 在从外来 TCP/IP 通道 (tcp_local) 到 l 通道收件人的排入的邮件的条目中，请注意由于启用了 LOG_CONNECTION=3 而包含了超过默认值范围的信息。特别是，发送系统在其 HELO 或 EHLO 线路上具有的名称、在连接 IP 号上由 DNS 反向查找到的发送系统的名称，以及发送系统的 IP 地址均被记录下来；有关对影响此性能的通道关键字的讨论，请参见第 12 章 “配置通道定义”。
4. 关闭入站连接。字符 C 表示此条目与连接关闭有关；字符 + 表示此条目与外来连接有关。

启用分发程序调试

分发程序错误和调试输出 （如果已启用）将被写入 MTA 日志目录中的 dispatcher.log 文件。在 *msg_svr_base*/imta/dispatcher.cnf 文件中指定了分发程序配置信息。安装时将创建一个默认的配置文件，它可以不作更改，直接使用。但是，如果出于安全性或性能原因，需要修改默认配置文件，则可以通过编辑 dispatcher.cnf 文件来实现此操作。

➤ 启用分发程序错误调试输出

1. 编辑 dispatcher.cnf 文件。
2. 将 DEBUG 选项设置为 -1。

   您还可以设置逻辑或环境变量 IMTA_DISPATCHER_DEBUG (UNIX)，它将以十六进制定义 32 位调试掩码为值 FFFFFFFF。下表介绍了每个位的含义。

表 21-3 分发程序调试位

位	十六进制值	十进制值	用法
0	x 00001	1	基本服务分发程序主模块调试。
1	x 00002	2	附加服务分发程序主模块调试。
2	x 00004	4	服务分发程序配置文件日志记录。
3	x 00008	8	基本服务分发程序杂项调试。
4	x 00010	16	基本服务调试。

表 21-3 分发程序调试位 （续）

位	十六进制值	十进制值	用法
5	x 00020	32	附加服务调试。
6	x 00040	64	进程相关服务调试。
7	x 00080	128	不使用。
8	x 00100	256	基本服务分发程序和进程通信调试。
9	x 00200	512	附加服务分发程序和进程通信调试。
10	x 00400	1024	软件包级别通信调试。
11	x 00800	2048	不使用。
12	x 01000	4096	基本工作进程调试。
13	x 02000	8192	附加工作进程调试。
14	x 04000	16384	附加工作进程调试，特别是连接切换。
15	x 08000	32768	不使用。
16	x 10000	65536	基本工作进程到服务分发程序 I/O 调试。
17	x 20000	131072	附加工作进程到服务分发程序 I/O 调试。
20	x 100000	1048576	基本统计信息调试。
21	x 200000	2097152	附加统计信息调试。
24	x 1000000	16777216	将 PORT_ACCESS 拒绝记录到 dispatcher.log 文件中。

➤ 设置分发程序参数 (Solaris)

分发程序配置文件中提供的分发程序服务将影响各种系统参数的要求。系统的堆大小 (datasize) 必须能够满足分发程序的线程堆栈使用。

1. 要显示堆大小 （即默认的 datasize），请使用以下命令之一：

   csh 命令：

   ```
   # limit
   ```

   ksh 命令

   ```
   # ulimit -a
   ```

   Solaris 实用程序

   ```
   # sysdef
   ```

2. 对每个分发程序服务计算 STACKSIZE*MAX_CONNS，然后把每项服务计算的值相加。系统的堆大小必需至少是此数目的两倍。

管理服务日志

本节介绍了邮件存储 （POP、 IMAP 和 HTTP）、 Admin 和 Default 服务的日志记录。（请参见表 21-1 第 644 页。）

对于这些服务，您可以使用 Console 来指定日志设置和查看日志。您指定的设置将影响所记录的事件以及事件的数目。分析日志文件时，您可以使用这些设置和其他特性来完善日志事件的搜索。

本节包含以下小节：

- 了解服务日志特性
- 了解服务日志文件格式
- 定义和设置服务日志记录选项
- 搜索并查看服务日志
- 使用邮件存储日志记录的邮件跟踪
- 邮件存储日志记录示例

了解服务日志特性

本节描述了邮件存储和管理服务的以下日志特性：日志记录级别、日志事件的类别、日志文件名约定和日志文件目录。

日志记录级别

日志记录的级别或优先级定义了日志记录活动的详细程度或冗长度。高优先级意味着较简略，仅记录具有高优先级 （高严重程度）的事件。低级别意味着更为详细，将在日志文件中记录更多事件。

您可以通过设置 `logfile.`*service*`.loglevel` 配置参数来为每种服务 （POP、 IMAP、 HTTP、 Admin 和 Default）单独设置日志记录级别 （请参见第 672 页的 “定义和设置服务日志记录选项”）。您还可以使用日志记录级别来过滤日志事件的搜索。表 21-4 对可用级别进行了说明。这些日志记录级别是 UNIX `syslog` 工具定义的那些级别的子集。

表 21-4 存储和管理服务的日志记录级别

级别	说明
Critical	最少的日志记录信息。发生严重问题或紧急情况时 （例如服务器无法访问邮箱或需要其运行的库），一个事件将被写入日志。

表 21-4 存储和管理服务的日志记录级别

级别	说明
Error	发生错误情况时 （例如尝试连接到客户机或其他服务器失败），一个事件将被写入日志。
Warning	发生警告情况时 （例如服务器无法理解客户机所发送的通信），一个事件将被写入日志。
Notice	发生通知 （正常但重要的情况）时 （例如用户登录失败或会话关闭），一个事件将被写入日志。这是默认日志级别。
Information	执行每个重要操作 （例如用户成功登录、注销、创建或重命名邮箱）时，一个事件将被写入日志。
Debug	最冗长的日志记录。仅供调试使用。执行每个进程或任务中的单个步骤时都将事件写入日志，用以确定问题。

当选择一个特定日志记录级别时，与该级别以及高于该级别 （较低冗长度）的所有级别相对应的事件都将包括在日志记录内。日志记录的默认级别为 `Notice`。

注 指定的日志记录越冗长，日志文件将占用的磁盘空间就越大；有关指导原则，请参见第 672 页的 “定义和设置服务日志记录选项”。

日志事件的类别

在每个支持的服务或协议中， Messaging Server 将根据日志事件所发生的设备或功能区进一步对日志事件进行分类。每个日志事件都包含生成日志事件的设备的名称。这些类别将有助于在搜索过程中过滤事件。表 21-5 列出了 Messaging Server 为日志记录目的所标识的类别。

表 21-5 日志事件的发生类别

设备	说明
General	与此协议或服务相关的无明显特征的操作
LDAP	与 Messaging Server 访问 LDAP 目录数据库相关的操作
Network	与网络连接相关的操作 （套接字错误归入此类别）
Account	与用户帐户相关的操作 （用户登录归入此类别）
Protocol	与特定于协议的命令相关的协议级操作 （由 POP、 IMAP 或 HTTP 函数返回的错误归入此类别）
Stats	与收集服务器统计信息相关的操作
Store	与访问邮件存储相关的低级操作 （读 / 写错误归入此类别）

有关在日志搜索中将类别用作过滤器的示例，请参见第 674 页的 “搜索并查看服务日志”。

服务日志文件目录

每项日志记录服务均被指定了单独的目录，其中存储了服务的日志文件。所有 IMAP 日志文件均存储在一起，所有 POP 日志文件及其他服务的日志文件也是如此。您可以定义每个目录的位置，也可以定义目录中允许存在的日志文件的最大大小和数目。

请确保存储容量足够所有日志文件使用。日志数据可能量很大，尤其在较低 （较冗长）的日志记录级别中。

同时，定义适当的日志记录级别、日志旋转、日志过期和服务器备份策略也很重要，以便备份所有日志文件目录并使这些目录都不会过载；否则，就可能丢失信息。请参见第 672 页的 “定义和设置服务日志记录选项”。

了解服务日志文件格式

所有由 Messaging Server 创建的邮件存储和管理服务日志文件都具有相同的内容格式。日志文件是多行文本文件，其中每行描述一个日志事件。对于每项支持的服务，所有事件说明都具有通用格式：

dateTime hostName processName [pid] :category logLevel :eventMessage

表 21-6 列出了日志文件组件。请注意，除了日期 / 时间格式不同以及此格式包括两个附加组件 （*category* 和 *logLevel*）以外，此事件说明的格式与 UNIX `syslog` 工具定义的格式相同。

表 21-6 存储和管理日志文件组件

组件	定义
dateTime	记录事件时的日期和时间，以 *dd/mm/yyyy hh:mm:ss* 格式表示，时区字段以来自 GMT 的 *+/-hhmm* 表示。例如：`02/Jan/1999:13:08:21 -0700`
hostName	服务器在其上运行的主机名：例如， `showshoe`。 注意：如果主机上有多个 Messaging Server 示例，则可以使用进程 ID (pid) 将不同示例的日志事件相互分开。
processName	生成事件的进程名称：例如， `cgi_store`。
pid	生成事件的进程 ID：例如， `18753`。
category	事件所属的种类：例如， `General` （请参见第 670 页的表 21-5）。

表 21-6 存储和管理日志文件组件

组件	定义
logLevel	事件所表示的日志记录级别：例如， `Notice`（请参见第 669 页的表 21-4）。
eventMessage	可为任意长度的特定于事件的解释消息：例如， `Log created (894305624)`。

以下是使用 Console 所查看到的三个日志事件示例：

```
02/May/1998:17:37:32 -0700 showshoe cgi_store[18753]:
General Notice:
  Log created (894155852)

04/May/1998:11:07:44 -0400 xyzmail cgi_service[343]:General Error:
  function=getserverhello|port=2500|error=failed to connect

03/Dec/1998:06:54:32 +0200 SiroePost imapd[232]:Account Notice:
  close [127.0.0.1] [unauthenticated] 1998/12/3 6:54:32
  0:00:00 0 115 0
```

IMAP 和 POP 事件条目可能会以三个数字结束。以上示例具有：0 115 0。第一个数字是客户机发送的字节数，第二个数字是服务器发送的字节数，第三个数字是选定的邮箱数（对于 POP 通常为 1）。

在“日志查看器”窗口中查看日志文件时，您可以通过搜索事件中的任意特定组件（例如特定的日志记录级别或种类或特定的进程 ID）来限制显示的事件。有关详细信息，请参见第 674 页的“搜索并查看服务日志”。

每个日志条目事件消息的格式都特定于所记录事件的类型，即每个服务都定义了出现在其任何事件消息中的内容。许多事件消息简单明了，而其他事件消息则复杂一些。

定义和设置服务日志记录选项

您可以定义能最好地满足管理需要的邮件存储和管理服务日志记录配置。本节讨论了可帮助您决定最佳配置和策略的问题，并解释了如何实现这些配置和策略。

灵活的日志记录体系结构

日志文件的命名模式 (*service.sequenceNum.timeStamp*) 有助于您设计灵活的日志旋转和备份策略。将不同服务的事件写入不同的文件便于您快速隔离问题。同时，由于文件名中的序列号持续增长，并且时间戳始终是唯一的，因此当有限的序列号集用尽后，以后的日志文件也不会简单地覆写早期的日志文件。而是仅在达到更灵活的生存期限制、文件数目或存储总数时，才会覆写或删除较旧的日志文件。

Messaging Server 支持日志文件的自动旋转，此功能简化了管理，也使备份变得更容易。不必手动删除当前日志文件并创建新日志文件以保留后续日志事件。您可以随时备份目录中除当前日志文件之外的所有日志文件，而不必停止服务器或手动通知服务器启动新日志文件。

设置日志记录策略的过程中，您可以针对每种服务设置选项，这些选项控制着日志存储总数、最大日志文件数、单个文件大小、最大文件生存期和日志文件旋转的速度等限制。

规划所需的选项

请记住，您必须设置若干个限制，超过其中一个限制可能会导致日志文件的旋转或删除。最先到达的限制为控制限制。例如，如果最大日志文件大小是 3.5 MB，并且您指定每天创建一个新日志，如果每 24 小时建立的日志数据不止 3.5 MB，那么每天实际创建的日志文件则不止一个。而且，如果最大日志文件数目是 10 个并且最大生存期是 8 天，则可能永远不会达到日志文件的生存期限制，因为较快的日志旋转将意味着在不到 8 天之内便已创建 10 个文件。

为 Messaging Server 管理日志提供的以下默认值可能是规划的合理起始点：

目录中日志文件的最大数目：10
最大日志文件大小：2 MB
所有日志文件允许的最大大小总计：20 MB
允许的最小可用磁盘空间：5 MB
日志翻滚时间：1 天
过期之前的最大生存期：7 天
日志记录的级别：Notice

您可以看到此配置假设预计服务器管理日志数据每天累积大约 2 MB，每周备份，分配给管理日志的存储空间总数至少是 25 MB。（如果日志记录级别更冗长，则这些设置可能不足。）

对于 POP、 IMAP 或 HTTP 日志，相同的值可能是合理的启动值。如果所有服务具有大致相同的日志存储要求 （如此处所示的默认值），您可能期望初始规划总计约 150 MB 的日志存储容量。（请注意，这仅意味着存储要求的一般指示；实际的要求可能会显著不同。）

了解日志记录选项

您可以使用 Console 或命令行来设置控制邮件存储日志记录配置的选项。

这些选项的最优设置取决于日志数据积累的速度。可能需要 4,000 到 10,000 个日志条目以占用 1 MB 存储。在较冗长的日志记录级别 （例如 Notice），一般忙碌的服务器每周可能生成成百上千兆字节的日志数据。可遵循以下方法：

- 设置与存储限制一致的日志记录级别 — 即，估计该级别将导致日志数据积累的速度与估计存储限制所使用的速度大致相同。
- 定义日志文件大小，以便不影响搜索性能。同时，将日志文件大小与旋转时间安排和存储限制总数置于同一级别。假定日志条目以某速度积累，您可以将最大速度设置为稍大于自动发生旋转时期望的积累速度。最大文件大小乘以最大文件数可能约等于存储限制总数。

  例如，如果每天进行 IMAP 日志旋转，您期望的 IMAP 日志数据积累为每天 3 MB，IMAP 日志的存储限制总数是 25 MB，您可将最大 IMAP 日志文件大小设为 3.5 MB。（本示例中，如果日志数据累积得很快，以致于所有日志文件都是最大大小并且已到达日志文件的最大数目，则可能仍会丢失日志数据。）
- 如果服务器每周备份一次而您每天旋转 IMAP 日志文件，则可以将 IMAP 日志文件的最大数目指定为 10 左右 （如果超过单个日志大小限制，则说明旋转得更快），并将最大生存期指定为 7 或 8 天。
- 拾取一个存储限制总数，该数目位于硬件容量内并与为服务器规划的备份时间安排相协调。估计您期望日志数据积累的速度、添加安全因素并定义存储限制总数，以使在服务器备份的间隔期间内不会超过此速度。

  例如，如果期望平均每天积累 3 MB 的 IMAP 日志文件数据，服务器每周备份一次，则可以指定大约 25 - 30 MB 作为 IMAP 日志的存储限制 （假设您的磁盘存储容量足够）。
- 为了安全起见，请在保留日志文件的卷中拾取允许的最小可用磁盘空间量。即，如果非日志文件大小因素导致了卷填满，则在尝试将日志数据写入装满的磁盘而发生故障之前将删除旧日志文件。

搜索并查看服务日志

Console 提供了用于查看邮件存储和管理日志数据的基本界面。它允许选择单个日志文件，并允许在那些文件中执行灵活的日志条目的过滤搜索。

对于给定的服务，日志文件以时间先后次序列出。选择要搜索的日志文件后，您可以通过指定搜索参数来缩小对单个事件的搜索范围。

搜索参数

以下是可以指定用于查看日志数据的搜索参数：

- **时间段**。您可以指定从其中检索事件的特定时间段的开始和结束时间，也可以指定要搜索的天数 （当前日期之前）。通常，您可以指定一个范围以查看导致服务器崩溃的日志事件或在已知时间发生的其他事件。或者，您可以指定一天的范围以仅查看在当前日志文件中的今天的事件。

- **日志记录的级别**。您可以指定日志记录级别 （请参见第 669 页的 “日志记录级别”）。您可以选择特定的级别来揭露特定的问题；例如，选择 “Critical”以查看服务器关闭的原因，或选择 “Error”以查找失败的协议调用。

- **设备**。您可以指定设备 （请参见第 670 页的 “日志事件的类别”）。如果您知道包含问题的功能区，则可以选择特定的设备；例如，如果确信服务器崩溃涉及磁盘错误，则选择 “Store”，或如果问题在于 IMAP 协议命令错误，则选择 “Protocol”。

- **文本搜索模式**。您可以提供文本搜索模式以进一步缩小搜索范围。您可以包括可表示为通配符类型搜索的事件的任何组件 （请参见第 671 页的 “了解服务日志文件格式”），例如已知定义要检索的某个事件或多个事件的事件时间、进程名称、进程 ID 和事件消息的任何部分 （例如远程主机名、函数名、错误编号等等）。

  您的搜索模式可以包括以下特定字符和通配字符：

  `*` 任何字符集 （示例：`*.com`）
  `?` 任何单字符 （示例：`199?`）
  `[`*nnn*`]` *nnn* 集中的任何字符 （示例：`[aeiou]`）
  `[^`*nnn*`]` *nnn* 集中没有的任何字符 （示例：`[^aeiou]`）
  `[`*n*`-`*m*`]` 任何在 *n*-*m* 范围内的字符 （示例：`[A-Z]`）
  `[^`*n*`-`*m*`]` 任何不在 *n*-*m* 范围内的字符 （示例：`[^0-9]`）
  \ 换码符：置于 `*`、 `?`、 `[` 或 `]` 之前以将这些符号用作字面值

注意：搜索区分大小写。

查看日志时，组合日志记录级别和设备的示例可能包括以下几种：

- 指定 “Account”设备 （和 “Notice”级别）以显示失败的登录，这在调查潜在的安全破坏时可能会有用
- 指定 “Network”设备 （和所有日志记录级别）以调查连接问题
- 指定所有设备 （和 "Critical" 日志记录级别）以查找服务器功能方面的基本问题

处理服务日志

本节介绍了如何通过使用 configutil 命令和 Console 来处理服务日志以便搜索和查看日志。

➤ 向系统日志发送服务日志

- 运行带有 syslogfacility 选项的 configutil 命令：

  ```
  configutil -o logfile.service.syslogfacility -v value
  ```

  其中 *service* 是 admin、pop、imap、imta 或 http，*value* 是 user、mail、daemon、local0 至 local7 或 none。

设置了值之后，系统会将邮件记录到与设置值相应的 syslog 设备并忽略所有其他日志文件服务选项。如果未设置选项或值为 none，则日志记录将使用 Messaging Server 日志文件。

➤ 使用 Console 设置日志记录选项

1. 打开要设置其日志文件选项的 Messaging Server。
2. 单击“配置”选项卡，打开左窗格中的“日志文件”文件夹，并选择某一服务（例如 IMAP、HTTP 或 Admin）的日志文件。
3. 从“详细程度”下拉列表中选择日志记录级别。
4. 在“日志文件的目录路径”字段中，输入将保留日志文件的目录名称。
5. 在“每个日志的文件大小”字段中，输入最大日志文件大小。
6. 在“创建一个新日志，每隔”字段中，输入日志旋转时间安排的数目。
7. 在“每个目录的日志数目”和“如果日志超过生存期”字段中，输入与备份时间安排相协调的最大日志文件数目和最大生存期。
8. 在“如果超出总日志大小”字段中，输入期望的存储限制总数。
9. 在“如果可用磁盘空间小于”字段中，输入希望保留的最小可用磁盘空间量。

➤ 禁用 HTTP 日志记录

如果系统不支持 HTTP 邮件访问（即 Web 邮件），则可以通过设置以下变量来禁用 HTTP 日志记录。如果系统要求 Web 邮件支持（例如 Messenger Express），请勿设置这些变量。

- 运行以下 configutil 命令：

  ```
  configutil -o service.http.enable -v no
  configutil -o service.http.enablesslport -v no
  ```

➤ 设置服务器日志级别

- 运行以下 configutil 命令：

  ```
  configutil -o logfile.service.loglevel -v level
  ```

  其中 *service* 是 admin、 pop、 imap、 imta 或 http， *loglevel* 是 Nolog、 Critical、 Error、 Warning、 Notice、 Information 或 Debug。

➤ 指定服务器日志文件的目录路径

- 运行以下 configutil 命令：

  ```
  configutil -o logfile.service.logdir -v dirpath
  ```

➤ 指定每个服务日志的最大文件大小

- 运行以下 configutil 命令：

  ```
  configutil -o logfile.service.maxlogfilesize -v size
  ```

  其中 *size* 指定了字节数。

➤ 指定服务日志旋转时间安排

- 运行以下 configutil 命令：

  ```
  configutil -o logfile.service.rollovertime -v number
  ```

其中 *number* 指定了秒数。

➤ 指定每个目录的服务日志文件的最大数目

- 运行以下 configutil 命令：

  ```
  configutil -o logfile.service.maxlogfiles -v number
  ```

  其中 *number* 指定了日志文件个数。

➤ 指定存储限制

- 运行以下 configutil 命令：

  ```
  configutil -o logfile.service.maxlogsize -v number
  ```

  其中 *number* 指定了一个以字节为单位的数目。

➤ 指定要保留的可用磁盘空间的最小量

- 运行以下 configutil 命令：

  ```
  configutil -o logfile.service.minfreediskspace -v number
  ```

  其中 *number* 指定了一个以字节为单位的数目。

➤ **指定日志到期的生存期**

```
configutil -o logfile.service.expirytime -v number
```

其中 *number* 指定了一个以秒为单位的数目。

➤ **指定搜索和查看结果**

请按以下步骤使用给定服务所属的特定的特性来搜索日志事件：

1. 在 Console 中，打开希望检查其日志文件的 Messaging Server。
2. 请执行以下任一步骤以显示给定日志记录服务的日志文件 “内容”选项卡：
   - 单击 “任务”选项卡，然后单击 “查看**服务**日志”，其中**服务**是日志记录服务的名称 （例如 “IMAP 服务”或 “管理”）。
   - 单击 “配置”选项卡，然后打开左窗格中的 “日志文件”文件夹并选择某一服务 （例如 IMAP 或 Admin）的日志文件。然后单击右窗格中的 “内容”选项卡。
3. 系统将显示该日志记录服务的 “内容”选项卡。
4. 在 “日志文件名”字段中，选择您要检查的日志文件。
5. 单击 “查看所选日志”按钮将打开 “日志查看器”窗口。
6. 在 “日志查看器”窗口中，指定所需的搜索参数 （已在上一节 " 搜索参数 " 中描述）。
7. 单击 “更新”将执行搜索并将结果显示在 “日志条目”字段中。

使用邮件存储日志记录的邮件跟踪

您可以通过邮件 ID 使用邮件存储日志记录来跟踪邮件，该方式类似于 MTA 跟踪邮件的方式。以此方式跟踪邮件使您可以跟踪邮件生命周期的紧急事件。

要在邮件存储日志中跟踪邮件，除了常规的日志记录配置外，您还需要配置邮件跟踪。默认情况下，不启用邮件跟踪。

注 邮件跟踪将填满大量的磁盘空间。请勿启用此功能，除非您有足够的磁盘空间。

邮件存储日志记录可以跟踪以下操作：

- 附加 — 邮件存储库向文件夹添加邮件的主要方式。跟踪附加显示了输入邮件存储的邮件。

- 获取 — 为最终用户检索邮件或部分邮件的 IMAP 命令。对于邮件跟踪，它的含义将扩展为任何服务为最终用户检索要阅读的邮件的时间。

  在邮件跟踪中，您阅读了某邮件的标题后，有时可能希望避免进行跟踪，因此，主体获取将参考检索邮件主体的某一部分的时间。

- 清除：在这种情况下，扩展的 IMAP 术语，以便参考任何服务从用户文件夹中删除邮件的时间。

➤ 启用邮件跟踪

- 运行以下 `configutil` 命令：

  ```
  configutil -o local.msgrace.active -v "yes"
  ```

  系统将邮件跟踪信息写入每个进程的默认日志中。 IMAP 获取显示在 `imap` 日志文件中。 ims_master 附加显示在 `ims_master` 通道日志文件中。

➤ 将邮件跟踪重定向到单个日志文件

- 要将邮件跟踪日志记录重定向到单个 "msgtrace" 日志文件，您必须使用 `configutil` 命令来配置日志文件参数。 msgtrace 日志文件与其他日志文件不同，它要在本地进行配置。例如：

```
configutil -o "local.logfile.msgtrace.buffersize" -v "0"
configutil -o "local.logfile.msgtrace.expirytime" -v "604800"
configutil -o "local.logfile.msgtrace.flushinterval" -v "60"
configutil -o "local.logfile.msgtrace.logdir" -v "/opt/SUNWmsgsr/data/log"
configutil -o "local.logfile.msgtrace.loglevel" -v "Information"
configutil -o "local.logfile.msgtrace.logtype" -v "NscpLog"
configutil -o "local.logfile.msgtrace.maxlogfiles" -v "10"
configutil -o "local.logfile.msgtrace.maxlogfilesize" -v "2097152"
configutil -o "local.logfile.msgtrace.maxlogsize" -v "20971520"
configutil -o "local.logfile.msgtrace.minfreediskspace" -v "5242880"
configutil -o "local.logfile.msgtrace.rollovertime" -v "86400"
```

➤ 取消配置邮件跟踪日志记录

- 要取消配置 msgtrace 日志文件，请使用 `configutil` 命令以删除所有对其配置的引用。例如：

```
configutil -o "local.logfile.msgtrace.buffersize" -v ""
configutil -o "local.logfile.msgtrace.expirytime" -v ""
configutil -o "local.logfile.msgtrace.flushinterval" -v ""
configutil -o "local.logfile.msgtrace.logdir" -v ""
configutil -o "local.logfile.msgtrace.loglevel" -v ""
configutil -o "local.logfile.msgtrace.logtype" -v ""
configutil -o "local.logfile.msgtrace.maxlogfiles" -v ""
configutil -o "local.logfile.msgtrace.maxlogfilesize" -v ""
configutil -o "local.logfile.msgtrace.maxlogsize" -v ""
configutil -o "local.logfile.msgtrace.minfreediskspace" -v ""
configutil -o "local.logfile.msgtrace.rollovertime" -v ""
```

➤ 配置 LMTP 日志记录

- 如果您使用的是 LMTP，而未使用单个 "msgtrace" 日志文件，则必须也在本地配置 `tcp_lmtp_server` 日志文件。如果您未使用 LMTP，或未使用邮件跟踪，或使用的是 "msgtrace" 日志文件中的邮件跟踪，则无需初始化 LMTP 邮件存储端日志。（LMTP 已分别记录了 MTA 信息。）例如：

```
configutil -o "local.logfile.tcp_lmtp_server.buffersize" -v "0"
configutil -o "local.logfile.tcp_lmtp_server.expirytime" -v "604800"
configutil -o "local.logfile.tcp_lmtp_server.flushinterval" -v "60"
configutil -o "local.logfile.tcp_lmtp_server.logdir" -v "/opt/SUNWmsgsr/data/log"
configutil -o "local.logfile.tcp_lmtp_server.loglevel" -v "Information"
configutil -o "local.logfile.tcp_lmtp_server.logtype" -v "NscpLog"
configutil -o "local.logfile.tcp_lmtp_server.maxlogfiles" -v "10"
configutil -o "local.logfile.tcp_lmtp_server.maxlogfilesize" -v "2097152"
configutil -o "local.logfile.tcp_lmtp_server.maxlogsize" -v "20971520"
configutil -o "local.logfile.tcp_lmtp_server.minfreediskspace" -v "5242880"
configutil -o "local.logfile.tcp_lmtp_server.rollovertime" -v "86400"
```

邮件存储日志记录示例

记录在邮件存储日志文件中的确切字段格式和字段列表将根据设置的日志记录选项而有所不同。本节将描述一些解释典型日志条目类别的示例。

邮件存储日志记录示例：错误密码

用户键入无效密码时，系统将记录“验证”失败，与之相对的是“未找到用户”消息。出于安全原因，“未找到用户”消息将以文本形式传递给客户机，但系统将记录真实原因（无效密码）。

代码示例 21-11 邮件存储日志记录：无效密码

```
 [30/Aug/2004:16:53:05 -0700] vadar imapd[13027]:Account
Notice:badlogin:[192.18.126.64:40718] plaintext user1 authentication failure
```

邮件存储日志记录示例：帐户禁用

以下示例显示了用户无法登录的原因（由于帐户被禁用）。此外，禁用的帐户被说明为 "(inactive)" 或 "(hold)"。

代码示例 21-12 邮件存储日志记录：帐户禁用

```
[30/Aug/2004:16:53:31 -0700] vadar imapd[13027]:Account
Notice:badlogin:[192.18.126.64:40720] plaintext user3 account disabled (hold)
```

邮件存储日志记录示例：邮件附加

以下示例显示了附加邮件，每当将邮件附加至文件夹时它都会出现。邮件存储日志记录了所有通过 `ims_master` 和 `lmtp` 通道输入邮件存储的邮件。记录了“附加”的用户 ID、文件夹、邮件大小和邮件 ID。

代码示例 21-13 邮件存储日志记录：附加

```
[31/Aug/2004:16:33:14 -0700] vadar ims_master[13822]:Store
Information:append:user1:user/user1:659:<Roam.SIMC.2.0.6.1093995286.11265.user1@vadar.siroe
.com>
```

邮件存储日志记录示例：由客户机检索的邮件

当客户机检索邮件时，邮件存储日志将编写 “获取”邮件。邮件存储日志将至少记录客户机对一个主体部分的所有获取。记录 “获取”的用户 ID、文件夹和邮件 ID。

代码示例 21-14 邮件存储日志记录：由客户机检索的邮件

```
 [31/Aug/2004:15:55:26 -0700] vadar imapd[13729]:Store
Information:fetch:user1:user/user1:<Roam.SIMC.2.0.6.1093051161.3655.user1@vadar.siroe.com>
```

邮件存储日志记录示例：从文件夹删除的邮件

当从文件夹中删除 IMAP 或 POP 邮件 （但不是从系统中删除）时，邮件存储将编写 “清除”邮件。系统将记录它是被用户还是被实用程序清除的。记录 “清除”的文件夹和邮件 ID。

代码示例 21-15 邮件存储日志记录：从文件夹删除的邮件

```
31/Aug/2004:16:57:36 -0700] vadar imexpire[13923]:Store
Information:expunge:user/user1:<Roam.SIMC.2.0.6.1090458838.2929.user1@vadar.siroe.com>
```

邮件存储日志记录示例：复制登录邮件

如果您为一个 msgtrace 日志文件配置邮件跟踪，则显示在 imap 和 pop 日志文件中的常规 “登录”邮件将在 msgtrace 文件中进行复制。

代码示例 21-16 邮件存储日志记录：登录

```
[30/Aug/2004:16:53:13 -0700] vadar imapd[13027]:Account Information:login
[192.18.126.64:40718] user1 plaintext
```

第 22 章

MTA 故障排除

本章介绍了对邮件传输代理 （MTA）进行故障排除的常用工具、方法和过程。其中包括以下各节：

- 第 683 页的 “故障排除概述”
- 第 684 页的 “标准 MTA 故障排除过程”
- 第 693 页的 “常见 MTA 问题和解决方案”
- 第 703 页的 “一般错误消息”
- 第 563 页的 “修复邮箱和邮箱数据库”（另一章）

可以参见第 23 章 “监视 Messaging Server”中的监视过程相关主题。

注 阅读本章之前，您应该查阅本指南的第 5 章至第 10 章以及 Sun Java System Messaging Server Administration Reference 中关于 MTA 配置和命令行实用程序的章节。

故障排除概述

对 MTA 进行故障排除的第一步之一是确定从何处开始诊断。您可能要根据问题在日志文件中查找错误消息。在其他情况下，您可能要检查所有标准 MTA 进程，查看 MTA 配置或启动和停止单个通道。无论使用何种方法，对 MTA 进行故障排除时请考虑以下问题：

- 配置或环境问题 （例如，磁盘空间或配额问题）是否阻止了邮件的接收？
- 邮件进入邮件队列时， MTA 服务 （如分发程序和作业控制器）是否存在？
- 网络连接性或路由问题是否造成了邮件在远程系统上阻塞或路由错误？

- 问题出现在邮件进入邮件队列之前还是之后？

本章将在后续各节中解答这些问题。

标准 MTA 故障排除过程

本节概述了 MTA 的标准故障排除过程。如果问题未生成错误消息、如果错误消息未提供足够的诊断信息、如果要对 MTA 执行整体完好性检查、测试和标准维护，请按照以下过程进行。

- 第 684 页的 “检查 MTA 配置”
- 第 685 页的 “检查邮件队列目录”
- 第 685 页的 “检查重要文件的拥有权”
- 第 686 页的 “检查作业控制器和分发程序是否正在运行”
- 第 687 页的 “检查日志文件”
- 第 688 页的 “手动运行通道程序”
- 第 688 页的 “启动和停止各个通道”
- 第 689 页的 “MTA 故障排除示例”

检查 MTA 配置

使用 `imsimta test -rewrite` 实用程序测试您的地址配置。使用此实用程序，您可以测试 MTA 的地址重写和通道映射，而不必实际发送邮件。有关更多信息，请参见 Sun Java System Messaging Server Administration Reference 中的 "MTA Command-line Utilities" 一章。

实用程序通常会显示要应用的地址重写以及邮件将排入其中的通道。但是，MTA 配置中的语法错误将导致实用程序发出错误消息。如果输出不是您所期望的，则可能需要更正您的配置。

检查邮件队列目录

检查邮件是否在 MTA 邮件队列目录中，该目录通常为 *msg_svr_base*/data/queue/。使用命令行实用程序（如 imsimta qm）检查期望的邮件文件是否在 MTA 邮件队列目录下。有关 imsimta qm 的更多信息，请参阅 Sun Java System Messaging Server Administration Reference 中关于 MTA 命令行实用程序的章节以及第 731 页的“imsimta qm counters”。

如果 imsimta test -rewrite 输出看上去正确，请检查邮件是否确实放在 MTA 邮件队列子目录中。要执行此操作，请启用邮件日志记录（有关 MTA 日志记录的更多信息，请参见第 647 页的“管理 MTA 邮件和连接日志”）。然后，您应该查看目录 /*msg_svr_base*/log/ 中的 mail.log_current 文件。可以根据特定邮件的邮件 ID 跟踪该邮件以确保该邮件将放在 MTA 邮件队列子目录中。如果找不到该邮件，则可能是文件磁盘空间或目录权限有问题。

检查重要文件的拥有权

安装 Messaging Server 时，应该已选择邮件服务器用户帐户（默认情况下为 nobody）。此帐户应拥有以下目录、子目录和文件：

/*msg_svr_base*/data/queue/
/*msg_svr_base*/log/
/tmp

类似以下 UNIX 系统示例中的命令可以用于检查这些目录的保护和拥有权：

```
ls -l -p -d /opt/SUNWmsgsr/data/queue
drwx------ 6 inetuser bin 512 Feb 7 09:32 /opt/SUNWmsgsr/data/queue

ls -l -p -d /opt/SUNWmsgsr/log/imta
drwx------ 2 inetuser bin 1536 Mar 10 09:00 /opt/SUNWmsgsr/log/imta

ls -l -p -d /opt/SUNWmsgsr/imta/tmp
drwx------ 2 inetuser bin 512 Feb 7 10:00 /opt/SUNWmsgsr/imta/tmp
```

使用类似以下 UNIX 系统示例中的命令检查 /*msg_svr_base*/data/queue 中的文件是否由 MTA 帐户拥有：

```
ls -l -p -R /opt/SUNWmsgsr/data/queue
```

检查作业控制器和分发程序是否正在运行

MTA 作业控制器可以控制 MTA 处理作业的执行，包括大多数外发（主）通道作业。

某些 MTA 通道 （例如 MTA 的多线程 SMTP 通道）包括处理外来邮件的常驻服务器进程。这些服务器可以控制通道的从 （外来）方向。 MTA 分发程序可以控制此类 MTA 服务器的创建。分发程序配置选项可以控制服务器的可用性、创建的服务器的数量和每个服务器可以控制的连接数量。

要检查作业控制器和分发程序是否存在以及查看 MTA 服务器和处理作业是否正在运行，请使用命令 `imsimta process`。在闲置情况下，该命令应导致启动 `job_controller` 和 `dispatcher` 进程。例如：

```
imsimta process

USER       PID  S     VSZ     RSS    STIME      TIME     COMMAND
inetuser   9567  S   18416    9368   02:00:02   0:00   /opt/SUNWmsgsr/lib/tcp_smtp_server

inetuser   6573  S   18112    5720    Jul_13    0:00    /opt/SUNWmsgsr/lib/job_controller

inetuser   9568  S   18416    9432    02:00:02  0:00   /opt/SUNWmsgsr/lib/tcp_smtp_server

inetuser   6574  S   17848    5328    Jul_13      0:00    /opt/SUNWmsgsr/lib/dispatcher
```

如果作业控制器不存在，则 */msg_svr_base*`/data/queue` 目录中的文件将会被备份，而邮件不会被传送。如果不具备分发程序，则将无法接收任何 SMTP 连接。

有关 `imsimta process` 的更多信息，请参见 Sun Java System Messaging Server Administration Reference。

如果作业控制器和分发程序都不存在，则应该查阅 */msg_svr_base*`/data/log` 中的 `dispatcher.log-*` 或 `job_controller.log-*` 文件。

如果日志文件不存在或未指出错误，请使用 `msg-start` 命令来启动进程。有关更多信息，请参见 Sun Java System Messaging Server Administration Reference 中关于 MTA 命令行实用程序的章节。

注 运行 `imsimta process` 时，不应该看到分发程序或作业控制器的多个实例，除非系统在执行 (`exec()`) 需要运行的程序之前在处理分叉 (`fork()`) 子进程。但是，此类重复过程的时间范围很小。

检查日志文件

如果 MTA 处理作业运行正常，但邮件仍留在邮件队列目录中，您可以检查日志文件以查看发生的情况。所有 MTA 日志文件均创建于目录 */msg_svr_base*/log 之中。表 22-1 中显示了各种 MTA 处理作业的日志文件名称格式。

表 22-1 MTA 日志文件

文件名	日志文件内容
*channel*_master.log-*uniqueid*	*channel* 的主程序 （通常为客户机上的程序）的输出。
*channel*_slave.log-*uniqueid*	*channel* 的从程序 （通常为服务器上的程序）的输出。
dispatcher.log-*uniqueid*	分发程序调试。无论是否设置了分发程序 DEBUG 选项，都会创建此日志。但是，要获取详细的调试信息，应将 DEBUG 选项设置为非零值。
imta	传送中存在问题时显示的 ims-ms 通道错误消息。
job_controller.log-*uniqueid*	作业控制器日志记录。无论是否设置了作业控制器 DEBUG 选项，都会创建此日志。但是，要获取详细的调试信息，应将 DEBUG 选项设置为非零值。
tcp_smtp_server.log-*uniqueid*	调试 tcp_smtp_server。此日志中的信息是针对服务器 （而不是邮件）的。
return.log-*uniqueid*	周期性 MTA 邮件退回程序作业的调试输出；如果在 option.dat 中使用了 return_debug 选项，则将创建此日志文件。

注 每个日志文件均使用唯一的 ID (*uniqueid*) 创建以避免覆写先前由同一通道创建的日志。要查找特定日志文件，可以使用 imsimta view 实用程序。也可以使用 imsimta purge 命令清理过时的日志文件。有关更多信息，请参见 Sun Java System Messaging Server Administration Reference 中关于 MTA 命令行实用程序的章节。

在以下任何一种情况下，将创建 *channel*_master.log-*uniqueid* 和 *channel*_slave.log-*uniqueid* 日志文件：

- 您当前的配置存在错误。
- 在 imta.cnf 文件中的通道上设置了 master_debug 或 slave_debug 关键字。
- 如果在 option.dat 文件 （在目录 */msg_svr_base*/config/ 中）中，将 mm_debug 设置为非零值 (mm_debug > 0)。

有关调试通道主程序和从程序的更多信息，请参见 Sun Java System Messaging Server Administration Reference。

手动运行通道程序

诊断 MTA 传送问题时，手动运行 MTA 传送作业 （特别在启动了一个或多个通道的调试之后）将非常有帮助。

命令 `imsimta submit` 将通知 MTA 作业控制器运行通道。如果针对所述通道启用了调试，`imsimta submit` 将在目录 */msg_svr_base*/`log` 中创建一个日志文件，如表 22-1 中所示。

命令 `imsimta run` 将在当前活动进程下执行该通道的外发传送，并将输出指向您的终端。这可能比提交作业更方便，特别是在您怀疑作业提交本身有问题时。

注 要手动运行通道，作业控制器必须正在运行。

有关 `imsimta submit` 和 `imsimta run` 命令的语法、选项、参数和示例的信息，请参见 Sun Java System Messaging Server Administration Reference 中关于 MTA 命令行实用程序的章节。

启动和停止各个通道

在某些情况下，停止和启动各个通道更易于诊断和调试邮件队列问题。停止邮件队列使您可以检查排列的邮件以确定存在的循环和垃圾邮件侵袭。

停止特定通道的外发处理 （排出队列）

1. 使用 `imsimta qm stop` 命令停止特定通道。执行此操作可以不必停止作业控制器以及重新编译配置。在以下示例中，将停止 `conversion` 通道：

   ```
   imsimta qm stop conversion
   ```

2. 要恢复处理，请使用 `imsimta qm start` 命令以重新启动通道。在以下示例中，将启动 `conversion` 通道：

   ```
   imsimta qm start conversion
   ```

有关 `imsimta qm start` 和 `imsimta qm stop` 命令的更多信息，请参见 Sun Java System Messaging Server Administration Reference 中关于 MTA 命令行实用程序的章节。

从特定域或 IP 地址停止外来处理 （进入通道队列）

将临时 SMTP 错误返回到客户机主机时，如果要停止某个特定域或 IP 地址的外来邮件处理，可以运行以下进程之一。执行此操作，邮件将不会保存在您的系统中。请参见第 455 页的 “第 1 部分：映射表”。

- 要停止特定主机或域名的外来处理，请将以下访问规则添加到 MTA 映射文件（通常为 */msg_svr_base*/config/mappings）中的 ORIG_SEND_ACCESS 映射表：

```
ORIG_SEND_ACCESS

    *|*@sesta.com|*|*              $X4.2.1|$NHost$ blocked
```

  通过使用此进程，发件人的远程 MTA 将把邮件保存在其系统上，继续定期重新发送这些邮件直到您重新启动外来处理。

- 要停止特定 IP 地址的外来处理，请将以下访问规则添加到 MTA 映射文件（通常为 */msg_svr_base*/config/mappings）中的 PORT_ACCESS 映射表：

```
PORT_ACCESS

    TCP|*|25|IP_address_to_block|*                $N500$ unable$ to$ \
connect$ at$ this$ time
```

当希望从域或 IP 地址重新启动外来处理时，请确保从映射表中删除这些规则并重新编译配置。此外，您可能需要为每个映射表创建唯一的错误消息。这样做将使您可以确定正在使用哪个映射表。

MTA 故障排除示例

本节介绍了如何逐步对特定 MTA 问题进行故障排除。在本例中，邮件收件人没有收到电子邮件消息的附件。注意：为了与 MIME 协议术语保持一致，在本节中，“附件”称为“邮件组成部分”。前面提到的故障排除技巧可用来识别邮件组成部分消失的位置和原因（请参见第 684 页的“标准 MTA 故障排除过程”）。通过使用以下步骤，可以确定邮件通过 MTA 的路径。此外，您还可以确定邮件组成部分是在邮件进入邮件队列之前还是之后消失的。要实现此目的，您需要手动停止和运行通道以捕获相关文件。

注　　手动使邮件通过通道时，作业控制器必须正在运行。

识别邮件路径中的通道

通过识别邮件路径中的通道，您可以将 master_debug 和 slave_debug 关键字应用于相应的通道。这些关键字将在通道的主日志文件和从日志文件中生成调试输出，反过来，主调试信息和从调试信息将帮助识别邮件组成部分消失的位置。

1. 在目录 */msg_svr_base*/config 中的 option.dat 文件中添加 log_message_id=1。使用此参数，您将在 mail.log_current 文件中看到邮件的 ID: 标题行。
2. 运行 imsimta cnbuild 以重新编译配置。
3. 运行 imsimta restart dispatcher 以重新启动 SMTP 服务器。
4. 使最终用户重新发送带有邮件组成部分的邮件。
5. 确定邮件通过的通道。

   尽管识别通道有各种方法，但建议使用以下方法：

   a. 在 UNIX 平台上，使用 grep 命令可以在 */msg_svr_base*/log 目录的 mail.log_current 文件中搜索邮件 ID: 标题行。

   b. 找到邮件的 ID: 标题行之后，查找 E （入队列）记录和 D （出队列）记录以确定邮件的路径。有关日志记录条目代码的更多信息，请参见第 648 页的“了解 MTA 日志条目格式”。有关此示例，请参见以下 E 记录和 D 记录：

```
29-Aug-2001 10:39:46.44 tcp_local conversion      E 2 ...

29-Aug-2001 10:39:46.44 conversion tcp_intranet   E 2 ...

29-Aug-2001 10:39:46.44 tcp_intranet              D 2 ...
```

左边的通道是源通道，右边的通道是目标通道。在本示例中， E 记录和 D 记录表明邮件路径是从 tcp_local 通道到 conversion 通道，最后到达 tcp_intranet 通道。

手动启动和停止通道以收集数据

本节介绍如何手动启动和停止通道。有关更多信息，请参见第 688 页的“启动和停止各个通道”。通过手动启动和停止邮件路径中的通道，您可以在 MTA 进程的不同阶段保存邮件和日志文件。这些文件随后将用于第 692 页的“识别邮件故障点”。

1. 在目录 */msg_svr_base*/config 的 option.dat 文件中设置 mm_debug=5 以提供重要的调试信息。

2. 将 slave_debug 和 master_debug 关键字添加到目录 */msg_svr_base*/config 中的 imta.cnf 文件中的相应通道。

   a. 在发送带有邮件组成部分的邮件的远程系统的外来通道 （或初始对话期间邮件被切换到的任意通道）中，使用 slave_debug 关键字。在本示例中，slave_debug 关键字将被添加到 tcp_local 通道。

   b. 将 master_debug 关键字添加到邮件所通过并在第 690 页的 “识别邮件路径中的通道”中已经识别的其他通道。在本示例中， master_debug 关键字将被添加到 conversion 和 tcp_intranet 通道。

   c. 运行命令 imsimta restart dispatcher 以重新启动 SMTP 服务器。

3. 使用 imsimta qm stop 和 imsimta qm start 命令以手动启动和停止特定通道。有关使用这些关键字的详细信息，请参见第 688 页的 “启动和停止各个通道”。

4. 为启动捕获邮件文件的进程，请使最终用户重新发送带有邮件组成部分的邮件。

5. 当邮件进入某个通道时，如果使用 imsimta qm stop 命令停止了该邮件，则该邮件将停留在通道中。有关更多信息，请参见步骤步骤 3。

   a. 在手动运行邮件路径中的下一个通道之前，复制并重命名邮件文件。请参见以下 UNIX 平台示例：

      ```
      # cp ZZ01K7LXW76T7O9TD0TB.00 ZZ01K7LXW76T7O9TD0TB.KEEP1
      ```

      邮件文件通常位于类似 */msg_svr_base*/data/queue/*destination_channel*/001 的目录中。 *destination_channel* 是邮件将通过的下一个通道 （例如：tcp_intranet）。如果要在 *destination_channel* 目录中创建子目录 （如 001、002 等等），请将 subdirs 关键字添加到通道。

   b. 建议每次捕获和复制邮件时为该邮件的扩展名编号，以标识处理该邮件的顺序。

6. 恢复通道中的邮件处理并排入邮件路径中的下一个目标通道。要执行此操作，请使用 imsimta qm start 命令。

7. 复制并保存位于目录 */msg_svr_base*/log 中的相应通道日志文件（例如：tcp_intranet_master.log-*）。选择包含您正在跟踪的邮件数据的相应日志文件。确保邮件进入通道时，复制的文件与该邮件的时间戳和主题标题相匹配。在 tcp_intranet_master.log-* 的示例中，可以将文件保存为 tcp_intranet_master.keep，这样文件不会被删除。

8. 重复步骤 5 至步骤 7 直到邮件到达其最终目标。

   在步骤步骤 7 中复制的日志文件应该与在步骤步骤 5 中复制的邮件文件相互关联。例如，如果在丢失邮件组成部分的情况下停止所有通道，则需保存 conversion_master.log-* 和 tcp_intranet_master.log-* 文件。也要保存源通道日志文件 tcp_local_slave.log-*。此外，还要保存每个目标通道中相应邮件文件的副本：conversion 通道中的 ZZ01K7LXW76T7O9TD0TB.KEEP1 和 tcp_intranet 通道中的 ZZ01K7LXW76T7O9TD0TB.KEEP2。

9. 复制完邮件文件和日志文件后，删除调试选项。

   a. 从目录 */msg_svr_base*/config 的 imta.cnf 文件中的相应通道中删除 slave_debug 和 master_debug 关键字。

   b. 重置 mm_debug=0 并删除目录 */msg_svr_base*/config 中的 option.dat 文件中的 log_message_id=1。

   c. 使用 imsimta cnbuild 重新编译配置。

   d. 运行命令 imsimta restart dispatcher 以重新启动 SMTP 服务器。

识别邮件故障点

1. 在完成启动和停止通道程序后，您应该具有可用于解决问题的以下文件：

   a. 每个通道程序中的邮件文件 （例如：ZZ01K7LXW76T7O9TD0TB.KEEP1）的所有副本

   b. 一个 tcp_local_slave.log-* 文件

   c. 每个目标通道的一组 *channel*_master.log-* 文件

   d. 可以显示邮件路径的一组 mail.log_current 记录

   所有文件应该具有与 mail.log_current 记录中的邮件 ID: 标题行相匹配的时间戳和邮件 ID 值。请注意有一个例外，当邮件被退回发件人时，这些退回的邮件将具有与原邮件不同的邮件 ID 值。

2. 检查 tcp_local_slave.log-* 文件以确定邮件进入邮件队列时是否具有邮件组成部分。

   查看 SMTP 对话和数据以查看从客户机发送的内容。

   如果邮件组成部分未出现在 tcp_local_slave.log-* 文件中，则问题是出现在邮件进入 MTA 之前。结果是，邮件被排入队列而没带邮件组成部分。如果是这样，则问题可能出现在发件人的远程 SMTP 服务器上或发件人的客户机中。

3. 审查邮件文件的副本以查看邮件组成部分被更改或丢失的位置。

   如果任一邮件文件显示邮件组成部分被更改或丢失，请检查以前的通道日志文件。例如，如果进入 tcp_intranet 通道的邮件中的邮件组成部分被更改或丢失，则应查看 conversion_master.log-* 文件。

4. 查看邮件的最终目标。

   如果邮件组成部分看起来没有在 tcp_local_slave.log、邮件文件 （例如：ZZ01K7LXW76T7O9TD0TB.KEEP1）和 *channel*_master.log-* 文件中更改，则 MTA 未更改邮件，邮件组成部分是在通向其最终目标的路径中的下一步上消失的。

   如果最终目标是 ims-ms 通道 （邮件存储），则可以从服务器将邮件下载到客户机上，以确定邮件组成部分是在此传输期间还是之后丢失的。如果目标通道是 tcp_* 通道，则需转至邮件路径中的 MTA。假设是 Messaging Server MTA，您将需要重复整个故障排除过程 （请参见第 690 页的 “识别邮件路径中的通道”、第 690 页的 “手动启动和停止通道以收集数据”和本节）。如果另一个 MTA 不受您的管理，则报告问题的用户应与特定站点联系。

常见 MTA 问题和解决方案

本节列出了 MTA 配置和操作的常见问题和解决方案。

- 第 694 页的 “对配置文件或 MTA 数据库的更改未生效”
- 第 694 页的 “MTA 可以发送外发邮件但不能接收外来邮件”
- 第 695 页的 “分发程序 （SMTP 服务器）无法启动”
- 第 695 页的 “外来 SMTP 连接超时”
- 第 697 页的 “邮件未被排出队列”
- 第 698 页的 “未传送 MTA 邮件”
- 第 699 页的 “邮件在循环”
- 第 701 页的 “接收到的邮件已编码”
- 第 702 页的 “服务器端规则 （SSR）不生效”

TLS 问题

如果在 SMTP 对话期间 STARTTLS 命令返回以下错误：

```
454 4.7.1 TLS 库初始化失败
```

并且如果您已经安装了证书并将其用于 pop/imap 访问，请检查以下事项：

- 必须设置证书的保护 / 拥有权以便 mailsrv 帐户可以访问这些文件
- 存储证书的目录需要设置保护 / 拥有权以便 mailsrv 帐户可以访问该目录内的文件。

在更改保护及安装证书后，必须运行以下命令：

```
stop-msg dispatcher
start-msg dispatcher
```

重新启动 MTA 即可，但最好是将其彻底关闭、安装证书，然后一切恢复正常。

对配置文件或 MTA 数据库的更改未生效

如果对配置、映射、转换、安全性、选项或别名文件的更改未生效，请检查以查看您是否执行了以下步骤：

1. 重新编译配置 （通过运行 imsimta cnbuild）。
2. 重新启动相应的进程 （如 imsimta restart dispatcher）。
3. 重新建立所有客户机连接。

MTA 可以发送外发邮件但不能接收外来邮件

大多数 MTA 通道依赖从程序或通道程序来接收外来邮件。对于某些由 MTA （如 TCP/IP 和 UUCP）支持的传输协议，需要确保传输协议激活的是 MTA 从程序而不是其标准服务器。将本地 sendmail SMTP 服务器替换为 MTA SMTP 服务器是作为 Messaging Server 安装的一部分执行的。有关更多信息，请参见 Sun Java Enterprise System 安装指南。

对于多线程 SMTP 服务器， SMTP 服务器的启动是由分发程序控制的。如果将分发程序配置为使用一个 MIN_PROCS 值 （大于或等于 SMTP 服务的值），则应始终至少有一个 SMTP 服务器进程在运行 （并且根据 SMTP 服务的 MAX_PROCS 值，可能更多）。 imsimta process 命令可用于检查 SMTP 服务器进程是否存在。有关更多信息，请参见 Sun Java System Messaging Server Administration Reference 中关于 MTA 命令行实用程序的章节。

分发程序 （SMTP 服务器）无法启动

如果分发程序无法启动，请首先检查 dispatcher.log-* 以获取相关错误消息。如果日志表明在创建或访问 /tmp/.SUNWmsgsr.dispatcher.socket 文件时有问题，则验证 /tmp 保护是否设置为 1777。该设置在权限中将显示如下：

```
drwxrwxrwt    8 root    sys           734  Sep 17 12:14      tmp/
```

.

还要对 .SUNWmsgsr.dispatcher.socket 文件执行 ls -l，并确认合适的拥有权。例如，如果这是由 root 创建的，则 inetmail 就无法访问。

请勿删除 .SUNWmsgsr.dispatcher.file，如果丢失，也不要创建。分发程序将创建该文件。如果保护未设置为 1777，则分发程序不会启动或重新启动，因为无法创建 / 访问套接字文件。此外，还可能出现与 Messaging Server 无关的其他问题。

外来 SMTP 连接超时

外来 SMTP 连接超时通常与系统资源及其分配相关。以下技巧可用于识别造成外来 SMTP 连接超时的原因：

1. 检查您允许同时进行多少个外来 SMTP 连接。这将由 SMTP 服务的 MAX_PROCS 和 MAX_CONNS 分发程序设置控制；允许同时进行的连接数量是 MAX_PROCS*MAX_CONNS。如果您可以提供系统资源，而连接数量太少不能满足使用要求，可以考虑增加此数量。

2. 可以使用的另一个技巧是打开 TELNET 会话。在以下示例中，用户连接到 127.0.0.1 端口 25。连接后，将返回 220 标题。例如：

```
telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 budgie.sesta.com -- Server ESMTP (Sun Java System Messaging Server 6.1
(built May  7 2001))
```

如果已连接并且收到 220 标题，但其它命令 （如 ehlo 和 mail from）没有违反响应，则应该运行 imsimta test -rewrite 以确保配置正确。

3. 如果 220 标题的响应时间较慢，如果在 SMTP 服务器上运行 pstack 命令时显示以下 iii_res* 函数 （这些函数表示正在执行的名称解析查找）：

```
febe2c04 iii_res_send (fb7f4564, 28, fb7f4de0, 400, fb7f458c, fb7f4564) + 142c
febdfdcc iii_res_query (0, fb7f4564, c, fb7f4de0, 400, 7f) + 254
```

则可能是主机必须进行反向名称解析查找，即使对于普通对 （如 localhost/127.0.0.1）。要防止此类性能降低，应该在 /etc/nsswitch.conf 文件中对主机的查找重新排序。要执行此操作，请将 /etc/nsswitch.conf 文件中的以下行从：

```
hosts:dns nis [NOTFOUND=return] files
```

更改为：

```
hosts:files dns nis [NOTFOUND=return]
```

在 /etc/nsswitch.conf 文件中进行此更改可以提高性能，由于只有少数 SMTP 服务器必须处理邮件，而不是多数 SMTP 服务器必须执行不必要的查找。

4. 您还可以通过 TCP/IP 邮件（通常为 tcp_local 和 tcp_intranet）将 slave_debug 关键字放在处理外来 SMTP 的通道中。完成此操作后，请查阅最近的 tcp_local_slave.log-*uniqueid* 文件以识别超时邮件的所有具体特征。例如，如果大量收件人的外来邮件将要超时，请考虑在通道中使用 expandlimit 关键字。

请记住，如果您的系统过载和过分扩展，则很难完全避免超时。

邮件未被排出队列

在 TCP/IP 传送期间遇到的错误通常是瞬态的，遇到问题时 MTA 通常会保留邮件并定期重试传送。在大型网络的特定主机上遇到周期性故障而其它主机连接运行完好，这是正常的。要验证该问题，请检查日志文件以查看与传送尝试相关的错误。您可能会看到例如 “来自 smtp_open 的致命错误”的错误消息。此类错误很常见并通常与瞬态网络问题相关联。要调试 TCP/IP 网络问题，请使用类似 PING、TRACEROUTE 和 NSLOOKUP 的实用程序。

以下示例显示了查看邮件停留在等待传送到 xtel.co.uk 的队列中的原因可能使用的步骤。要确定邮件未被排出队列的原因，可以创建 MTA 用于在 TCP/IP 上传送 SMTP 邮件的步骤。

```
% nslookup -query=mx xtel.co.uk (步骤 1)

Server:LOCALHOST
Address:127.0.0.1

Non-authoritative answer:
XTEL.CO.UK  preference = 10, mail exchanger = nsfnet-relay.ac.uk (步骤 2)

% telnet nsfnet-relay.ac.uk 25 (步骤 3)
Trying...[128.86.8.6]
telnet: Unable to connect to remote host: Connection refused
```

1. 使用 NSLOOKUP 实用程序以查看此主机的 MX 记录 （如果有）。如果没有 MX 记录，则应尝试直接连接到主机。如果确实有 MX 记录，则必须连接到指定的 MX 中继。 MTA 优先使用 MX 信息，除非明确地配置为不这样做。另请参见第 312 页的 “TCP/IP MX 记录支持”。

2. 在此示例中， DNS （域名服务）为 xtel.co.uk 返回了指定的 MX 中继的名称。这是 MTA 将实际连接到的主机。如果列出了不止一个 MX 中断，则 MTA 将连续尝试每个 MX 记录，首先尝试最低的首选项值。

3. 如果与远程主机之间确实存在连接，则应该通过 TELNET 连接到 SMTP 服务器端口 25 以检查远程主机是否接受外来 SMTP 连接。

注 如果使用 TELNET 时未指定端口，您将发现远程主机接受常规 TELNET 连接。这并不表示远程主机接受 SMTP 连接，许多系统接受常规 TELNET 连接但拒绝 SMTP 连接 （反之亦然）。因此，您应该始终在 SMTP 端口上进行测试。

在上一个示例中，远程主机拒绝连接到 SMTP 端口。这就是 MTA 无法传送邮件的原因。连接可能被拒绝是由于远程主机的错误配置或远程主机上的某种资源的耗尽。在这种情况下，无法在本地进行任何操作以解决该问题。通常应该让 MTA 继续重试对邮件进行操作。

如果在未使用 DNS 的 TCP/IP 网络上运行 Messaging Server，则可以跳过步骤 （步骤 1）和 （步骤 2）。而可以使用 TELNET 以直接访问所述主机。要注意与 MTA 使用同一个主机名。查看 MTA 上一次尝试的相关日志文件以确定主机名。如果使用的是主机文件，则应该确保主机名信息正确。强烈建议使用 DNS 而不使用主机名。

请注意，如果使用交互式测试测试与 TCP/IP 主机的连接性时未遇到任何问题，则问题很可能在 MTA 上次尝试传送邮件后就已经完全解决了。您可以在相应的通道上重新运行 `imsimta submit tcp_channel` 以查看邮件是否正在被排出队列。

未传送 MTA 邮件

除了邮件传输问题，还有两种常见问题可导致未处理的邮件存在于邮件队列中：

1. 队列高速缓存与队列目录中的邮件不同步。 MTA 队列子目录中正在等待传送的邮件文件进入到内存中的队列高速缓存。通道程序运行时，将询问此队列高速缓存以确定要在通道队列中传送的邮件。有些情况下，队列中有邮件文件，但是没有相应的队列高速缓存条目。

   a. 要检查队列高速缓存中是否有某个特定文件，可以使用 `imsimta cache -view` 实用程序；如果该文件不在队列高速缓存中，则需要同步队列高速缓存。

      通常每四小时同步队列高速缓存一次。如果需要，可以使用命令 `imsimta cache -sync` 手动重新同步高速缓存。同步后，通道程序将在处理了新邮件后处理原来未处理过的邮件。如果要更改默认值 （4 小时），则应该通过添加 `sync_time=`*timeperiod* （其中 *timeperiod* 反映同步队列高速缓存的频率）来修

改目录 */msg_svr_base*/config 中的 job_controller.cnf 文件。请注意，*timeperiod* 必须大于 30 分钟。在以下示例中，通过将 sync_time=02:00 添加到 job_controller.cnf 的全局默认部分，队列高速缓存同步时间被修改为 2 小时：

```
! VERSION=5.0
!IMTA job controller configuration file
!
!Global defaults
tcp_port=27442
secret=N1Y9[HzQKW
slave_command=NULL
sync_time=02:00
```

您可以运行 imsimta submit *channel* 以在运行 imsimta cache -sync 后清除邮件的待办事项。要特别注意，如果邮件的待办事项较大（大于 1000），则清除通道可能需要花很长时间。

要获取队列高速缓存的摘要信息，请运行 imsimta qm -maint dir -database -total。

b. 如果在同步了队列高速缓存后，仍没有传送邮件，则应该重新启动作业控制器。要执行此操作，请使用 imsimta restart job_controller 命令。

重新启动作业控制器将导致从磁盘上的邮件队列重建邮件数据结构。

注意 重新启动作业控制器是一个激烈步骤，应该仅在完全用尽了所有其他方法时才执行。

有关作业控制器的更多信息，请参见第 179 页的 “作业控制器”。

2. 通道处理程序无法运行，因为无法创建其处理日志文件。请检查访问权限、磁盘空间和配额。

邮件在循环

如果 MTA 检测到某个邮件在循环，则该邮件将停止传送，并保存为 .HELD 文件。请参见第 700 页的 “诊断和清理 .HELD 邮件”。某些特定情况可能会导致 MTA 无法检测到的邮件循环。

第一步是确定邮件循环的原因。当问题邮件文件存在于 MTA 队列区、与问题邮件相关的 MTA 邮件日志条目 （如果在所述通道的 MTA 配置文件中启用了 `logging` 通道关键字）以及所述通道的 MTA 通道调试日志文件中时，应该查看问题邮件文件的副本。确定问题邮件的 From: 地址和 To: 地址，查看 Received 标题行并查看邮件结构 （邮件内容的封装类型），这些均可以帮助准确地确定遇到的是哪种邮件循环情况。

某些更常见的情况包括：

1. 邮寄主管地址损坏。

   MTA 要求邮寄主管地址为可以接收电子邮件的有效地址。如果至邮寄主管的邮件在循环，请检查配置是否具有指向可以接收邮件的帐户的正确邮寄主管地址。

2. Received: 标题行的删除将阻止 MTA 检测邮件循环。

   邮件循环的常规检测基于 Received: 标题行。如果 Received: 标题行被删除 （明显在 MTA 系统本身中或是在类似防火墙的另一个系统中），将影响邮件循环的正确检测。在这些情况下，请检查是否没有出现不希望的 Received: 标题行的删除。也要检查邮件循环的潜在原因。可能的原因包括：系统名称的指定有问题或系统未配置为可以识别其自身名称的变体、 DNS 问题、缺少有关所述系统的授权的寻址信息或用户地址转发错误。

3. 其他邮件传送系统对通知邮件的不正确处理将在响应通知邮件时生成重新封装的邮件。

   Internet 标准要求通知邮件 （将要传送的邮件的报告或邮件退回）具有一个空包络 From: 地址，以防止邮件循环。但是，某些邮件传送系统不能正确地处理此类通知邮件。当转发或退回通知邮件时，这些邮件传送系统可能会插入一个新的包络 From: 地址。这可能会导致邮件循环。解决方案是修复不正确地处理通知邮件的邮件传送系统。

诊断和清理 .HELD 邮件

如果 MTA 检测到邮件在服务器或通道之间跳动，传送将被停止并且邮件将被存储在 */msg_svr_base*`/data/queue/`*channel* 中带有后缀 `.HELD` 的文件中。通常，出现邮件循环是因为每个服务器或通道认为另一个服务器或通道负责邮件的传送。

例如，最终用户可能设置了在两个独立的邮件主机上相互转发邮件的选项。在用户的 `sesta.com` 帐户上，最终用户启用了将邮件转发至其 `varrius.com` 帐户的设置。而用户忘记了已启用此设置，又在其 `varrius.com` 帐户上将邮件转发设置到 `sesta.com` 帐户。

错误的 MTA 配置也会导致出现循环。例如， MTA 主机 X 认为 `mail.sesta.com` 的邮件会转至主机 Y。而主机 Y 认为主机 X 应该处理 `mail.sesta.com` 的邮件；结果是主机 Y 将邮件返回到主机 X。

在这些情况下， MTA 忽略了邮件，而未尝试进一步的传送。出现此类问题时，请查看邮件中的标题行以确定退回邮件的服务器或通道。根据需要修复条目。

您还可以通过运行 `imsimta qm release` 或执行以下步骤来重试 .HELD 邮件：

1. 将 .HELD 扩展名重命名为除 00 以外的任何 2 位数。例如，将 .HELD 重命名为 .06。

注 在重命名 .HELD 文件前，请确保邮件已停止循环。

2. 运行 `imsimta cache -sync`。运行此命令将更新高速缓存。
3. 运行 `imsimta submit` *channel* 或 `imsimta run` *channel*。

由于邮件可能会再次标记为 .HELD，可能有必要多次执行这些步骤，因为 Received: 标题行会堆积。

接收到的邮件已编码

按已编码格式接收 MTA 发送的邮件。例如：

```
Date: Wed, 04 Jul 2001 11:59:56 -0700 (PDT)
From: "Desdemona Vilalobos" <Desdemona@sesta.com>
To: santosh@varrius.com
Subject: test message with 8bit data
MIME-Version: 1.0
Content-type: TEXT/PLAIN; CHARSET=ISO-8859-1
Content-transfer-encoding: QUOTED-PRINTABLE

2=00So are the Bo=F6tes Void and the Coal Sack the same?=
```

使用 MTA 解码器命令 `imsimta decode` 阅读时，这些邮件显示为未编码。有关更多信息，请参见 Sun Java System Messaging Server Administration Reference。

SMTP 协议仅允许如 RFC 821 中所述的 ASCII 字符 （七位字符集）的传输。实际上，通过 SMTP 的八位字符的非协商传输是非法的，并且会导致某些 SMTP 服务器出现各种问题。例如， SMTP 服务器可能转入计算联结循环。邮件被反复发送。八位字符会使 SMTP 服务器崩溃。最后，八位字符设置会对不能处理八位数据的浏览器和邮箱造成严重破坏。

过去处理包含八位数据的邮件时， SMTP 客户机只有三种选项：将邮件按无法传送返回发件人、对邮件进行编码或直接违反 RFC 821 发送邮件。但是随着 MIME 和 SMTP 扩展的出现，现在可以通过使用 ASCII 字符集将标准编码用于对八位数据进行编码。

在前面的示例中，收件人收到带有 TEXT/PLAIN 内容类型的 MIME 的编码邮件。远程 SMTP 服务器 （MTA SMTP 客户机将邮件传输到其上）不支持八位数据的传输。由于原邮件包含八位字符， MTA 必须对邮件进行编码。

服务器端规则 （SSR）不生效

过滤器由一个或多个适用于邮件消息的条件操作组成。由于是在服务器上存储和评估过滤器，通常参考服务器端规则 （SSR）。

本节包括有关以下 SSR 主题的信息：

- 第 702 页的 “测试 SSR 规则”
- 第 703 页的 “常见语法问题”

另请参见第 486 页的 “调试用户级别的过滤器”。

测试 SSR 规则

- 要检查 MTA 的用户过滤器，请使用以下命令：

```
# imsimta test -rewrite -debug -filter user@domain
```

在输出中，查找以下信息：

```
mmc_open_url called to open ssrf:user@ims-ms
   URL with quotes stripped:ssrd:user@ims-ms
Determined to be a SSRD URL.
   Identifier:user@ims-ms-daemon
Filter successfully obtained.
```

- 此外，可以将 slave_debug 关键字添加到 tcp_local 通道以查看过滤器是如何应用的。结果显示在 tcp_local_slave.log 文件中。请确保在目录 */msg_svr_base*/config 中的 option.dat 文件中添加 mm_debug=5 以获取足够的调试信息。

常见语法问题

- 如果过滤器存在语法问题，则在 tcp_local_slave.log-* 文件中查找以下消息：
  Error parsing filter expression:...
  - 如果过滤器没问题，则将在输出的末端显示过滤器信息。
  - 如果过滤器有问题，则将在输出的末端显示以下错误：
    Address list error -- 4.7.1 Filter syntax error:
    desdaemona@sesta.com

    此外，如果过滤器有问题，则 SMTP RCPT TO 命令将返回一个临时错误响应代码：

```
RCPT TO:user@domain
452 4.7.1 Filter syntax error
```

地址的本地部分或接收字段中的星号

现在 MTA 在地址的本地部分以及其建立的接收字段查找 8 位字符 （而不是 ASCII 字符），并用星号代替这些字符。

一般错误消息

MTA 无法启动时，一般错误消息显示在命令行中。本节将介绍和诊断常见的一般错误消息。

注 要诊断您自己的 MTA 配置，请使用 imsimta test -rewrite -debug 实用程序检查 MTA 的地址重写和通道映射进程。通过使用此实用程序，您可以检查配置而无需实际发送邮件。请参见第 684 页的 “检查 MTA 配置”。

MTA 子组件还可能发出本章中未介绍的其他错误消息。有关每个子组件的更多信息，应当参阅 Sun Java System Messaging Server Administration Reference 中关于 MTA 命令行使用程序和配置的章节以及第 5 章至第 10 章。本节包括以下类型的错误：

- 第 704 页的 “mm_init 中的错误”
- 第 707 页的 “编译的配置版本不匹配”
- 第 708 页的 “交换空间错误”
- 第 708 页的 “文件打开或创建错误”
- 第 709 页的 “非法主机 / 域错误”
- 第 709 页的 “SMTP 通道中的错误：os_smtp_* 错误”

mm_init 中的错误

mm_init 中的错误通常表示 MTA 配置问题。如果运行 `imsimta test -rewrite` 实用程序，就会显示这些错误。其他实用程序 （如 `imsimta cnbuild`）、通道、服务器或浏览器也可能返回此类错误。

经常遇到的 mm_init 错误包括：

- 第 705 页的 “别名的错误等值。. .”
- 第 705 页的 “无法打开别名包含文件。. .”
- 第 705 页的 “发现重复的别名。. .”
- 第 705 页的 “通道表中的重复的主机。. .”
- 第 705 页的 “发现重复的映射名称。. .”
- 第 705 页的 “映射名称太长。.”
- 第 705 页的 “初始化 ch_ facility 时出错：编译的字符集版本不匹配”
- 第 706 页的 “初始化 ch_ facility 时出错：没有空间进入。.”
- 第 706 页的 “对于系统来说本地主机别名或本来的名称太长。. .”
- 第 706 页的 “别名没有等值地址。. .”
- 第 706 页的 “通道没有正式主机名。. .”
- 第 707 页的 “正式主机名太长”

别名的错误等值。. .

别名文件条目右侧部分的格式不正确。

无法打开别名包含文件。. .

无法打开别名文件所包含的文件。

发现重复的别名。. .

两个别名文件条目具有相同的左侧部分。您需要找出并删除重复项。查找提示 `error line #XXX` 的错误消息，其中 `XXX` 是行号。您可以在此行上修复重复的别名。

通道表中的重复的主机。. .

此错误消息表示您在 MTA 配置中有两个具有相同正式主机名的通道定义。

请注意， MTA 配置文件 (`imta.cnf`) 的重写规则 （上部）中的多余空白行将导致 MTA 将配置文件的提示解释成通道定义。请确保文件的首行不是空白行。由于经常有多个相同模式 （左侧）的重写规则，这就导致 MTA 将其解释成带有非唯一正式主机名的通道定义。请检查 MTA 配置中的所有带有重复正式主机名的通道定义和文件的上部 （重写规则）中所有不正确的空白行。

发现重复的映射名称。. .

此消息表示两个映射表具有相同的名称，需要删除其中一个重复的映射表。但是，映射文件中的格式化错误可能会导致 MTA 将某些内容错误地解释成映射表的名称。例如，无法正确地缩进映射表条目将导致 MTA 认为该条目的左侧实际上是映射表的名称。请检查映射文件中的常规格式并检查映射表名称。

注 在带有映射表名称的任一行的前后应有一行空白行。但是，在映射表的条目中间不应插入任何空白行。

映射名称太长。.

此错误表示映射表名称太长，需要缩短。映射文件中的格式化错误可能会导致 MTA 将某些内容错误地解释成映射表名称。例如，无法正确地缩进映射表条目将导致 MTA 认为该条目的左侧实际上是映射表的名称。检查映射文件和映射表名称。

初始化 ch_ facility 时出错：编译的字符集版本不匹配

如果看到此消息，则需要通过命令 `imsimta chbuild` 重新编译并重新安装已编译的字符集表。有关更多信息，请参见 Sun Java System Messaging Server Administration Reference。

初始化 ch_ facility 时出错：没有空间进入。.

此错误消息通常表示您需要调整 MTA 字符集内部表的大小，然后使用以下命令重建已编译的字符集表：

```
imsimta chbuild -noimage -maximum -option
imsimta chbuild
```

请验证在作出此更改前是否不需要重新编译和重新启动任何其他字符集表。有关 `imsimta chbuild` 的更多信息，请参见 Sun Java System Messaging Server Administration Reference 中关于 MTA 命令行实用程序的章节。

对于系统来说本地主机别名或本来的名称太长。. .

此错误表示本地主机别名或本来的名称太长 （通道块中第二个名称或后续名称的可选右侧部分）。但是， MTA 配置文件中较早的某些语法错误（例如，重写规则中的多余空白行）可能会导致 MTA 将某些内容错误地解释成通道定义。除了检查配置文件的提示行，还要检查该行以上的其他语法错误。特别是，如果 MTA 在其中发出此错误的行是要作为重写规则，则请确保检查此行之上的多余空白行。

别名没有等值地址。. .

别名文件中的某个条目缺少右侧部分 （翻译值）。

通道没有正式主机名。. .

此错误表示通道定义块缺少所需第二行 （正式主机名行）。有关通道定义块的更多信息，请参见 Sun Java System Messaging Server Administration Reference 中关于 MTA 配置及命令行实用程序的章节以及第 12 章 “配置通道定义”。在每个通道定义块的前后需要一个空白行，但空白行不能存在于通道定义的通道名称行和正式主机名行之间。还要注意， MTA 配置文件的重写规则部分不允许有空白行。

正式主机名太长

通道的正式主机名 （通道定义块的第二行）的长度限制为 128 个八位字节。如果要尝试在通道上使用较长的正式主机名，请将其缩短成占位符名称，然后使用重写规则使较长名称与短的正式主机名匹配。如果使用 `l` （本地）通道主机名，您可能会看到此情形。例如：

```
Original l Channel:
!delivery channel to local /var/mail store
l subdirs 20 viaaliasrequired maxjobs 7 pool LOCAL_POOL
walleroo.pocofronitas.thisnameismuchtoolongandreallymakesnosense
butitisanexample.monkey.gorilla.orangutan.antidisestablismentari
anism.newt.salamander.lizard.gecko.komododragon.com

Create Place Holder:
!delivery channel to local /var/mail store
l subdirs 20 viaaliasrequired maxjobs 7 pool LOCAL_POOL
newt

Create Rewrite Rule:
newt.salamander.lizard.gecko.komododragon.com   $U%$D@newt
```

请注意，使用 `l` （本地）通道时，需要使用 REVERSE 映射表。有关用法和语法的信息，请参见 Sun Java System Messaging Server Administration Reference 中关于 MTA 配置的章节。

较早出现在 MTA 配置文件 （例如，重写规则中的多余空白行）中的某些语法错误可能会导致 MTA 将某些内容错误地解释成通道定义。这可能会导致将预定的重写规则解释为正式主机名。除了检查配置文件的提示行，还要检查该行以上的其他语法错误。特别是，如果 MTA 在其中发出此错误的行是要作为重写规则，请确保检查此行之上的多余空白行。

编译的配置版本不匹配

`imsimta cnbuild` 实用程序的功能之一是将 MTA 配置信息编译成可以快速装入的图像。编译的格式定义相当严格，经常在 MTA 的不同版本之间发生重大更改。修补程序发行版的部分可能会出现较小的更改。

发生此类更改时，内部版本部分也将更改，以便可以检测到不兼容的格式。检测到不兼容的格式时， MTA 组件将停止，并显示上述错误。此问题的解决方案是使用命令 `imsimta cnbuild` 生成一个新的、编译的配置。

还有个好办法是使用 `imsimta restart` 命令重新启动所有常驻 MTA 服务器进程，这样可以获得更新的配置信息。

交换空间错误

要确保正确操作，重要的是在邮件传送系统上配置足够的交换空间。所需交换空间的容量将根据配置而有所不同。一般的协调建议是，交换空间的容量应该至少是主内存容量的三倍。

如下所示的错误消息表示交换空间不足：

```
jbc_channels:chan_execute [1]:fork failed:Not enough space
```

您可能会在作业控制器日志文件中看到此错误。其他交换空间错误将根据配置而有所不同。

使用以下命令可以确定您剩余的交换空间以及确定您已使用的交换空间。

- Solaris 系统：`swap -s` （在 MTA 进程繁忙时）、`ps -elf` 或 `tail /var/adm/messages`
- HP-UX 系统：`swapinfo` 或 `tail /var/adm/syslog/syslog.log`

文件打开或创建错误

为发送邮件， MTA 将读取配置文件并在 MTA 邮件队列目录中创建邮件文件。配置文件必须可由 MTA 或使用 MTA 的 SDK 编写的任何程序读取。在安装期间，可将适当的权限指定给这些文件。创建配置文件的 MTA 实用程序和过程也可指定权限。如果这些文件受系统管理员、其他授权的用户或某些站点特定过程的保护，则 MTA 可能无法读取配置信息。这将导致 “文件打开”错误或不可预测的性能。读取配置文件时遇到问题， `imsimta test -rewrite` 实用程序将报告附加信息。请参见 Sun Java System Messaging Server Administration Reference 的 MTA 有关章节中的 `imsimta test -rewrite` 文档。

如果 MTA 表现为从授权的帐户 （而不是非授权帐户）运行时，则 MTA 表目录中的文件权限可能是导致该问题的原因。检查配置文件及其目录的权限。请参见第 685 页的 “检查重要文件的拥有权”。

“文件创建”错误通常表示在 MTA 邮件队列目录中创建邮件文件时发生的问题。要诊断文件创建问题，请参见第 685 页的 “检查邮件队列目录”。

非法主机 / 域错误

当通过浏览器为 MTA 提供地址时，可能会看见此错误。或者，该错误可能被延迟并作为错误返回邮件消息的部分被返回。两种情况下，此错误消息均表示 MTA 无法将邮件传送到指定的主机。要确定不会将邮件发送到指定主机的原因，应按以下故障排除过程进行：

- 验证所述地址没有拼写错，没有抄写错，也没有使用不再存在的主机名或域名。
- 通过 `imsimta test -rewrite` 实用程序运行所述地址。如果此实用程序也返回关于该地址的 “非法主机 / 域”错误，则 MTA 在 `imta.cnf` 文件和相关文件中不具有处理该地址的规则。验证已正确配置了 MTA、已相应回答了所有配置问题，并保持了最新的配置信息。
- 如果 `imsimta test -rewrite` 未遇到有关地址的错误，则 MTA 可以确定如何处理地址，但网络传输将不接受该地址。您可以通过其他细节的传送尝试检查相应的日志文件。瞬态网络路由或名称服务错误不应该导致返回的错误消息，但是严重配置错误的域名服务器有可能会导致这些问题。
- 如果是在 Internet 上，请检查已正确配置 TCP/IP 通道以支持 MX 记录查找。不能直接在 Internet 上访问许多域地址，因此需要您的邮件系统能够正确解析 MX 条目。如果您在 Internet 上，并且您的 TCP/IP 已配置为支持 MX 记录，则应该已配置了 MTA 以启用 MTA 支持。有关更多信息，请参见 TCP/IP 连接和 DNS 查找支持第 308 页的 “TCP/IP 连接和 DNS 查找支持”。如果您的 TCP/IP 软件包没有配置为支持 MX 记录查找，则无法访问仅用于 MX 的域。

SMTP 通道中的错误：os_smtp_* 错误

如下所示的错误不一定是 MTA 错误：os_smtp_* 错误，如 os_smtp_open、os_smtp_read 和 os_smtp_write 错误。这些错误是 MTA 报告在网络层遇到的问题时生成的。例如， os_smtp_open 错误表示无法打开与远程端的网络连接。由于寻址错误或通道配置错误， MTA 可能会配置为与无效系统连接。os_smtp_* 错误通常是由于 DNS 或网络连接性问题，特别是如果这是以前的工作通道或地址。os_smtp_read 和 os_smtp_write 错误通常表示其他端中止了连接或由于网络问题而中止了连接。

网络和 DNS 问题在本质上通常是瞬态的。通常不必担心偶尔的 os_smtp_* 错误。但是，如果不断地看到这些错误，可能表示有潜在的网络问题。

要获取有关特定 os_smtp_* 错误的详细信息，请在所述通道上启用调试。审查将显示所尝试的 SMTP 对话的详细信息的调试通道日志文件。特别是要查看在 SMTP 对话期间出现网络问题的时间。时间可以暗示网络问题和远程端问题的类型。在某些情况下，您可能还需要执行网络级别调试（例如， TCP/IP 软件包跟踪）来确定已发送或已接收的内容。

第 23 章

监视 Messaging Server

在大多数情况下，一个经过很好计划和很好配置的服务器在执行时不需要管理员的过多介入。但是，作为管理员，监视服务器的问题信号是您的工作。本章介绍 Messaging Server 的监视。其中包含以下各节：

- 第 712 页的 “每天的监视任务”
- 第 713 页的 “监视系统性能”
- 第 716 页的 “监视 MTA”
- 第 719 页的 “监视邮件访问”
- 第 719 页的 “监视 LDAP 目录服务器”
- 第 722 页的 “监视邮件存储”
- 第 723 页的 “用于监视的实用程序和工具”

有关故障排除的过程，请参见第 22 章 “MTA 故障排除”。

自动监视和重新启动

Messaging Server 提供了一种方法，可以透明地监视服务并在服务崩溃或不响应（服务挂起或冻结）时自动重新启动服务。它可以监视所有邮件存储、 MTA 和 MMP 服务，包括 IMAP、 POP、 HTTP、作业控制器、分发程序和 MMP 服务器。它不监视其他服务，例如 SMS 或 TCP/SNMP 服务器。（TCP/SNMP 由作业控制器监视。）有关详细信息，请参阅第 101 页的 “失败的服务或未响应服务的自动重新启动”和第 733 页的 “使用 msprobe 和 watcher 功能进行监视”。

每天的监视任务

应当每天执行的最重要的任务是检查邮寄主管邮件、监视日志文件和设置 stored 实用程序。下面介绍这些任务。

检查邮寄主管邮件

Messaging Server 具有一个为邮寄主管电子邮件设置的预定义的管理邮递列表。属于此邮递列表的所有用户将自动接收发给邮寄主管的邮件。

RFC822 中定义了邮寄主管邮件的规则，它要求每个电子邮件站点都接受发送给名为邮寄主管的用户或邮递列表的邮件，并且发送到此地址的邮件应当传送给一个实际的个人。发送到 postmaster@host.domain 的所有邮件都被发送到邮寄主管帐户或邮递列表。

通常，邮寄主管地址是用户应当发送有关其邮件服务的电子邮件的位置。作为邮寄主管，您可能会收到来自本地用户有关服务器响应时间的邮件、来自其他服务器管理员 （他们在向您的服务器发送邮件时遇到问题）的邮件等等。您应当每天检查邮寄主管邮件。

您也可以将服务器配置为向邮寄主管地址发送特定的错误消息。例如，当 MTA 无法路由或传送邮件时，您可以通过发送给邮寄主管地址的电子邮件得到通知。您还可以向邮寄主管发送异常情况警告 （磁盘空间不足、服务器响应迟缓）。

监视和维护日志文件

Messaging Server 为其支持的每个主要协议或服务（包括 SMTP、IMAP、POP 和 HTTP）都创建了一组单独的日志文件。这些日志文件位于 *msg_svr_base*/data/log 中。您应当将监视这些日志文件作为例行程序，尤其是在服务器出现问题时。

请注意日志记录可能会影响服务器性能。在给定的时间内，指定的日志记录越详尽，日志文件所占用的磁盘空间越多。您应当为服务器定义有效且实际的日志轮转、到期和备份策略。有关为服务器定义日志记录策略的信息，请参见第 21 章 “管理日志记录”。

设置 msprobe 实用程序

msprobe 实用程序将自动执行监视和重新启动功能。有关详细信息，请参见第 733 页的 “使用 msprobe 和 watcher 功能进行监视”。

监视系统性能

虽然本章着重介绍的是 Messaging Server 监视，但是还需要监视服务器所在的系统。很好配置的服务器在未经过很好优化的系统上无法获得很好的性能，服务器的故障症状可能表明硬件不足以支持电子邮件负载。本章未提供有关监视系统性能的所有详细信息，因为其中的许多过程都是特定于平台的，并且可能要求您参考特定于平台的系统文档。下面介绍了性能监视的过程：

- 第 713 页的 “监视端对端邮件传送时间”
- 第 713 页的 “监视磁盘空间”
- 第 716 页的 “监视 CPU 的使用率”

监视端对端邮件传送时间

电子邮件需要按时传送。这可能是一项服务协议要求，但尽快传送邮件也是一个很好的策略。较长的端对端时间可能预示着许多问题。可能是服务器运行不正常，或者是在一天中的特定时间内发生了邮件超负荷的情况，或者是对现有硬件资源的使用已经超出了它们的能力。

低效的端对端邮件传送时间的症状

邮件的传送时间比正常情况下要长。

监视端对端邮件传送时间

- 使用任何发送和接收邮件的工具。比较服务器中继器之间的标题时间以及起始点和检索点之间的时间。请参见第 724 页的 “immonitor-access”。

监视磁盘空间

磁盘空间不足是导致邮件服务器出现问题和故障的最常见原因之一。如果没有用于写入到 MTA 队列或写入到邮件存储的空间，邮件服务器将会失败。此外，除非监视并清除日志文件，否则它们会无节制地增长并填满所有磁盘空间。

邮件存储分区将随着新邮件传送到邮箱而增长；例如，如果不强制邮件存储配额，邮件存储可能会超出分区的可用磁盘空间。导致磁盘空间耗尽的另一个原因是 MTA 邮件队列增长得过大。涉及的第三个方面为问题是否因日志文件监视工具和日志文件增长失控而发生。（请注意，有许多日志文件，例如 LDAP、 MTA 和邮件访问，其中的每个日志文件都可以存储在不同的磁盘上。）

磁盘空间问题的症状

根据耗尽空间的磁盘或分区不同，所出现的症状会有所不同。MTA 队列会溢出并拒绝 SMTP 连接，邮件可能保留在 ims_master 队列中而没有传送到邮件存储，并且日志文件会溢出。

如果邮件存储分区填满，则邮件访问守护进程可能会失败，邮件存储数据可能会被破坏。邮件存储维护实用程序（例如 `imexpire` 和 `reconstruct`）可以修复损坏并减少磁盘空间的使用。但是，这些实用程序需要其他磁盘空间，而且修复填满整个磁盘的分区可能会导致停机时间。

监视磁盘空间

根据系统配置，您可能需要监视各种磁盘和分区。例如， MTA 队列、邮件存储和日志文件可能分别位于不同的磁盘 / 分区上。其中的每个空间都需要监视，并且监视这些空间的方法也可能不同。

Messaging Server 提供特定的方法，以监视邮件存储磁盘空间的使用并防止分区填满所有可用磁盘空间。

您可以执行以下步骤来监视邮件存储磁盘空间的使用情况：

- 设置参数以监视邮件存储磁盘空间的使用
- 达到磁盘使用量阈值时锁定邮件存储分区

有关详细信息，请参见以下内容：" 监视邮件存储 " 和 " 监视邮件存储分区 "。

监视邮件存储

建议邮件存储的磁盘用量不要超过磁盘容量的 75%。您可以通过配置以下警报属性（使用 `configutil` 实用程序）来监视邮件存储的磁盘用量：

- `alarm.diskavail.msgalarmstatinterval`
- `alarm.diskavail.msgalarmthreshold`
- `alarm.diskavail.msgalarmwarninginterval`
- `alarm.diskavail.msgalarmdescription`

通过设置这些参数，您可以指定系统应监视磁盘空间的频率以及系统应在什么情况下发送警告。例如，如果您希望系统每 600 秒监视磁盘空间一次，请指定以下命令：

```
configutil -o alarm.diskavail.msgalarmstatinterval -v 600
```

如果您希望无论何时当可用磁盘空间低于 20% 时都接收到警告，请指定以下命令：

```
configutil -o alarm.diskavail.msgalarmthreshold -v 20
```

有关这些参数的详细信息，请参见表 23-6 第 735 页。

监视邮件存储分区

当邮件分区填充超过可用磁盘空间的指定百分比时，您可以停止向邮件存储分区传送邮件。设置两个 configutil 参数以启用此功能并指定磁盘使用量阈值即可完成此设置。

邮件存储守护进程可以使用此功能来监视分区磁盘使用量。随着磁盘使用量的增加，存储守护进程将更加频繁地动态检查分区 （从每 100 分钟一次到每 1 分钟一次）。

如果磁盘使用量超过指定的阈值，存储守护进程将：

- 锁定该分区。外来邮件将保存在 MTA 邮件队列中而不传送到邮件存储分区中的邮箱。
- 将邮件记录到默认日志文件中。
- 向邮寄主管发送电子邮件通知。（您可以通过设置 configutil 参数 alarm.msgalarmnoticercpt 来更改电子邮件的收件人。）

磁盘使用量降至阈值以下时，分区将取消锁定，邮件将再次传送到存储。

configutil 参数如下：

- local.store.checkdiskusage 启用分区监视功能。

  允许的值：yes、 no

  默认值：yes

- local.store.diskusagethreshold 指定磁盘使用量阈值。local.store.diskusagethreshold 的值为 1% 到 99%。

  默认值：99

应将磁盘使用量阈值设置为一个足够低的百分比，以便有时间重新进行分区或为本地邮件存储指定更多的磁盘空间。

例如，假设分区以每小时 2% 的速率填充磁盘空间，并且需要一个小时的时间为本地邮件存储分配其他磁盘空间。在这种情况下，应将磁盘使用量阈值设置为低于 98% 的值。

监视 *MTA* 队列和日志记录空间

您需要监视 MTA 队列和日志记录空间的磁盘用量。

有关管理日志空间的信息，请参见 第 21 章 “管理日志记录”例如，要了解如何监视 mail.log 文件，请参见第 647 页的 “管理 MTA 邮件和连接日志”。

监视 CPU 的使用率

高 CPU 使用率表明针对该使用级别没有足够的 CPU 容量，或者某些进程使用的 CPU 循环超出了正常范围。

CPU 使用问题的症状

系统响应时间长。用户的登录缓慢。传送率低。

监视 CPU 使用率

监视 CPU 使用率是一个特定于平台的任务。请参考相关的平台文档。

监视 MTA

本节包含以下小节：

- 第 716 页的 “监视邮件队列的大小”
- 第 717 页的 “监视传送失败率”
- 第 717 页的 “监视入站 SMTP 连接”
- 第 718 页的 “监视分发程序和作业控制器进程”

监视邮件队列的大小

邮件队列的过度增长可能表明邮件没有被传送出去，或者传送被延迟，或者传入的速度比系统所能传送它们的速度要快。这可能是由多种原因造成的，例如由系统中泛滥的大量邮件导致拒绝服务攻击，或者作业控制器未运行。

有关邮件队列的更多信息，请参见第 177 页的 “通道邮件队列”、第 697 页的 “邮件未被排出队列”和第 698 页的 “未传送 MTA 邮件”。

邮件队列问题的症状

- 磁盘空间用量增长。
- 用户没有在合理的时间内收到邮件。
- 邮件队列大小异常大。

监视邮件队列的大小

监视邮件队列的最好方法可能是使用 `imsimta qm`。请参见第 731 页的 “imsimta qm counters”。

您也可以监视队列目录 (*msg_svr_base*/data/queue/) 中的文件的数量。文件数量是特定于站点的，您需要建立一个基线历史记录以找出文件数量 “过多”的标准。这可以通过记录两周内队列文件的大小获得一个近似平均值来完成。

监视传送失败率

传送失败是指尝试将邮件传送给外部站点时失败。传送失败率的大幅增加可能是网络问题 （例如 DNS 服务器死机或者远程服务器在响应连接时超时）的信号。

传送失败率的症状

没有外部症状。 `mail.log_current` 中会出现许多 `Q` 记录。

监视传送失败率

传送失败将记录在 MTA 日志中，并具有日志记录条目代码 `Q`。可以查看文件 *msg_svr_base*/data/log/mail.log_current 中的记录。示例：

```
mail.log:06-Oct-2003 00:24:03.66 501d.0b.9 ims-ms    Q  5
durai.balusamy@Sun.COM rfc822;durai.balusamy@Sun.COM durai@ims-ms-daemon
<00ce01c38bda$c7e2b240$6501a8c0@guindy> Mailbox is busy
```

监视入站 SMTP 连接

来自给定 IP 地址的入站 SMTP 连接数的异常增长可能表示：

- 外部用户正在尝试转发邮件。
- 外部用户正在尝试进行拒绝服务攻击。

未经授权的 SMTP 连接的症状

- **外部用户转发邮件**：没有外部症状。
- **拒绝服务攻击**：外部用户尝试用邮件请求使 SMTP 服务器过载。

监视入站 SMTP 连接

- **外部用户转发邮件**：在 *msg_svr_base*/log/mail.log_current 中查找具有日志记录条目代码 J（拒绝的转发）的记录。要启用远程 IP 地址的日志记录，请向 option.dat 文件添加以下行：

  ```
  log_connection=1
  ```

  请注意，启用此功能要付出少量性能代价。

- **拒绝服务攻击**：要查找连接到 SMTP 服务器的用户及其数量，您可以运行命令 netstat 并检查 SMTP 端口 （默认值：25）上的连接。示例：

```
Local address       Remote address                                  State
192.18.79.44.25     192.18.78.44.56035    32768   0  32768    0   CLOSE_WAIT
192.18.79.44.25     192.18.136.54.57390    8760   0  24820    0   ESTABLISHED
192.18.79.44.25     192.18.26.165.48508   33580   0  24820    0   TIME_WAIT
```

请注意，您首先需要确定系统的 SMTP 连接的适当数目及其状态 （ESTABLISHED、CLOSE_WAIT 等），以便确定某个特定的读取是否超出了正常范围。

如果发现许多连接处于 SYN_RECEIVED 状态，则这可能是由断开的网络或拒绝服务攻击造成的。此外， SMTP 服务器进程的生存期是有限的。这是由 dispatcher.cnf 文件中的 MTA 配置变量 MAX_LIFE_TIME 控制的。默认值为 86,400 秒 （一天）。类似地， MAX_LIFE_CONNS 指定了服务器进程在其生存期内所能处理的最大连接数。如果发现某个特定的 SMTP 服务器已经运行了很长时间，则可能需要进行调查。

监视分发程序和作业控制器进程

分发程序和作业控制器进程必须运行， MTA 才能工作。您应当具有每一种进程。

分发程序和作业控制器进程故障的症状

如果分发程序出现故障或没有足够的资源，则 SMTP 连接将被拒绝。

如果作业控制器出现故障，则队列的大小将增加。

监视分发程序和作业控制器进程

检查以确定存在名为 dispatcher 和 job_controller 的进程。请参见第 686 页的 “检查作业控制器和分发程序是否正在运行”。

监视 LDAP 目录服务器

本节包含以下小节：

- 第 719 页的 “监视 slapd”

监视 slapd

LDAP 目录服务器 (slapd) 为邮件传送系统提供了目录信息。如果 slapd 出现故障，系统将无法正常工作。如果 slapd 响应时间太长，则会影响登录速度以及任何需要 LDAP 查找的其他事务。

slapd 问题的症状

- 客户机 POP、 IMAP 或 Webmail 验证失败或者比预期的速度慢。
- MTA 无法正常工作

监视 slapd

- 检查 ns-slapd 进程是否在运行。
- 检查 slapd-*instance*/logs/ 中的 slapd 日志文件 access 和 errors
- 检查搜索用户时 ns-slapd 的响应时间。
- 查看 Console 来监视 slapd。
- 请参见第 724 页的 “immonitor-access”。

监视邮件访问

本节包含以下小节：

- 第 720 页的 “监视 imapd、 popd 和 httpd”
- 第 721 页的 “监视 stored”

监视 imapd、 popd 和 httpd

这些进程提供了对 IMAP、POP 和 Webmail 服务的访问。如果其中的任何进程未运行或未响应，则服务将无法正常工作。如果服务正在运行，但是出现了过载情况，您可以通过监视检测到这种情况并对其进行更合适的配置。

imapd、 popd 和 httpd 问题的症状

连接被拒绝或系统的连接速度太慢。例如，如果 IMAP 未在运行而您尝试连接到 IMAP 目录，则会看到类似如下的内容：

```
telnet 0 143
Trying 0.0.0.0...
telnet: Unable to connect to remote host: Connection refused
```

如果尝试与客户机连接，则会收到一条消息，例如：

```
Client is unable to connect to the server at the location you have
specified. The server may be down or busy.
```

监视 imapd、 popd 和 httpd

- 可以使用 `watcher` 和 `msprobe` 进行监视。请参见第 101 页的 “失败的服务或未响应服务的自动重新启动”和第 733 页的 “使用 msprobe 和 watcher 功能进行监视”
- 可以使用 SNMP 进行监视。

  如果您设置了 SNMP，则这是监视这些进程的一个非常好的方法。请参见附录 A “SNMP 支持”。服务器信息位于网络服务监视 MIB 中。
- 检查日志文件。

  在目录 *msg_svr_base*`/log/`*service* 中查找，其中 *service* 可以是 http、 IMAP 或 POP。在该目录中，您会找到许多日志文件。其中一个文件名是 *service* 的名称（imap、 pop 或 http），其他文件名是服务名称加上序列号以及连接到该服务名称的日期。例如：

  ```
  imap  imap.29.1010221593 imap.31.1010394412  imap.33.1010567224
  ```

  只具有服务名称的文件是最新的日志。其他文件按序列号排列 （在这里是 29、31、 33），序列号最大的文件是次新的文件。（请参见第 21 章 “管理日志记录”。）

  如果服务器被关闭，您可能会看到类似如下的内容：

  ```
  imap.12.1065431243:[07/Oct/2003:01:15:43 -0700] gotmail-2
  imapd[20525]: General Warning: Sun Java System Messaging Server
  IMAP4 6.1 (built Sep 24 2003) shutting down
  ```

- 可以使用 counterutil 进行检查。请参见第 724 页的 “counterutil”和 Sun Java System Messaging Server Administration Reference。
- 运行特定于平台的命令来验证 imapd、 popd 和 httpd 进程是否正在运行。例如，在 Solaris 中，您可以使用 ps 命令并查找 imapd、 popd 和 mshttpd。
- 您可以通过设置服务器响应配置参数 （如第 735 页的 “警报邮件”中所述）为指定的服务器性能阈值设置警报。
- 请参见第 724 页的 “immonitor-access”。

监视 stored

stored 可执行各种重要的任务，例如邮件数据库的死锁和事务操作、强制执行生存期策略以及擦除和删除磁盘上存储的邮件。如果 stored 停止运行，则邮件传送服务器最终将出现问题。如果 start-msg 运行时 stored 未启动，则其他进程也不会启动。有关 stored 的详细信息，请参见 Sun Java System Messaging Server Administration Reference。

stored 问题的症状

没有外部症状。

监视 stored

- 检查 stored 进程是否正在运行。 stored 将在 *msg_svr_base*/config 中创建和更新一个名为 pidfile.store 的 pid 文件。 pid 文件在恢复时会显示 init 状态，在就绪时会显示 ready 状态。例如：

  ```
  231: cat pidfile.store
  28250
  ready
  ```

  第一行中的数字是 stored 的进程 ID。

  ```
  232: ps -eaf | grep stored
  inetuser 28250     1  0   Jan 05 ? 8:44 /opt/SUNWmsgsr/lib/stored -d
  ```

- 检查在 *msg_svr_base*/store/mboxlist 中生成的日志文件。请注意，并非每个生成的日志文件都是直接由 stored 问题造成的。如果 imapd 中断或出现数据库问题，也可能会生成日志文件。

- 检查 *msg_svr_base*/config 中以下文件上的时间戳：

  stored.ckp — 当尝试进行检查点操作时触及该文件。应当每 1 分钟标记一次时间戳
  stored.lcu — 每次清除数据库日志时触及该文件。应当每 5 分钟标记一次时间戳
  stored.per — 每次产生精读用户数据库写出时触及该文件。应当每 60 分钟标记一次时间戳

- 在默认日志文件 *msg_svr_base*/log/default/default 中检查 stored 邮件
- 可以使用 watcher 和 msprobe 进行监视。请参见第 101 页的 “失败的服务或未响应服务的自动重新启动”和第 733 页的 “使用 msprobe 和 watcher 功能进行监视”

监视邮件存储

邮件存储在数据库中。用户在磁盘上的分布、用户邮箱大小以及磁盘要求都会影响存储性能。以下几个部分介绍了这些因素：

- 第 714 页的 “监视磁盘空间”
- 第 722 页的 “监视邮件存储数据库锁定的状态”
- 第 723 页的 “监视 mboxlist 目录中的数据库日志文件的数目”
- 第 537 页的 “监视配额限制”

监视邮件存储数据库锁定的状态

数据库锁定的状态由不同的服务器进程保留。这些数据库锁定可以影响邮件存储的性能。在死锁情况下，邮件将无法以合理的速度插入到存储中，并且最终会使 ims-ms 通道队列变得很大。由于一些合理的理由，需要将队列备份；因此，为诊断问题而保留队列长度的历史记录是很有用的。

邮件存储数据库锁定问题的症状

事务数目不断积累且没有得到解决。

监视邮件存储数据库锁定

使用命令 counterutil -o db_lock。

监视 mboxlist 目录中的数据库日志文件的数目

数据库日志文件是指 sleepycat 事务检查点操作日志文件 (*msg_svr_base*/store/mboxlist)。如果生成日志文件，则表明没有发生数据库检查点操作。 stored 问题也会导致生成日志文件。

数据库日志文件问题的症状

应当有 2 个或 3 个日志文件。如果有更多的日志文件，则表明可能出现了潜在的严重问题。邮件存储使用了一些用于邮件和配额的数据库，这些数据库的问题会导致所有邮件服务器出现问题。

监视数据库日志文件

在 *msg_svr_base*/store/mboxlist 目录中查看并确保其中只有 2 个或 3 个文件。

用于监视的实用程序和工具

以下工具可用于进行监视：

- 第 724 页的 “stored”
- 第 724 页的 “counterutil”
- 第 728 页的 “日志文件”
- 第 728 页的 “imsimta 计数器”
- 第 731 页的 “imsimta qm counters”
- 第 731 页的 “使用 SNMP 的 MTA 监视”
- 第 732 页的 “用于邮箱配额检查的 imquotacheck”
- 第 733 页的 “使用 msprobe 和 watcher 功能进行监视”

immonitor-access

immonitor-access 可监视以下 Messaging Server 组件 / 进程的状态：邮件传送（SMTP 服务器）、邮件访问和存储 （POP 和 IMAP 服务器）、目录服务 （LDAP 服务器）和 HTTP 服务器。此实用程序可测定各种服务的响应时间以及发送和检索邮件所需的总的往返时间。目录服务是通过在目录中查找指定的用户并测定响应时间来监视的。邮件传送是通过发送邮件 (SMTP) 来监视的，而邮件访问和存储是通过检索邮件来监视的。对 HTTP 服务器的监视限于查看它是否已启动并正在运行。

有关完整的说明，请参见 Sun Java System Messaging Server Administration Reference。

stored

stored 实用程序在服务器上执行维护任务，还可以执行监视任务。但是，监视任务现在受到了 msprobe 的更好地处理。请参见第 733 页的 “使用 msprobe 和 watcher 功能进行监视”。

counterutil

此实用程序提供了从不同系统计数器获得的统计信息。下面是可用计数器对象的当前列表：

```
# /opt/SUNWmsgsr/sbin/counterutil -l
Listing registry (/opt/SUNWmsgsr/data/counter/counter)
numobjects = 11
refcount = 1
created = 25/Sep/2003:02:04:55 -0700
modified = 02/Oct/2003:22:48:55 -0700
       entry = alarm
       entry = diskusage
       entry = serverresponse
       entry = db_lock
       entry = db_log
       entry = db_mpool
       entry = db_txn
       entry = imapstat
       entry = httpstat
       entry = popstat
       entry = cgimsg
```

每个条目都表示一个计数器对象，并且为该对象提供了各种有用的计数。在本节中，我们将只讨论 alarm、diskusage、serverresponse、db_lock、popstat、imapstat 和 httpstat 计数器对象。有关 counterutil 命令的用法的详细信息，请参见 Sun Java System Messaging Server Administration Reference 。

counterutil 输出

counterutil 具有各种标志。此实用程序的命令格式可能为：

```
counterutil -o CounterObject -i 5 -n 10
```

其中，

-o *CounterObject* 表示计数器对象 alarm、diskusage、serverresponse、db_lock、popstat、 imapstat 和 httpstat。

-i 5 指定了 5 秒的时间间隔。

-n 10 表示重复次数 （默认值：无穷大）。

以下是 counterutil 用法的示例：

```
# counterutil -o imapstat -i 5 -n 10
Monitor counteroobject (imapstat)
registry /gotmail/iplanet/server5/msg-gotmail/counter/counter opened
counterobject imapstat opened

count = 1 at 972082466 rh = 0xc0990 oh = 0xc0968

global.currentStartTime [4 bytes]: 17/Oct/2000:12:44:23 -0700
global.lastConnectionTime [4 bytes]: 20/Oct/2000:15:53:37 -0700
global.maxConnections [4 bytes]: 69
global.numConnections [4 bytes]: 12480
global.numCurrentConnections [4 bytes]: 48
global.numFailedConnections [4 bytes]: 0
global.numFailedLogins [4 bytes]: 15
global.numGoodLogins [4 bytes]:  10446
  ...
```

使用 counterutil 的警报统计信息

这些警报统计数据是针对由 stored 发送的警报。警报计数器提供了以下统计数据：

表 23-1 counterutil alarm 统计数据

后缀	说明
alarm.countoverthreshold	超出阈值的次数。

表 23-1 counterutil alarm 统计数据

后缀	说明
alarm.countwarningsent	发送的警告数。
alarm.current	当前监视的值。
alarm.high	所记录的最高值。
alarm.low	所记录的最低值。
alarm.timelastset	上次设置当前值的时间。
alarm.timelastwarning	上次发送警告的时间。
alarm.timereset	上次执行重置的时间。
alarm.timestatechanged	上次更改警报状态的时间。
alarm.warningstate	警告状态 （是 [1] 或否 [0]）。

使用 counterutil 的 IMAP、 POP 和 HTTP 连接统计数据

要获取有关当前 IMAP、 POP 和 HTTP 连接数、失败的登录次数、自开始时间以来的总连接数等的信息，可以使用命令 `counterutil -o` *CounterObject* `-i 5 -n 10`。其中 *CounterObject* 表示计数器对象 `popstat`、 `imapstat` 或 `httpstat`。表 23-2 中显示了 `imapstat` 后缀的含义。`popstat` 和 `httpstat` 对象以相同的格式和结构提供了相同的信息。

表 23-2 counterutil imapstat 统计数据

后缀	说明
currentStartTime	当前 IMAP 服务器进程的开始时间。
lastConnectionTime	上次接受新客户机的时间。
maxConnections	IMAP 服务器处理的最大并行连接数。
numConnections	由当前 IMAP 服务器提供服务的连接总数。
numCurrentConnections	当前的活动连接数。
numFailedConnections	由当前 IMAP 服务器提供服务的失败的连接数。
numFailedLogins	由当前 IMAP 服务器提供服务的失败的登录次数。
numGoodLogins	由当前 IMAP 服务器提供服务的成功的登录次数。

使用 counterutil 的磁盘使用情况统计数据

命令 counterutil -o diskusage 将生成以下信息：

表 23-3 counterutil diskstat 统计数据

后缀	说明
diskusage.availSpace	磁盘分区中的总的可用空间。
diskusage.lastStatTime	上次进行统计的时间。
diskusage.mailPartitionPath	邮件分区路径。
diskusage.percentAvail	可用磁盘分区空间的百分比。
diskusage.totalSpace	磁盘分区中的总空间。

服务器响应统计数据

命令 counterutil -o serverresponse 将生成以下信息。此信息可用于检查服务器是否在运行以及它们响应的速度。

表 23-4 counterutil serverresponse 统计数据

后缀	说明
http.laststattime	上次检查 HTTP 服务器响应的时间。
http.responsetime	HTTP 的响应时间。
imap.laststattime	上次检查 IMAP 服务器响应的时间。
imap.responsetime	IMAP 的响应时间。
pop.laststattime	上次检查 POP 服务器响应的时间。
pop.responsetime	POP 的响应时间。
ldap_host1_389.laststattime	上次检查 ldap_host1_389 服务器响应的时间。
ldap_host1_389.responsetime	ldap_host1_389 的响应时间。
ugldap_host2_389.laststattime	上次检查 ugldap_host2_389 服务器响应的时间。
ugldap_host2_389.responsetime	ugldap_host2_389 的响应时间。

日志文件

Messaging Server 为 SMTP、 IMAP、 POP 和 HTTP 提供事件记录日志。可以自定义创建和管理 Messaging Server 日志文件的策略。

由于日志记录会影响服务器的性能，因此在向服务器添加这一负担之前应当对日志记录进行慎重考虑。有关更多信息，请参阅第 21 章 “管理日志记录”。

imsimta 计数器

MTA 会为其每个活动通道积累邮件通信流量计数器 （基于邮件监视 MIB， RFC 1566）。通道计数器旨在帮助表明电子邮件系统的趋势和运行状况。通道计数器并不用于提供精确的邮件通信流量计数。而要获得精确的计数，请查看 MTA 日志记录，如第 21 章 “管理日志记录”中所述。

MTA 通道计数器是使用可用的最轻量级的机制实现的，以尽可能减小它们对实际操作的影响。通道计数器并不尝试成为强硬功能：如果尝试映射某部分失败，则不会记录任何信息；如果几乎无法立即获得该部分中的其中一个锁定，也不会记录任何信息；当关闭系统时，内存中的部分所包含的信息将永远丢失。

imsimta counters -show 命令提供了 MTA 通道邮件统计数据（请参见下面的内容）。在一段时间过后需要检查这些计数器并记下所看到的最小值。对于某些通道，最小值实际上可能为负数。负值意味着在某个通道的计数器归零时该通道中有排队的邮件 （例如，创建了计数器的群集范围的数据库）。当这些邮件取消排队时，将从该通道所关联的计数器中减去邮件数量，从而导致出现了负的最小值。对于这样的计数器，正确的 “绝对”值是当前值减去计数器自初始化以来曾经具有的最小值。

```
Channel          Messages    Recipients    Blocks
-------          --------    ----------    -------
tcp_local
   Received       29379       79714      982252                        (1)
   Stored            61         113       -2004                        (2)
   Delivered      29369       79723      983903 (29369 first time)     (3)
   Submitted      13698       13699       18261                        (4)
   Attempted          0           0           0                        (5)
   Rejected           1          10           0                        (6)
   Failed           104         104        4681                        (7)

   Queue time/count        16425/29440 = 0.56                           (8)
   Queue first time/count  16425/29440 = 0.56                           (9)

   Total In Assocs           297637
   Total Out Assocs           28306
```

1) Received 是加入到名为 tcp_local 的通道队列中的邮件数。即，由任何其他通道加入到 tcp_local 通道队列中的邮件 （mail.log* 文件中的 E 记录）。

2) Stored 是存储在要被传送的通道队列中的邮件数。

3) Delivered 是已经由通道 tcp_local 处理 （排出队列）的邮件数。（即，mail.log* 文件中的 D 记录。）排出队列操作可能是由于传送成功 （即，加入到另一个通道队列中），也可能是由于邮件被返回给发件人而进行的排出队列操作。通常此值等于 Received 值与 Stored 值之差。

MTA 还跟踪了在第一次尝试时被排出队列的邮件数，此数值显示在括号中。

4) Submitted 是由通道 tcp_local 加入到任何其他通道队列中的邮件数 （mail.log 文件中的 E 记录）。

5) Attempted 是在排除队列过程中遇到临时问题的邮件数 （即，mail.log* 文件中的 Q 记录或 Z 记录。

6) Rejected 是被拒绝的入队尝试次数 （即，mail.log* 文件中的 J 记录）。

7) Failed 是失败的排出队列尝试次数 （即， mail.log* 文件中的 R 记录）。

8) Queue time/count 是所传送的邮件在队列中花费的平均时间。这包括第一次尝试时传送的邮件 （请参见 [9]）以及需要进行额外传送尝试的邮件 （因而通常会在队列中花费很长的闲置等待时间）。

9) Queue first time/count 是第一次尝试时传送的邮件在队列中所花费的平均时间。

请注意，提交的邮件数可能会大于传送的邮件数。这是一个很常见的情况，因为通道排出队列 （传送）的每封邮件都将导致至少一封新邮件入队 （提交），但可能会多于一封。例如，如果一封邮件具有两个收件人 （通过不同的通道到达），则需要进行两次入队。或者，如果邮件退回，则一个副本将返回给发件人，同时另一个副本可能会发送给邮寄主管。通常将有两次提交 （除非两者通过同一个通道到达）。

更常见的情况是， Submitted 和 Delivered 之间的连接会根据通道的类型而不同。例如，在转换通道中，邮件将由任意的某个其他通道入队，然后，转换通道将处理该邮件并将其入队到第三个通道中，同时将该邮件标记为从其自己的队列中排出。每封单独的邮件都将获取一个路径：

```
elsewhere -> conversion   E record   Received
conversion -> elsewhere   E record   Submitted
conversion                 D record   Delivered
```

但是，对于诸如 tcp_local 这样的通道 （它不是一个 “直通式”通道，而是具有两个单独的部分 [从部分和主部分]），在 Submitted 和 Delivered 之间没有连接。Submitted 计数器必须使用 tcp_local 通道的 SMTP 服务器部分，而 Delivered 通道则必须使用 tcp_local 通道的 SMTP 客户机部分。它们是两个完全独立的程序，通过它们传送的邮件也可能是完全独立的。

提交给 *SMTP* 服务器的邮件：

```
tcp_local -> elsewhere  E record    Submitted
```

通过 *SMTP* 客户机发送给其他 *SMTP* 主机的邮件：

```
elsewhere -> tcp_local  E record    Received
tcp_local               D record    Delivered
```

通道的出队列 （传送）操作将导致至少一封新邮件入队 （提交），但可能会多于一封。例如，如果一封邮件具有两个收件人 （通过不同的通道到达），则需要进行两次入队。或者，如果邮件退回，则一个副本将返回给发件人，同时另一个副本可能会发送给邮寄主管。通常将通过同一个通道到达。

在 UNIX 和 NT 上的实现

由于性能原因，运行 MTA 的节点将使用共享的内存部分 （在 UNIX 上）或共享的文件映射对象 （在 NT 上）在内存中保留通道计数器的高速缓存。当该节点上的进程将邮件排入或排出队列时，将更新此内存中的高速缓存中的计数器。如果通道运行时该内存中的部分不存在，则会自动创建该部分。（如果内存中的部分不存在，`imta start` 命令也会创建该部分。）

可以使用命令 `imta counters -clear` 或 `imta qm` 命令 `counters clear` 将计数器重置为零。

imsimta qm counters

`imsimta qm counters` 实用程序可显示 MTA 通道队列邮件计数器。您必须是超级用户或 `inetuser` 用户才能运行此实用程序。输出字段与第 728 页的 “imsimta 计数器”中所述的字段相同。有关用法的详细信息，请参见 Sun Java System Messaging Server Administration Reference。

示例：

```
# imsimta counters -create
# imsimta qm counters show

Channel                 Messages    Recipients     Blocks
---------------------   ----------  ----------    ----------
tcp_intranet
   Received              13077        13859         264616
   Stored                   92           91           -362
   Delivered             12985        13768         264978
   Submitted              2594         2594           3641
...
```

每次重新启动 MTA 时，都必须运行：**`# imsimta counters -create`**

使用 SNMP 的 MTA 监视

Messaging Server 支持通过简单网络管理协议 (SNMP) 进行系统监视。使用 SNMP 客户机 （有时称为**网络管理器**），例如 Sun Net Manager 或 HP OpenView （没有随此产品提供），您可以监视 Messaging Server 的特定部分。有关详细信息，请参阅附录 A “SNMP 支持”。

用于邮箱配额检查的 imquotacheck

您可以使用 imquotacheck 实用程序监视邮箱配额使用情况和限制。 imquotacheck 实用程序将生成列出定义的配额和限制的报告，并提供有关配额使用情况的信息。

例如，以下命令将列出所有用户配额信息：

```
% imquotacheck
--------------------------------------------------------------------------
Domain red.siroe.com (diskquota = not set msgquota = not set) quota usage
--------------------------------------------------------------------------
diskquota        size(K)    %use    msgquota      msgs    %use    user
# of domains = 1
# of users = 705

no quota         50418              no quota      4392            ajonkish
no quota         5                  no quota      2               andrewt
no quota         355518             no quota      2500            aniksri
...
```

以下示例显示了用户 sorook 的配额使用情况：

```
% imquotacheck -u sorook
--------------------------------------------------------------------------
quota usage for user sorook
--------------------------------------------------------------------------
diskquota      size(K)    %use    msgquota      msgs     %use    user

no quota       1487             no quota      305             sorook
```

使用 msprobe 和 watcher 功能进行监视

Messaging Server 提供了两个进程 watcher 和 msprobe 来监视各种系统服务。watcher 将监视服务器崩溃并根据需要重新启动服务器。 msprobe 将监视服务器挂起（不响应）。特别是， msprobe 将监视以下内容：

- **服务器响应时间**。 msprobe 将使用其协议命令连接到已启用的服务器并测定这些服务器的响应时间。如果响应时间超出警报阈值，系统将发送警报邮件 （请参见第 735 页的 “警报邮件”）。如果启用了自动重新启动，当 msprobe 无法连接到服务器或服务器响应时间超出指定的超时值时，则将重新启动服务器。服务器响应时间被同时记录到计数器数据库和默认日志文件中。 counterutil 可用于显示服务器响应时间统计信息 （第 724 页的 “counterutil”）。

  以下服务器由 msprobe 监视：imap、pop、http、cert、job_controller、smtp、lmtp、 mmp 和 ens。 smtp 或 lmtp 未响应时，将重新启动分发程序。无法自动重新启动 ens。

- **磁盘使用量**。 msprobe 将检查每个邮件存储分区的磁盘可用性和使用量。特别是，它将检查邮件存储 mboxlist 数据库目录和 MTA 队列目录。如果磁盘使用量超出了配置的阈值，则发送警报邮件。磁盘大小和使用量被同时记录到计数器数据库和默认日志文件中。管理员可以使用 counterutil 实用程序 （请参见第 724 页的 “counterutil”）来显示磁盘使用量统计信息。

- **邮件存储 mboxlist 数据库日志文件积累**。日志文件积累表明了 mboxlist 数据库错误。 msprobe 计算了活动日志文件的数目，如果活动日志文件的数目大于阈值， msprobe 会将紧急错误消息记录到 default 日志文件中通知管理员重新启动服务器。如果启用了 autorestart （local.autorestart 为 yes），将重新启动存储守护进程。

watcher 和 msprobe 是由 configutil 选项 （如表 23-5 所示）控制的。可以在第 101 页的 “失败的服务或未响应服务的自动重新启动”找到详细信息

表 23-5 msprobe 和 watcher configutil 选项

选项	说明
local.watcher.enable	启用 watcher，用于监视服务失败。 IMAP、 POP、 HTTP、作业控制器、分发程序、邮件存储 (stored)、 imsched 和 MMP。（LMTP/SMTP 服务器由分发程序监视， LMTP/SMTP 客户机由 job_controller 监视。）对于特定失败，会将错误消息记录到默认日志文件中。默认值：启用
local.autorestart	启用服务器自动重新启动。自动重新启动失败或挂起服务。默认值：否
local.autorestart.timeout	失败重试超时。如果服务器在此指定时间内失败超过两次，则系统将停止尝试重新启动服务器。应当将该值 （以秒为单位设置）设置为比 msprobe 间隔 (local.schedule.msprobe) 长的时间段值。默认值：600 秒

表 23-5 msprobe 和 watcher configutil 选项

选项	说明
local.schedule.msprobe	msprobe 运行时间安排。 crontab 式样的时间安排字符串 （请参见表 18-10 第 527 页）。默认值为 600 秒。
service.readtimeout	重新启动之前的默认服务器超时。 默认值：（smtp/lmtp 为 120 秒，其他协议为 30 秒）
local.probe.service.timeout	重新启动之前的特定服务器超时。 *service* 可以是 imap、 pop、 http、 cert、 job_controller、 smtp、 lmtp、 mmp 或 ens。 默认值：使用 service.readtimeout
local.probe.warningthreshold	警告邮件被记录到 default 日志文件之前的服务器非响应秒数。 默认值：5 秒
local.probe.service.warningthreshold	警告邮件被记录到 default 日志文件之前的特定服务器非响应秒数。 *service* 可以是 imap、 pop、 http、 cert、 job_controller、 smtp、 lmtp、 mmp 或 ens。 默认值：使用 local.probe.warningthreshold
local.queuedir	当队列大小超过由 alarm.diskavail.msgalarmthreshold 定义的阈值时，要检查的 MTA 队列目录。 默认值：无
local.schedule.msprobe	msprobe 运行时间安排。值为 crontab 样式的时间安排字符串。 默认值：600 秒
service.readtimeout	重新启动该服务器之前的服务器非响应时段。请参见 local.schedule.msprobe。 默认值：10 秒

警报邮件

msprobe 可以向邮寄主管发出电子邮件形式的警报（请参见第 721 页），针对指定的情况发出警告。下面显示了当超出特定阈值时发送的一个电子邮件警报样例：

```
Subject:ALARM: server response time in seconds of "ldap_siroe.com_389" is 10
Date:Tue, 17 Jul 2001 16:37:08 -0700 (PDT)
From:postmaster@siroe.com
To: postmaster@siroe.com

Server instance: /opt/SUNWmsgsr
Alarmid: serverresponse
Instance: ldap_siroe_europa.com_389
Description: server response time in seconds
Current measured value (17/Jul/2001:16:37:08 -0700): 10
Lowest recorded value: 0
Highest recorded value: 10
Monitoring interval: 600 seconds
Alarm condition is when over threshold of 10
Number of times over threshold:  1
```

您可以指定 msprobe 监视磁盘和服务器性能的频率，以及在什么情况下发送警报。这可以通过使用 configutil 命令设置警报参数来完成。表 23-6 显示了有用的警报参数及其默认设置。有关完整列表，请参见 Sun Java System Messaging Server Administration Reference。

表 23-6 有用的警报邮件 configutil 参数

参数	说明 （括号中为默认设置）
alarm.msgalarmnoticehost	(localhost) 向其发送警告邮件的计算机。
alarm.msgalarmnoticeport	(25) 发送警报邮件时要连接的 SMTP 端口。
alarm.msgalarmnoticercpt	(Postmaster@localhost) 向其发送警报通知的用户。
alarm.msgalarmnoticesender	(Postmaster@localhost) 警报发件人的地址。
alarm.diskavail.msgalarmdescription	（可用邮件分区磁盘空间的百分比。）磁盘可用性警报的说明字段的文本。
alarm.diskavail.msgalarmstatinterval	(3600) 磁盘可用性检查之间的时间间隔 （秒）。设置为 0 将禁用磁盘使用情况的检查。
alarm.diskavail.msgalarmthreshold	(10) 当磁盘空间的可用性低于此百分比时将发送警报。

表 23-6 有用的警报邮件 configutil 参数 （续）

参数	说明 （括号中为默认设置）
alarm.diskavail.msgalarmthresholddirection	(-1) 指定当磁盘空间的可用性低于阈值 (-1) 或高于阈值 (1) 时是否发出警报。
alarm.diskavail.msgalarmwarninginterval	(24). 后续重复的磁盘可用性警报之间的时间间隔 （小时）。
alarm.serverresponse.msgalarmdescription	（以秒为单位的服务器响应时间。）服务器响应警报的说明字段的文本。
alarm.serverresponse.msgalarmstatinterval	(600) 服务器响应检查之间的时间间隔 （秒）。设置为 0 将禁用服务器响应的检查。
alarm.serverresponse.msgalarmthreshold	(10) 如果服务器响应时间超过此值 （秒），则发出警报。
alarm.serverresponse.msgalarmthresholddirection	(1) 指定当服务器响应时间大于 (1) 或小于 (-1) 阈值时是否发出警报。
alarm.serverresponse.msgalarmwarninginterval	(24) 后续重复的服务器响应警报之间的时间间隔 （小时）。

附录 A

SNMP 支持

Messaging Server 支持通过简单网络管理协议 (SNMP) 进行系统监视。使用 SNMP 客户机 （有时称作**网络管理器**），例如 Sun Net Manager 或 HP OpenView （不随此产品提供），可以监视 Messaging Server 的特定部分。有关监视 Messaging Server 的详细信息，请参见第 23 章 “监视 Messaging Server”。

本章介绍如何启用 Messaging Server 的 SNMP 支持功能。同时还概述了 SNMP 所提供的信息类型。请注意，本章不介绍如何从 SNMP 客户机查看此信息。有关如何使用 SNMP 客户机查看基于 SNMP 的信息的详细信息，请参见 SNMP 客户机文档。本文档还介绍了 Messaging Server SNMP 实现的某些可用数据，但有关完整的 MIB 详细信息，请参见 RFC 2788 和 RFC 2789。

本章由以下各节组成：

- 第 738 页的 “SNMP 实现”
- 第 739 页的 “在 Solaris 8 中为 Messaging Server 配置 SNMP 支持”
- 第 740 页的 “通过 SNMP 客户机监视”
- 第 741 页的 “与 Unix 平台中的其他 Sun Java System 产品共存”
- 第 741 页的 “来自 Messaging Server 的 SNMP 信息”

SNMP 实现

Messaging Server 实现两个标准的 MIB，即网络服务监视 MIB (RFC 2788) 和邮件监视 MIB (RFC 2789)。网络服务监视 MIB 提供对网络服务 （例如 POP、 IMAP、HTTP 和 SMTP 服务器）的监视。邮件监视 MIB 提供对 MTA 的监视。邮件监视 MIB 允许监视每个 MTA 通道的状态，包括活动状态和历史状态。活动信息主要是当前排入队列的邮件和打开的网络连接 （例如，入队邮件的计数、打开的网络连接的源 IP 地址），而历史信息则提供累积总数 （例如，已处理邮件总数、外来连接的总数）。

注 有关 Messaging Server SNMP 监视信息的完整列表，请参见 RFC 2788 和 RFC 2789。

在 Solaris 8 和 9 以及 Java Enterprise System 所支持的所有版本的 Microsoft Windows 平台上均支持 SNMP。以后的版本中会有其他平台的支持。 Solaris 中的 SNMP 支持使用本地 Solaris SNMP 技术 Solstice Enterprise Agent (SEA)。用户无需在 Solaris 8 系统中安装 SEA：所需的运行时库都已经存在。

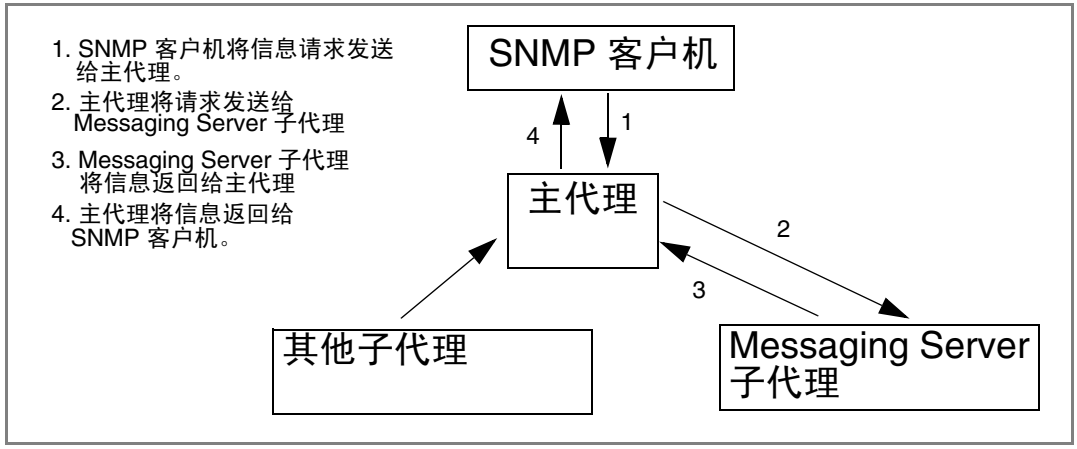
对 Messaging Server SNMP 支持的限制如下：

- 每个主机中只能通过 SNMP 监视一个 Messaging Server 实例。
- SNMP 支持仅用于监视。不支持 SNMP 管理。
- 不实现 SNMP 陷阱。（RFC 2788 提供相似的功能，但不使用陷阱。）

Messaging Server 中的 SNMP 操作

在 Solaris 平台上， Messaging Server SNMP 进程是一个 SNMP 子代理，该子代理在启动时将自身注册到平台的本机 SNMP 主代理。来自客户机的 SNMP 请求进入主代理。主代理将发送给 Messaging Server 的所有请求转发给 Messaging Server 子代理进程。 Messaging Server 子代理进程将处理请求，并通过主代理将响应重新转发给客户机。图 A-1 显示了该进程。

图 A-1 SNMP 信息流



在 Solaris 8 中为 Messaging Server 配置 SNMP 支持

尽管 SNMP 监视的开销非常小，但 Messaging Server 出厂时仍然禁用了 SNMP 支持。要启用 SNMP 支持，请运行以下命令：

```
# su user-id-for-ims
# configutil -o local.snmp.enable -v 1
# start-msg snmp
```

启用 SNMP 后， `start-msg` 命令 （无需指定任何参数）将自动启动 SNMP 子代理进程和其他 Messaging Server 进程。

请注意，必须运行 Solaris 本地 SNMP 主代理， Messaging ServerSNMP 子代理才能操作。 Solaris 本地 SNMP 主代理是 `snmpdx` 守护程序，此程序通常作为 Solaris 引导过程的一部分启动。

SNMP 子代理将自动选择要侦听的 UDP 端口。如果需要，可以使用以下命令为子代理指定固定的 UDP 端口：

```
# configutil -o local.snmp.port -v port-number
```

以后可以通过将此端口号的值指定为零来撤销此设置。缺省设置零告诉 Messaging Server 允许子代理自动选择任意可用的 UDP 端口。

有两个 SNMP 子代理配置文件放置在 `/etc/snmp/conf` 目录中：`ims.acl` 包含 SNMP 访问控制信息，而 `ims.reg` 包含 SNMP MIB OID 注册信息。

通常无需编辑这两个文件。 Messaging Server 分发的 MIB 是只读的，而且无需在 `ims.reg` 文件中指定端口号。如果指定了端口号，该端口号将生效，除非使用 `configutil` 实用程序设置了另一端口号。在这种情况下，使用 `configutil` 设置的端口号是子代理将要使用的端口号。如果编辑了文件，则需要使用以下命令停止并重新启动 SNMP 子代理才能使更改生效：

```
# stop-msg snmp
# start-msg snmp
```

通过 SNMP 客户机监视

RFC 2788 和 RFC 2789 的基本 OID 是

mib-2.27 = 1.3.6.1.2.1.27

mib-2.28 = 1.3.6.1.2.1.28

将您的 SNMP 客户机指向上述两个 OID，并将其作为 “公用” SNMP 社区访问。

如果要将 MIB 副本装入 SNMP 客户机，可以在 *msg_svr_base*`/lib/config-templates` 目录的文件名 `rfc2788.mib` 和 `rfc2789.mib` 下查找 MIB 的 ASCII 副本。有关在 SNMP 客户机软件中装入 MIB 的指导信息，请参见 SNMP 客户机软件文档。某些较旧的 SNMP 客户机可能无法识别这些 MIB 中使用的 `SnmpAdminString` 数据类型。在这种情况下，请使用位于同一目录中的等效文件 `rfc2248.mib` 和 `rfc2249.mib`。

与 Unix 平台中的其他 Sun Java System 产品共存

提供 SNMP 支持的其他 Netscape 或 Sun Java System 产品可能通过取代平台的本机 SNMP 主代理来做到这一点。如果要在同一主机中运行 Messaging Server 这样的 Sun Java System 产品，并要通过 SNMP 对两种产品进行监视，请按照 Managing Servers with iPlanet Console (http://docs.sun.com/source/816-5572-10/11_snmp.htm) 第 11 章所述配置 Sun Java System Proxy SNMP Agent。这将允许 Messaging Server SNMP 子代理 （本机 SNMP 子代理）与其他 Sun Java System 产品中的非本机 Sun Java System SNMP 子代理共存。

来自 Messaging Server 的 SNMP 信息

本节概括了通过 SNMP 提供的 Messaging Server 信息。有关详细信息，请参见 RFC 2788 和 RFC 2789 中的单个 MIB 表。请注意， RFC/MIB 术语将邮件传送服务（MTA、 HTTP 等）称作**应用程序** (`appl`)，将 Messaging Server 网络连接称作**关联** (`assoc`)，将 MTA 通道称作 *MTA* **组** (`mtaGroups`)。

请注意，在可以同时监视多个 Messaging Server 实例的平台中， `applTable` 中可能会有多组 MTA 和服务器，其他表中可能会有多个 MTA。

注 重新引导后将把 MIB 中报告的累积值 （例如，被传送邮件的总数、IMAP 连接总数等）重置为零。

每个站点都有不同的阈值和重要的监视值。好的 SNMP 客户机允许进行趋势分析，并在突然出现背离历史趋势的情况时发送警告。

applTable

`applTable` 提供服务器信息。它是一维表格，一行用于 MTA，其他每一行用于以下一个服务器 （如果已启用）：WebMail HTTP、 IMAP、 POP、 SMTP 和 SMTP Submit。该表提供版本信息、正常运行时间、当前操作状态 （up、 down、 congested）、当前连接数量、累积连接总数和其他相关数据。

以下是 applTable (mib-2.27.1.1) 数据的示例。

```
applTable:

    applName.1[1] = mailsrv-1[2] MTA on mailsrv-1.west.sesta.com
    applVersion.1 = 5.1
    applUptime.1 = 7322[3]
    applOperStatus.1 = up[4]
    applLastChange.1 = 7422[3]
    applInboundAssociations.1 = 5
    applOutboundAssociations.1 = 2
    applAccumulatedInboundAssociations.1 = 873
    applAccumulatedOutboundAssociations.1 = 234
    applLastInboundActivity.1 = 1054822[3]
    applLastOutboundActivity.1 = 1054222[3]
    applRejectedInboundAssociations.1 = 0[5]
    applFailedOutboundAssociations.1 = 17
    applDescription.1 = Sun Java System Messaging Server 6.1
    applName.2[1] = mailsrv-1 HTTP WebMail server on mailsrv-1.west.sesta.com
    ...
    applName.3 = mailsrv-1 IMAP server on mailsrv-1.west.sesta.com
    ...
    applName.4 = mailsrv-1 POP server on mailsrv-1.west.sesta.com
    ...
    applName.5 = mailsrv-1 SMTP server on mailsrv-1.west.sesta.com
    ...
    applName.6 = mailsrv-1 SMTP Submit server on mailsrv-1.west.sesta.com
    ...
```

说明：

1. 此处的 .1、.2 等后缀是行编号 applIndex。applIndex 的值 1 代表 MTA，值 2 代表 HTTP 服务器，等等。因此，在此示例中，表格第一行提供 MTA 中的数据，第二行提供 POP 服务器中的数据，等等。
2. 受监视的 Messaging Server 实例的名称。在此示例中，实例名称是 mailsrv-1。
3. 这些是 SNMP 时间戳值，是事件发生时 sysUpTime 的值。而 sysUpTime 是 SNMP 主代理启动后以百分之一秒为单位的计数。
4. 通过已配置的 TCP 端口实际连接到 HTTP、 IMAP、 POP、 SMTP 和 SMTP Submit 服务器，并使用适当协议 （例如，用于 HTTP 的 HEAD 请求和响应，用于 SMTP 的 HELO 命令和响应等）执行简单操作可以确定这些服务器的运行状态。通过此连接尝试可以确定每个服务器的状态 — up (1)、down (2) 或 congested (4)。

   请注意，这些探测看似正常的服务器外来连接，并影响每个服务器的 applAccumulatedInboundAssociations MIB 变量的值。

对于 MTA，操作状态即作业控制器的操作状态。如果 MTA 显示为 “up”，则作业控制器也为 "up" 。如果 MTA 显示为 "down" ，则作业控制器也为 "down" 。该 MTA 操作状态独立于 MTA 的服务分发程序的状态。MTA 的操作状态只有 up 值或 down 值。尽管作业控制器有 "congested" 这一概念，但 MTA 状态中没有此概念。

5. 对于 HTTP、 IMAP 和 POP 服务器， `applRejectedInboundAssociations` MIB 变量表示失败的登录尝试的数量，而不是被拒绝的外来连接尝试的数量。

applTable 的用法

监视每个列出的应用程序的服务器状态 (`applOperStatus`) 对于监视每个服务器是至关重要的。

如果自最后一次 MTA 外来活动 （如 `applLastInboundActivity` 所表示）已经过了很久，则可能出现了故障，因而无法连接。如果 `applOperStatus=2` (down)，则监视服务已关闭。如果 `applOperStatus=1` (up)，则问题可能出在其他地方。

assocTable

该表提供 MTA 的网络连接信息。这是二维表格，提供有关每个活动的网络连接的信息。不提供其他服务器的连接信息。

以下是 applTable (mib-2.27.2.1) 数据的示例。

```
assocTable:

    assocRemoteApplication.1.1[1] = 129.146.198.167[2]
    assocApplicationProtocol.1.1[1] = applTCPProtoID.25[3]
    assocApplicationType.1.1 = peerinitiator(3)[4]
    assocDuration.1.1 = 400[5]
...
```

说明：

1. 在后缀 .x.y 中， x 是应用程序索引 `applIndex`，表示报告的是 `applTable` 中的哪个应用程序。在此示例中为 MTA。 y 用于枚举所报告的应用程序的每个连接。
2. 远程 SMTP 客户机的源 IP 地址。
3. 这是一个 OID，表示网络连接所使用的协议。 `aplTCPProtoID` 表示 TCP 协议。后缀 .n 表示使用的 TCP 端口， .25 表示基于 TCP 端口 25 使用 SMTP 协议。
4. 无法判断远程 SMTP 客户机是用户代理 (UA) 还是其他 MTA。因此，子代理始终报告 `peer-initiator` ； 而从不报告 `ua-initiator`。

5. 这是 SNMP `TimeInterval`，以百分之一秒为单位。在此示例中，连接已打开 4 秒钟。

assocTable 的用法

该表用来诊断活动问题。例如，如果突然有 200,000 个外来连接，查看此表可以知道它们的来源。

mtaTable

这是一维表格，每一行用于 `applTable` 表中的一个 MTA。每一行为 `mtaGroupTable` 中的选定变量提供了该 MTA 中所有通道 （称作组）的总数。

以下是 `applTable` (mib-2.28.1.1) 中的数据的示例。

```
mtaTable:

    mtaReceivedMessages.1[1] = 172778
    mtaStoredMessages.1 = 19
    mtaTransmittedMessages.1 = 172815
    mtaReceivedVolume.1 = 3817744
    mtaStoredVolume.1 = 34
    mtaTransmittedVolume.1 = 3791155
    mtaReceivedRecipients.1 = 190055
    mtaStoredRecipients.1 = 21
    mtaTransmittedRecipients.1 = 3791134
    mtaSuccessfulConvertedMessages.1 = 0[2]
    mtaFailedConvertedMessages.1 = 0
    mtaLoopsDetected.1 = 0[3]
```

说明：

1. 在 `applTable` 中，后缀 `.x` 为此应用程序提供了行编号。在此示例中， `.1` 表示此数据用于 `applTable` 中第一个应用程序。因此，这是 MTA 中的数据。
2. 对于转换通道，仅使用非零值。
3. 对当前存储在 MTA 邮件队列中的 `.HELD` 邮件文件进行计数。

mtaTable 的用法

如果 `mtaLoopsDetected` 不为零，则存在循环邮件问题。请查找并诊断 MTA 队列中的 `.HELD` 文件以解决问题。

如果系统对转换通道进行病毒扫描并拒绝被感染邮件，则除了其他转换失败外，`mtaSuccessfulConvertedMessages` 还将给出被感染邮件的计数。

mtaGroupTable

此二维表格提供 applTable 中每个 MTA 的通道信息。此信息包括诸如已存储 （即已入队）邮件消息计数和已传送邮件消息计数等数据。监视每个通道的已存储邮件 (mtaGroupStoredMessages) 的计数是很重要的：当该值变得异常庞大时，邮件正在队列中备份。

以下是 mtaGroupTable (mib-2.28.2.1) 数据的示例。

```
mtaGroupTable:

mtaGroupName.1.1[1] = tcp_intranet[2]
        ...
mtaGroupName.1.2[1] = ims-ms
        ...
mtaGroupName.1.3[1] = tcp_local
    mtaGroupDescription.1.3 = mailsrv-1 MTA tcp_local channel
    mtaGroupReceivedMessages.1.3 = 12154
    mtaGroupRejectedMessages.1.3 = 0
    mtaGroupStoredMessages.1.3 = 2
    mtaGroupTransmittedMessages.1.3 = 12148
    mtaGroupReceivedVolume.1.3 = 622135
    mtaGroupStoredVolume.1.3 = 7
    mtaGroupTransmittedVolume.1.3 = 619853
    mtaGroupReceivedRecipients.1.3 = 33087
    mtaGroupStoredRecipients.1.3 = 2
    mtaGroupTransmittedRecipients.1.3 = 32817
    mtaGroupOldestMessageStored.1.3 = 1103
    mtaGroupInboundAssociations.1.3 = 5
    mtaGroupOutboundAssociations.1.3 = 2
    mtaGroupAccumulatedInboundAssociations.1.3 = 150262
    mtaGroupAccumulatedOutboundAssociations.1.3 = 10970
    mtaGroupLastInboundActivity.1.3 = 1054822
    mtaGroupLastOutboundActivity.1.3 = 1054222
    mtaGroupRejectedInboundAssociations.1.3 = 0
    mtaGroupFailedOutboundAssociations.1.3 = 0
    mtaGroupInboundRejectionReason.1.3 =
    mtaGroupOutboundConnectFailureReason.1.3 =
    mtaGroupScheduledRetry.1.3 = 0
    mtaGroupMailProtocol.1.3 = applTCPProtoID.25
    mtaGroupSuccessfulConvertedMessages.1.3 = 0[3]
    mtaGroupFailedConvertedMessages.1.3 = 0
    mtaGroupCreationTime.1.3 = 0
    mtaGroupHierarchy.1.3 = 0
    mtaGroupOldestMessageId.1.3 = <01IFBV8AT8HYB4T6UA@red.iplanet.com>
    mtaGroupLoopsDetected.1.3 = 0[4]
    mtaGroupLastOutboundAssociationAttempt.1.3 = 1054222
```

说明：

1. 在后缀 .x.y 中， x 是应用程序索引 applIndex，表示报告的是 applTable 中的哪个应用程序。在此示例中为 MTA。 y 用于枚举 MTA 中的每个通道。枚举索引 mtaGroupIndex 也用于 mtaGroupAssociationTable 和 mtaGroupErrorTable 表。
2. 所报告的通道的名称。在此示例中为 tcp_intranet 通道。
3. 对于转换通道，仅使用非零值。
4. 对当前存储在此通道的邮件队列中的 .HELD 邮件文件进行计数。

mtaGroupTable 的用法

对 *Rejected* 和 *Failed* 的趋势分析可能有助于确定潜在的通道问题。

mtaGroupStoredVolume 对 mtaGroupStoredMessages 的比率突然增高可能意味着队列附近正退回一个巨大的垃圾邮件。

mtaGroupStoredMessages 突然增高可能表示正在发送非请求的批量电子邮件或由于某种原因导致传送失败。

如果 mtaGroupOldestMessageStored 的值大于无法传送的邮件通知次数（notices 通道关键字）的值，则可能表示即使采用退回处理也无法处理该邮件。请注意，退回在夜间进行，因此您需要使用 mtaGroupOldestMessageStored > （最大生存期 + 24 小时）进行测试。

如果 mtaGroupLoopsDetected 大于 0，则检测到邮件循环。

mtaGroupAssociationTable

这是三维表格，其条目是 assocTable 的索引。对于 applTable 中的每个 MTA，都有一个二维子表。此二维子表中的每一行用于相应 MTA 中的一个通道。对于每个通道，通道当前正在进行的每一个活动的网络连接都有一个条目。该条目的值是 assocTable 的索引 （通过条目的值以及正在查看的 MTA 的 applIndex 索引进行索引）。这表示 assocTable 中的条目是通道所拥有的网络连接。

简而言之， mtaGroupAssociationTable 表将 assocTable 中所示的网络连接与 mtaGroupTable 中的重要通道相关联。

以下是 mtaGroupAssociationTable (mib-2.28.3.1) 中的数据的示例。

```
mtaGroupAssociationTable:

    mtaGroupAssociationIndex.1.3.1[1] = 1[2]
    mtaGroupAssociationIndex.1.3.2 = 2
    mtaGroupAssociationIndex.1.3.3 = 3
    mtaGroupAssociationIndex.1.3.4 = 4
    mtaGroupAssociationIndex.1.3.5 = 5
    mtaGroupAssociationIndex.1.3.6 = 6
    mtaGroupAssociationIndex.1.3.7 = 7
```

说明：

1. 在后缀 .x.y.z 中， x 是应用程序索引 applIndex，它表示报告的是 applTable 中的哪个应用程序。在此示例中为 MTA。y 表示报告的是 mtaGroupTable 的哪个通道。在此示例中，3 表示 tcp_local 通道。z 用于枚举向通道打开或来自通道的关联。
2. 该值是 assocTable 的索引。具体地说， x 和该值分别成为 applIndex 和 assocIndex 在 assocTable 中的索引值。或者，换句话说 （忽略 applIndex），assocTable 中的第一行说明了 tcp_local 通道控制的网络连接。

mtaGroupErrorTable

这又是三维表格，它给出尝试传送邮件时每个 MTA 的每个通道遇到的临时错误和永久性错误的计数。索引值为 4000000 的条目是临时错误，索引值为 5000000 的条目是永久性错误。临时错误导致将邮件重新入队，以后再尝试传送；永久性错误导致邮件被拒绝或作为无法传送的邮件被返回。

以下是 `mtaGroupErrorTable` (mib-2.28.5.1) 中的数据的示例。

```
mtaGroupErrorTable:

    mtaGroupInboundErrorCount.1.1.4000000[1] = 0
    mtaGroupInboundErrorCount.1.1.5000000 = 0
    mtaGroupInternalErrorCount.1.1.4000000 = 0
    mtaGroupInternalErrorCount.1.1.5000000 = 0
    mtaGroupOutboundErrorCount.1.1.4000000 = 0
    mtaGroupOutboundErrorCount.1.1.5000000 = 0

    mtaGroupInboundErrorCount.1.2.4000000[1] = 0
    ...

    mtaGroupInboundErrorCount.1.3.4000000[1] = 0
    ...
```

说明：

1. 在后缀 `.x.y.z` 中， `x` 是应用程序索引 `applIndex`，它表示报告的是 `applTable` 中的哪个应用程序。在此示例中为 MTA。`y` 表示报告的是 `mtaGroupTable` 的哪个通道。在此示例中， 1 指定 tcp_intranet 通道， 2 指定 ims-ms 通道， 3 指定 tcp_local 通道。最后， `z` 为 4000000 或 5000000，分别表示为该通道尝试邮件传送时遇到的临时性错误和永久性错误的计数。

mtaGroupErrorTable 的用法

错误计数的突然增高很可能表示出现不正常的传送问题。例如， tcp_ 通道的错误计数突然增高可能表示出现 DNS 问题或网络问题。 ims_ms 通道的错误计数突然增高可能表示向邮件存储传送邮件时遇到问题（例如，分区已满、 `stored` 问题，等等）。

在 Messaging Server 中管理事件通知服务

本附录介绍启用 Event Notification Service Publisher (ENS Publisher) 以及管理 Messaging Server 中的 Event Notification Service (ENS) 所需的操作。

本章 / 附录包含以下各节：

- 在 Messaging Server 中装入 ENS Publisher
- 运行样例事件通知服务程序
- 管理事件通知服务

有关 ENS 和 ENS API 的更多信息，请参见位于 http://docs.sun.com/db/coll/CalendarServer_05q1 和 http://docs.sun.com/db/coll/CalendarServer_05q1_zh 的 Sun Java System Calendar Server 中的 Sun Java System Communications Services 的事件服务通知手册和位于 http://docs.sun.com/db/coll/MessagingServer_05q1 和 http://docs.sun.com/db/coll/MessagingServer_05q1_zh 的 Messaging Server 文档 Web 页面。

在 Messaging Server 中装入 ENS Publisher

事件通知服务 (ENS) 是基本的发布和订阅服务。 ENS 起着分发程序的作用， Sun Java System 应用程序将它用作这些应用程序感兴趣的、某些类型**事件**的集合的中心点。事件是对资源的一个或多个属性的值所作的更改。任何要了解这些类型的事件何时发生的应用程序将使用 ENS 注册， ENS 按顺序标识事件，并使通知与订阅相匹配。

ENS 和 iBiff （用于 Messaging Server 的 ENS Publisher）被捆绑为与 Messaging Server 一起启动。默认情况下启用了 ENS，但是未装入 iBIFF。请参见 “在 Messaging Server 上装入 ENS Publisher”。

要在 Messaging Server 中订阅通知，您需要在 Messaging Server 主机上装入 `libibiff` 文件，然后停止并重新启动邮件传送服务器。

在 Messaging Server 上装入 ENS Publisher

从命令行执行以下步骤。在这些步骤中， Messaging Server 安装目录的位置为 *msg_svr_base*， Messaging Server 用户为 *inetuser*。这些变量的典型值分别为 `/opt/SUNWmsgsr` 和 `inetuser`。

1. 作为 `inetuser` 时，请运行 `configutil` 实用程序以装入 `libibiff` 文件。

   `cd` *msg_svr_base*

   `./configutil -o "local.store.notifyplugin" -v "`*msg_svr_base*`/lib/libibiff"`**

2. 作为超级用户时，请先停止然后重新启动邮件传送服务器。

   `cd` *msg_svr_base*`/sbin`

   `./stop-msg`

   `./start-msg`

3. 现在准备通过 ENS 接收通知。有关更多信息，请参见 " 运行样例事件通知服务程序 "。

运行样例事件通知服务程序

Messaging Server 包含帮助您了解如何接收通知的样例程序。这些样例程序位于 *msg_svr_base*`/examples` 目录。

运行样例 ENS 程序

1. 更改到 *msg_svr_base*`/examples` 目录。
2. 使用 C 编译器编译使用 `Makefile.sample` 文件的 `apub` 和 `asub` 实例。将库搜索路径设置为包含 *msg_svr_base*`/examples` 目录。

3. 编译了程序之后，您可以在不同的窗口中按如下所示运行这些程序：

   apub localhost 7997

   asub localhost 7997

   在 apub 窗口中键入的任何内容都应显示在 asub 窗口中。此外，如果您使用默认设置，则所有 iBiff 通知均应显示在 asub 窗口中。

4. 要接收由 iBiff 发布的通知，请写入与 asub.c 类似的程序

   有关样例程序以及编写您自己的 ENS 程序的详细信息，请参见 iPlanet Event Notification Service for Messaging and Collaboration Manual。

注 将库搜索路径设置为包含 *msg_svr_base*/lib 目录之后，您将不能再停止和启动目录服务器。解决方法是从库搜索路径中删除该条目。

管理事件通知服务

管理 ENS 包括启动和停止该服务以及更改配置参数以控制用于 ENS 的 iBiff publisher 的性能。

启动和停止 ENS

您可以使用 start-msg ens 和 stop-message ens 命令启动和停止 ENS 服务器。您必须是超级用户才可以运行这些命令。

启动和停止 ENS

- 要启动 ENS，请运行以下命令：

  msg_svr_base/**sbin/start-msg ens**

- 要停止 ENS，请运行以下命令：

  msg_svr_base/**sbin/stop-msg ens**

iPlanet Event Notification Service 配置参数

若干配置参数控制 iBiff 的性能。可以使用 configutil 实用程序来设置这些参数。

表 B-1 iBiff 配置参数

参数	说明
local.store.notifyplugin.maxHeaderSize	指定将与通知一起传送的标题的最大大小 （以字节为单位）。默认值为 0 字节。
local.store.notifyplugin.maxBodySize	指定将与通知一起传送的主体的最大大小 （以字节为单位）。默认值为 0 字节。
local.store.notifyplugin.*eventType*.enable	指定给定的事件类型是否将生成通知。有关各种 *eventTypes*，例如 ReadMsg、 NewMsg 等，请参见 *Messaging Server for Messaging and Collaboration Manual*。合法值为 1 （要启用）和 0 （要禁用）。默认值为 1；即，将 local.store.notifyplugin.ReadMsg.enable 设置为 0 将禁用 ReadMsg 通知。
local.store.notifyplugin.ensHost	指定 ENS 服务器的主机名。默认值为 127.0.0.1。
local.store.notifyplugin.ensPort	指定 ENS 服务器的 TCP 端口。默认值为 7997。
local.store.notifyplugin.ensEventKey	指定要用于 ENS 通知的事件密钥。默认值为 enp://127.0.0.1/store。事件密钥的主机名部分不用来确定 ENS 主机。它只是 ENS 所使用的唯一标识符。 此密钥是订户应订阅的，以便获得与该密钥相匹配的事件的通知。

使用 Console 界面管理邮件用户和邮件列表 （不建议采用此方式）

本附录仅供参考。**请不要如本附录中所述使用 Console 界面创建和管理用户和邮递列表**。使用如用户管理实用程序等其他经批准的置备工具。

注意 使用 Console 界面创建用户和组将导致各种问题。使用如 Delegated Administrator 等其他经批准的置备工具。请参阅 Sun Java System Messaging Server 管理指南 (http://docs.sun.com/doc/819-1056)。

本附录仅供参考。建议您**不要**使用 Console 界面创建和管理您的用户的邮件帐户和邮递列表。

管理邮件用户

访问邮件用户

本节介绍如何为您的用户打开邮件管理界面。 Messaging Server 邮件帐户作为用户条目的属性存储在您企业的中心 LDAP 用户目录中。因此，要管理邮件帐户，您可以修改该目录中的用户条目。

创建新用户

要创建新邮件帐户，您可以在目录中创建新用户。您还必须为该用户安装一个邮件帐户，如果不安装邮件帐户，该用户将不能使用 Console 的邮件管理部分。（《Sun ONE Server Console 5.2 Server Management Guide 》中的 "User and Group Administration" 一章中更加详细地介绍了创建用户和指定其他类型用户信息的完整过程。）

要创建新邮件用户，请执行以下操作：

1. 在 Console 主窗口中，单击 “用户和组”选项卡。
2. 从下拉列表中，选择 “新用户”并单击 “创建”。
3. 为用户选择一个组织单位然后单击 “确定”。将打开 “创建用户”窗口。
4. 输入《Sun ONE Server Console 5.2 Server Management Guide》的 "User and Group Administration" 一章中所述的有关用户的信息。
5. 保持打开 “创建用户”窗口并单击 “帐户”选项卡。新用户帐户的已安装的产品列表将显示在右窗格中。
6. 单击 “邮件帐户安装”框。“创建用户”窗口中将显示 “邮件”选项卡。
7. 在 “创建用户”窗口中单击 “邮件”选项卡，然后在右窗格中单击所需的选项卡。
8. 输入您的更改，然后在 “创建用户”窗口的底部单击 “确定”。

注 确保在单击 “确定”之前完成相关选项卡中的所有设置过程。

访问现有用户

要修改现有邮件帐户或向现有用户添加邮件功能，您可以访问用户目录中的相应用户，然后添加或修改该用户的邮件帐户属性。

要访问现有用户的邮件信息，请执行以下操作：

1. 在 Console 主窗口中，单击 “用户和组”选项卡。
2. 在 “用户和组”主窗口中，单击 “搜索”或 “高级搜索”。
3. 在 “搜索”窗口中输入搜索条件 （例如用户的姓），然后执行用户目录的搜索。
4. 返回到 “用户和组”主窗口，从搜索结果中选择一个用户，然后单击 “编辑”。
5. 如果 “邮件”选项卡没有显示在 “编辑条目”窗口中，请执行以下操作：
   a. 单击 “帐户”选项卡。右窗格中将显示已安装的帐户的列表。
   b. 选中 “邮件帐户”框。“邮件”选项卡将显示在 “编辑条目”窗口中。

6. 在 “编辑条目”窗口中单击 “邮件”选项卡，然后在右窗格中单击所需的选项卡。

7. 输入您的更改，然后在 “编辑条目”窗口的底部单击 “确定”。

指定用户电子邮件地址

您必须为用户指定邮件寻址信息，然后才能将邮件成功传送给该用户。此信息包括 Messaging Server 主机名、用户的主地址以及任何备用地址。主机名和主地址信息是必需的，备用地址信息是可选的。

要指定用户的邮件寻址信息，请执行以下操作：

1. 在 Console 中，访问 “创建用户”或 “编辑条目”窗口，如第 753 页的 “访问邮件用户”中所述。

2. 单击 “邮件”选项卡。

3. 单击 “设置”选项卡 （如果它尚不是活动的选项卡）。

4. （必需）输入 Messaging Server 主机名。

   这是托管将处理此用户的邮件的 Messaging Server 的计算机。这必须是该计算机上的 Messaging Server 所知晓的全限定域名 (FQDN)。

5. （必需）输入用户的主电子邮件地址。

   这是公布的地址，此用户的邮件将发送到该地址。一个用户只能有一个主地址，它必须是有效的、具有正确格式的 SMTP 地址 （符合 RFC 821 规范）。

   如果希望隐藏主机名 （用户地址中的主机名不显示在外发邮件的标题中），请不要在 “主电子邮件地址”字段中指定主机名，而应当输入一个包含主机名的备用地址，如下一步中所述。

6. （可选）向 “备用地址”列表中添加地址。

   备用地址实质上是用户主地址的别名。您可以使用此功能执行下列操作：

   - 确保正确地传送经常拼错的地址 （例如，将 "Smith" 当作 "Smythe" 的别名）。
   - 在外发邮件标题中启用主机名隐藏功能。要实现此目的，请提供包含主机名的备用地址，而不要在用户的主电子邮件地址中包含主机名。例如，输入 `jsmith@siroe.com` 作为主电子邮件地址，然后输入 `jsmith@sesta.com` 作为备用地址。当此用户发送邮件时，外发邮件的标题将显示 `jsmith@siroe.com`，但是所有发送到该地址的邮件 （包括回复）实际上都被路由到 `jsmith@sesta.com` （假设 `sesta.com` 是有效的主机名）。

您可以为特定用户指定任意数量的备用地址，只要每个地址都是唯一的。发送给任何这些别名的邮件都将被定向到主地址。

要添加备用地址，请执行以下操作：

a. 单击 “备用地址”字段下面的 “添加”按钮。

b. 在 “备用地址”窗口中，输入备用地址。（您可以添加任意数量的备用地址，但是每次打开此窗口时只能输入一个地址。）

c. 单击 “确定”以添加备用地址并关闭 “备用地址”窗口。（要输入另一个备用地址，请再次单击 “添加”以重新打开 “备用地址”窗口。）

7. 如果完成了对此用户的邮件信息的更改，请在 “编辑条目”窗口的底部单击 “确定”。否则，请单击其他选项卡以继续进行更改。

配置传送选项

Messaging Server 支持三个主要的邮件传送选项，您可以为每个用户按任意组合启用和配置这些选项。您可以提供常规的 POP/IMAP 传送、程序传送以及 UNIX 传送 （适用于 UNIX Messaging Server 主机的客户机）。

如果使用的是 iPlanet Delegated Administrator for Messaging，它还提供了最终用户 HTML 界面，通过该界面用户可以自己启用和配置这些选项。 Console 界面和 iPlanet Delegated Administrator 界面可以处理相同的目录属性；打开时，两者都将显示当前设置，无论这些设置是由管理员还是由用户设置的。

注 Delegated Administrator for Messaging 只支持 Sun Java System LDAP Schema v.1，而不支持 v.2

要为用户配置传送选项，请执行以下操作：

1. 在 Console 中，访问 “创建用户”或 “编辑条目”窗口，如第 753 页的 “访问邮件用户”中所述。

2. 单击 “邮件”选项卡。

3. 单击 “传送”选项卡。

4. 选择要为此用户启用的传送方法：

- 要指定 POP/IMAP 传送，请按照第 757 页的 “指定 POP/IMAP 传送”中的说明操作。
- 要指定程序传送，请按照第 757 页的 “指定程序传送”中的说明操作。

- 要指定 UNIX 传送，请按照第 758 页的 “指定 UNIX 传送”中的说明操作。

5. 如果完成了对此用户的邮件信息的更改，请在 “编辑条目”窗口的底部单击 “确定”。否则，请单击其他选项卡以继续进行更改。

指定 POP/IMAP 传送

指定此选项将使邮件传送到用户的常规 POP3 或 IMAP4 邮箱。要为此用户启用 POP/IMAP 传送，请执行以下操作：

1. 单击 “传送”选项卡。
2. 选中 “POP/IMAP”框，然后单击 “属性”按钮以打开 “POP/IMAP 传送”窗口。
3. （可选）输入邮件存储分区的昵称 （而不是路径名或绝对物理路径），该用户的邮件将被传送到此分区并在其中存储以供处理。如果将此字段保留为空白，将使用当前主分区。有关更多信息，请参见第 491 页的 “管理邮件存储”。
4. （可选）输入要分配给该用户的存储限制或磁盘配额。配额可以是指定的默认值（请参见第 512 页的 “配置邮件存储配额”或无限制的 （没有最大存储限制），您也可以指定一个限制 （以 KB 或 MB 为单位）。
5. （可选）输入要分配给该用户的邮件数量限制。此限制可以是指定的默认值（请参见第 512 页的 “配置邮件存储配额”）或无限制的 （没有最大存储限制），您也可以指定一个限制 （数字）。

指定程序传送

指定此选项提供这样一个机制，即，将邮件转发给某个外部应用程序进行处理，然后再传送给用户。

注 本节只介绍如何使程序传送选项可供单个用户使用。您必须首先整体启用程序传送模块 （这需要执行若干其他管理任务），然后才能使其可供用户使用。

要为此用户启用程序传送，请执行以下操作：

1. 单击 “传送”选项卡。
2. 选中 “程序传送”框，然后单击 “属性”按钮以打开 “程序传送”窗口。
3. 输入要用来处理此用户的邮件的外部应用程序命令。
4. 单击 “确定”。

指定 UNIX 传送

指定此选项将为此用户选择 UNIX 传送。 UNIX 传送功能可以将邮件传送到用户的指定 UNIX 邮箱。 UNIX 传送仅对其 Messaging Server 在 UNIX 主机上运行的用户可用。

要为此用户启用 UNIX 传送，请执行以下操作：

1. 单击 “传送”选项卡。
2. 选中 “UNIX 传送”框。

注	要将 UNIX 传送提供给 Messaging Server 用户，您还必须执行常规的 UNIX 邮件管理任务

指定转发地址

Messaging Server 的邮件转发功能可以将用户的邮件转发到另一个地址而不是该用户的主地址，或者除了主地址以外再转发到另一个地址。

Delegated Administrator for Messaging 提供了最终用户 HTML 界面，通过该界面用户可以自己指定转发地址。 Console 界面和 Delegated Administrator 界面可以处理相同的目录属性；打开时，两者都将显示当前设置，无论这些设置是由管理员还是由用户设置的。

注	Delegated Administrator for Messaging 只支持 Sun Java System LDAP Schema v. 1，而不支持 v.2

要为用户指定转发地址信息，请执行以下操作：

1. 在 Console 中，访问 “创建用户”或 “编辑条目”窗口，如第 753 页的 “访问邮件用户”中所述。
2. 单击 “邮件”选项卡。
3. 单击 “转发”选项卡。

   “转发地址”字段显示了该用户当前的转发地址集 （如果有）。
4. 要添加转发地址，请单击 “添加”。
5. 在 “转发地址”窗口中，输入转发地址。
6. 单击 “确定”将该地址添加到 “邮件转发”选项卡的 “转发地址”字段中，然后关闭 “转发地址”窗口。

7. 如果完成了对此用户的邮件信息的更改，请在 “编辑条目”窗口的底部单击 “确定”。否则，请单击其他选项卡以继续进行更改。

注 对于同一个 Messaging Server 上的两个用户，如果这两个用户帐户都没有启用其他传送类型，请不要将他们的转发地址设置为指向彼此，否则会导致邮件传送问题。

配置自动回复设置

Messaging Server 的自动回复功能使您可以为用户指定对外来邮件的自动响应。您可以指定两种不同的自动回复模式：休假模式和自动回复模式。

Delegated Administrator for Messaging 还提供了最终用户 HTML 界面，通过该界面用户可以自己启用和配置自动回复设置。 Console 界面和 Delegated Administrator 界面可以处理相同的目录属性；打开时，两者都将显示当前设置，无论这些设置是由管理员还是由用户设置的。

注 Delegated Administrator for Messaging 只支持 Sun Java System LDAP Schema v.1，而不支持 v.2

要为用户启用自动回复服务，请执行以下操作：

1. 在 Console 中，访问 “创建用户”或 “编辑条目”窗口，如第 753 页的 “访问邮件用户”中所述。
2. 单击 “邮件”选项卡。
3. 单击 “自动回复”选项卡。
4. 选择其中一种自动回复模式：

   关闭：对此用户禁用自动回复。

   休假：此用户从给定发件人处收到第一封邮件后将生成一个自动响应；从该发件人处收到后续邮件将不会生成响应，直到自动回复超时。如果超时，系统将发送一封新邮件，到下一次超时再发送一封，以此类推。如果选择此模式，您可以使用 “休假开始 / 结束日期”选项并在 “回复文本”字段中输入回复邮件。

5. 如果选择休假模式，请提供日期和时间以确定自动回复邮件应当在何时开始和结束：

   - 选中 “休假开始 / 结束日期”复选框。
   - 单击 “开始”和 “结束”的 “编辑”按钮，然后使用显示的日历指定日期和时间。

6. 指定自动回复超时值 （小时或天）。
7. 如果选择了休假模式，请键入一个自动回复主题行，然后键入要返回给发件人的回复邮件。

   您可以分别为内部发件人和外部发件人键入回复邮件。如果只为内部发件人键入回复，则只有在您域中的发件人会收到自动回复。

   您可以使用若干种可用语言中的每种语言来创建邮件，可以从位于邮件文本区域上方的下拉列表中选择语言。
8. 如果完成了对此用户的邮件信息的更改，请在 “编辑条目”窗口的底部单击 “确定”。否则，请单击其他选项卡以继续进行更改。

配置授权服务

要启用使此用户可以访问邮件的邮件服务，请执行以下操作：

1. 在 Console 中，访问 “创建用户”或 “编辑条目”窗口，如第 753 页的 “访问邮件用户”中所述。
2. 单击 “邮件”选项卡。
3. 单击 “授权服务”选项卡。

   “授权服务”窗口将显示应用于特定域的服务。
4. 您可以通过单击相关联的按钮来添加、编辑或删除服务。将显示 “修改授权服务的规则”窗口。
5. 从服务下拉列表中，选择要为其创建规则的服务 （“IMAP”、“POP”、“SMTP”、“HTTP”和 “全部”）。
6. 指定 “允许”或 “拒绝”并指定此规则要应用到的域。
7. 单击 “确定”以提交所作的更改。

管理邮递列表

访问邮递列表

本节介绍如何访问用于邮递列表的管理界面。由于 Messaging Server 邮递列表是作为组条目的属性存储在 LDAP 用户目录中，因此管理邮递列表意味着要访问和修改目录组。

创建新组

要创建新邮递列表，您可以在目录中创建一个新组。您还必须为该组安装一个邮件帐户，如果不安装邮件帐户，该组将不能使用 Console 的邮件管理部分。（《Sun ONE Server Console 5.2 Server Management Guide 》中的 "User and Group Administration" 一章中更加详细地介绍了创建目录组和指定其他类型组信息的完整过程。）

要创建新邮递列表，请执行以下操作：

1. 在 Console 主窗口中，单击 “用户和组”选项卡。
2. 从下拉列表中，选择 “新组”然后单击 “创建”。
3. 为该组选择一个组织单位，然后单击 “确定”。
4. 在 “创建组”窗口中，输入创建组条目所需的信息，如 《 Sun ONE Server Console 5.2 Server Management Guide 》中的 "User and Group Administration" 一章中所述。

   请注意，如果只是为了处理邮递列表，则**不必**使用 “用户和组”的 “成员”选项卡来添加成员，您可以使用 “邮件”帐户的 “仅电子邮件成员”选项卡进行添加：

   - 常规组成员具有完全的邮递列表权限，但是他们也可以具有其组成员资格所表示的任何其他权限。您可以通过 “成员”选项卡来添加常规成员 （静态或动态的）。
   - 邮递列表成员具有组权限，这些权限被限制为由该组的邮递列表组件提供的权限 （这可能是该组存在的唯一目的，也可能不是）。邮递列表成员被称为**仅电子邮件成员**，您可以通过 “邮件”选项卡添加他们。
5. 保持打开 “创建组”窗口并单击 “帐户”选项卡。

   组帐户的已安装的产品列表将显示在右窗格中。

6. 单击 “邮件帐户” 框。

   “创建组” 窗口中将显示 “邮件” 选项卡。

7. 在 “创建组” 窗口中单击 “邮件” 选项卡，然后在右窗格中单击适当的选项卡。

8. 输入您的更改，然后在 “创建组” 窗口的底部单击 “确定”。

   此操作将提交您的条目并关闭 “创建组” 窗口。

注 在任何邮件管理窗口的底部单击 “确定” 都将提交在所有邮件管理选项卡中输入的所有当前邮件配置信息。确保在单击 “确定” 之前完成相关窗口中的所有设置过程。

访问现有组

要修改现有邮递列表或者向现有组添加邮递列表功能，您可以访问用户目录中的相应组，然后添加或修改其邮件帐户属性。

要访问现有组的邮递列表信息，请执行以下操作：

1. 在 Console 主窗口中，单击 “用户和组” 选项卡。

2. 在 “用户和组” 主窗口中，单击 “搜索” 或 “高级搜索”。

3. 在 “搜索” 窗口中输入搜索条件 （例如组的名称），然后执行用户目录的搜索。

4. 返回到 “用户和组” 主窗口，从搜索结果中选择一个组并单击 “编辑”。

5. 如果 “邮件” 选项卡没有显示在 “编辑条目” 窗口中，请执行以下操作：

   - 单击 “帐户” 选项卡。右窗格中将显示已安装的帐户的列表。
   - 选中 “邮件帐户” 框。“邮件” 选项卡将显示在 “编辑条目” 窗口中。

6. 在 “编辑条目” 窗口中，单击 “邮件” 选项卡，然后在右窗格中单击所需的选项卡。

   （这些选项卡与您通过 “创建组” 窗口访问的选项卡相同。）

7. 输入您的更改，然后在 “编辑条目” 窗口的底部单击 “确定” 以提交您的修改。

指定邮递列表设置

您必须指定邮递列表的邮件寻址信息，然后邮件才能成功传送到您的邮递列表。此信息包括该组的主地址以及您希望用作主地址的别名的任何备用地址。您还可以指定列表的拥有者以及邮递列表的可选描述性信息、成员、属性、限制和操作 （电子邮件响应）。

要指定邮递列表信息，请执行以下操作：

1. 在 Console 中，访问 “创建组”或 “编辑条目”窗口，如第 761 页的 “访问邮递列表”中所述。
2. 单击 “邮件”选项卡。
3. 单击 “设置”选项卡 （如果它尚不是活动的选项卡）。
4. （必需）输入邮递列表的主电子邮件地址。

   这是公布的地址，此列表的邮件将传送到该地址。一个列表只能有一个主地址。它必须是具有正确格式的 SMTP 地址 （符合 RFC 821 规范）。
5. （可选）为该邮递列表指定备用地址。

   备用地址是组的主地址的别名。您可以使用此功能执行下列操作：

   - 确保经常拼错的地址的正确传送。
   - 在外发邮件标题中启用主机名隐藏功能。要实现此目的，请提供包含主机名的备用地址，而不要在组的主电子邮件地址中包含主机名。

   您可以为组指定任意数量的备用地址，只要每个地址都是唯一的。发送给任何这些别名的邮件都将被定向到主地址。

   要添加备用电子邮件地址，请执行以下操作：

   a. 单击 “备用电子邮件地址”字段下面的 “添加”按钮。

   b. 在 “备用电子邮件地址”窗口中，输入一个备用地址。（您可以添加任意数量的备用地址，但是每次打开此窗口时只能输入一个地址。）

   c. 单击 “确定”以添加备用地址并关闭 “备用电子邮件地址”窗口。（要输入另一个备用地址，请再次单击 “添加”以重新打开 “备用电子邮件地址”窗口。）
6. （可选）在 “将错误消息发至”字段中，输入某人的电子邮件地址，如果在向列表传送邮件时出现错误，则向该地址发送错误消息。

7. （可选）在 “Messaging Server 主机名”字段中，输入托管此邮递列表的计算机的主机名。

   如果此邮递列表的 “主电子邮件地址”字段中包含一个主机名，您可以将此字段保留为空白。如果通过在主电子邮件地址中不包含主机名来隐藏主机名，请在此字段中指定主机名。

   与用户邮件帐户不同，如果您没有为邮递列表指定主机名，则任何能够访问该列表的 LDAP 条目的主机都将能够处理该列表 （在大多数情况下，这正是您希望的）。如果要将对列表的处理限制给一个或多个特定主机，则应当指定一个或多个主机名。例如，您可能希望强制将一个大型组放在一个使用率不高的服务器上进行处理，以便减轻一个使用率很高的服务器的压力。

   请注意，使用此窗口一次只能输入一个主机名。要输入多个主机名，请使用 `ldapmodify` 命令行实用程序。

8. （可选）输入一个邮递列表拥有者。

   列表拥有者具有添加或删除用户、修改配置设置或删除列表的管理权限。

   要指定新的邮递列表拥有者，请单击 “所有者”选项卡，然后执行以下操作之一：

   - 单击 “添加”，然后在 “输入列表所有者的 DN”窗口中输入新邮递列表拥有者的标识名 (DN) （例如， `uid=jsmith, ou=people, o=siroe.com`）并单击 “确定”。
   - 单击 “搜索”，打开 “搜索用户和组”窗口来查找所有者。

   请注意，从 “搜索用户和组”窗口中选择所有者会自动为您添加 DN 的正确语法。有关 “搜索用户和组”窗口的详细信息，请参见 《Sun ONE Server Console 5.2 Server Management Guide》中的 "User and Group Administration" 一章。

9. （可选）添加描述性信息。

   要出于提供信息的目的 （并非供 Messaging Server 使用）添加文本或 URL，请单击 “说明”选项卡，然后选择以下操作之一或两者都选择：

   - 输入邮递列表的用途或特性的说明。
   - 输入指向 HTML 页面的 URL，该页面提供了有关邮递列表的其他信息。这只是用于提供信息； Messaging Server 并不会使用该 URL。

10. 如果完成了对此邮递列表的更改，请在 “编辑条目”窗口的底部单击 “确定”。否则，请单击其他选项卡以继续进行更改。

指定列表成员

要向邮递列表中添加仅电子邮件成员，请使用以下方法之一或两者都使用：

- 向邮递列表中明确添加每个成员。
- 将要应用于用户目录的动态标准定义为确定组成员资格的过滤器。

这里介绍的邮递列表成员在 Console 的 “用户和组”界面中被称为**仅电子邮件成员**，因为他们具有组权限，这些权限被限制为由该组的邮递列表组件提供的权限。您使用该界面的不同部分添加的 “常规”组成员 （如 《Sun ONE Server Console 5.2 Server Management Guide》中的 "User and Group Administration" 一章所述）可能具有邮递列表成员所具有的权限以外的其他权限或责任。有关组的更多信息，请参见 《Sun ONE Server Console 5.2 Server Management Guide》中的 "User and Group Administration" 一章。

定义动态成员资格条件

动态条件由 LDAP 搜索 URL 组成，这些 URL 用作搜索用户目录以确定成员资格的过滤器。这种机制是动态的，即，当邮件到达该组时，收到邮件的各个成员是通过目录搜索确定的，而不是通过查询静态名称列表确定。这样，您便可以创建和维护非常大或非常复杂的组，而不必明确跟踪每个成员。

LDAP 搜索过滤器的格式必须采用 LDAP URL 语法。有关构建 LDAP 过滤器的详细信息，请参见 《 Sun ONE Server Console 5.2 Server Management Guide 》中的 "User and Group Administration" 一章。另请参见 Sun Java System Directory Server 文档和 RFC 1959。

LDAP URL 具有以下语法：

```
ldap://hostname:port/base_dn?attributes?scope?filter
```

其中 URL 的选项具有以下含义：

表 C-1 LDAP URL 选项

选项	说明
hostname	Directory Server 的主机名 （默认值为 Messaging Server 使用的 Directory Server 主机名）。
port	LDAP 服务器的端口号。如果未指定端口，则默认值为 Messaging Server 使用的标准 LDAP 端口。
base_dn	目录中的条目的标识名，将用作搜索基准。此部分是必需的。
attributes	要返回的属性。这些属性由 Messaging Server 提供。

表 C-1 LDAP URL 选项

选项	说明
scope	搜索范围： 范围 `base` 将只检索搜索基准 (*base_dn*) 本身上的信息。 范围 `one` 将检索搜索基准下一级的信息 （不包括搜索基准级别）。 范围 `sub` 将检索搜索基准以及搜索基准以下所有条目上的信息。
filter	应用于指定搜索范围内的条目的搜索过滤器。如果未指定过滤器，将使用 (`objectclass=*`)。

以下是一个 LDAP 搜索 URL 示例，它将过滤出使用 Sunnyvale 作为其邮件主机的用户：

```
ldap:///o=Siroe Corp,c=US??sub?(&(mailHost=sunnyvale.siroe.com)
  (objectClass=inetLocalMailRecipient))
```

上述 URL 将过滤出这样的用户，即，是 Siroe 组织 (`o=Siroe`) 的成员，位于美国 (`c=US`)，并且具有邮件主机 Sunnyvale (`mailHost=sunnyvale`)。 `objectClass` 属性定义了要搜索的条目类型，在本例中是 `inetLocalMailRecipient` (`objectClass=inetLocalMailRecipient`)。

请注意，当您使用 Console 创建搜索过滤器时，将忽略所有组的名称；也就是说，搜索结果中将只包含用户名，而不包含组成员。此设置的目的是为了避免在搜索结果中出现重复的用户 （他们同时也是组成员）。可以使用命令行配置实用程序 (`configutil`) 来覆盖此设置，但是并不建议这样做。

如下一节中所述， Console 提供了一个模板窗口 （“构造 LDAP 搜索 URL”窗口），可以使用其帮助构建搜索 URL。

添加邮递列表成员

要向邮递列表中添加 （仅电子邮件）成员，请执行以下操作：

1. 在 Console 中，访问 “创建组”或 “编辑条目”窗口，如第 761 页的 “访问邮递列表”中所述。
2. 单击 “邮件”选项卡。
3. 单击 “仅电子邮件成员”选项卡。
   - （可选）要指定用于确定成员资格的 LDAP 搜索 URL，请单击 “仅电子邮件成员资格的动态标准”字段下面的 “添加”按钮，然后在 “添加动态标准”窗口中执行以下操作：

- 在字段中输入 LDAP 搜索 URL，或者单击 “构造”按钮以打开 “构造 LDAP 搜索 URL”窗口，这是用于帮助构造搜索 URL 的模板。
- 单击 “确定”将您的输入添加到 “仅电子邮件成员资格的动态标准”字段中并关闭 “添加动态标准”窗口。

有关创建 LDAP 搜索 URL 的说明，请参见第 765 页的 “定义动态成员资格条件”。

4. （可选）要向邮递列表中添加单个成员，请单击 “仅通过电子邮件联系的成员”字段下面的 “添加”按钮，然后在 “添加仅电子邮件成员”窗口中执行以下操作：
   - 在字段中输入新成员的主地址。主地址必须是具有正确格式的 SMTP 地址（符合 RFC 821 规范）。您不应当输入备用地址，特别是您为该组指定了限制时。每次打开此窗口时只能添加一个新成员，该字段无法容纳多个地址。
   - 单击 “确定”将该用户添加到成员列表中并关闭 “添加仅电子邮件成员”窗口。要输入另一个地址，请再次单击 “添加”以重新打开 “添加仅电子邮件成员”窗口。
5. 如果完成了对此邮递列表的更改，请在 “编辑条目”窗口的底部单击 “确定”。否则，请单击其他选项卡以继续进行更改。

定义邮件邮寄限制

您可以为发送给邮递列表的邮件强加各种限制。您可以定义允许其邮寄邮件的用户集，可以要求对发件人进行验证，可以限制邮寄的邮件的来源，并且可以限制邮寄的邮件的大小。违反限制的邮件将被拒绝。

注	虽然这些限制对于为组控制外来邮件的若干方面很有用，但是它们并不能够提供高安全性的访问控制。

要为组定义邮件邮寄限制，请执行以下操作：

1. 在 Console 中，访问 “创建组”或 “编辑条目”窗口，如第 761 页的 “访问邮递列表”中所述。
2. 单击 “邮件”选项卡。
3. 单击 “限制”选项卡。
4. （可选）通过选择以下选项之一定义所允许的发件人：
   - **任何人**：对发件人没有限制。（这是默认设置。）请注意，如果选择此选项，则不能选择下一步中所介绍的 SMTP 验证。

- **邮递列表中的任何人**：只有邮递列表成员 （包括不是仅电子邮件成员的组成员）可以邮寄邮件。
- **以下列表中的任何人**：只有在以下字段中明确列出的那些用户可以邮寄邮件。

如果选择 “以下列表中的任何人”来添加发件人，请单击 “允许的发件人”字段下面的 “添加”，也可以单击 “搜索”打开 “搜索用户和组”窗口。如果单击 “添加”，将打开 “添加允许的发件人”窗口。在字段中输入允许的发件人的电子邮件地址或标识名 (DN)。单击 “确定”将该发件人添加到 “允许的发件人”字段中并关闭 “添加允许的发件人”窗口。对要添加的所有其他允许的发件人重复此步骤。

有关 “搜索用户和组”窗口的说明，请参见 《Sun ONE Server Console 5.2 Server Management Guide》中的 "User and Group Administration" 一章。

5. （可选）定义允许的发件人域以限制发件人可从中邮寄邮件的位置：
   - 单击 “允许的发件人域”字段下面的 “添加”按钮。
   - 在 “添加允许的发件人域”窗口中，输入一个域名，然后单击 “确定”将该域添加到列表中。

   请注意，域将自动包含其所有子域。例如， `siroe.com` 包含 `sales.siroe.com`。
6. （可选）定义所允许的最大邮件大小。

   输入大小 （以字节为单位）。
7. 如果完成了对此邮递列表的更改，请在 “编辑条目”窗口的底部单击 “确定”。否则，请单击其他选项卡以继续进行更改。

定义中介人

您可以为邮递列表添加一个或多个中介人。

当中介人收到转发的邮件时，他将确定如何处理该邮件。（在存在多个中介人的情况下，邮件的处理由第一个中介人采取的操作确定。）处理可能包括批准该邮件并将其转发回列表 （可能带有密码）或将其删除。

要为邮递列表定义中介人，请执行以下操作：

1. 在 Console 中，访问 “创建组”或 “编辑条目”窗口，如第 761 页的 “访问邮递列表”中所述。
2. 单击 “邮件”选项卡。

3. 单击“中介人”选项卡。
4. 单击“列出中介人”字段下面的“添加”按钮。
5. 在“添加中介人”窗口中，在字段中输入中介人的主电子邮件地址或标识名(DN)。您可以明确输入地址，也可以单击“搜索”以使用“搜索用户和组”窗口来查找地址。请注意，每次打开“添加中介人”窗口时只能添加一个中介人。

   有关“搜索用户和组”窗口的说明，请参见《Sun ONE Server Console 5.2 Server Management Guide》中的 "User and Group Administration" 一章。
6. 单击“确定”将中介人添加到“列出中介人”列表中并关闭“添加中介人”窗口。（要输入另一个地址，请再次单击“添加”以重新打开“添加中介人”窗口。）
7. 如果完成了对此邮递列表的更改，请在“编辑条目”窗口的底部单击“确定”。否则，请单击其他选项卡以继续进行更改。

短消息服务 (SMS)

本章说明如何在 Sun™ ONE Messaging Server 上实现短消息服务 (SMS)。本章包含以下主题：

- 第 771 页的 “介绍”
- 第 774 页的 “SMS 通道操作原理”
- 第 788 页的 “SMS 通道配置”
- 第 815 页的 “SMS Gateway Server 操作原理”
- 第 819 页的 “SMS Gateway Server 配置”
- 第 841 页的 “SMS Gateway Server 存储要求”

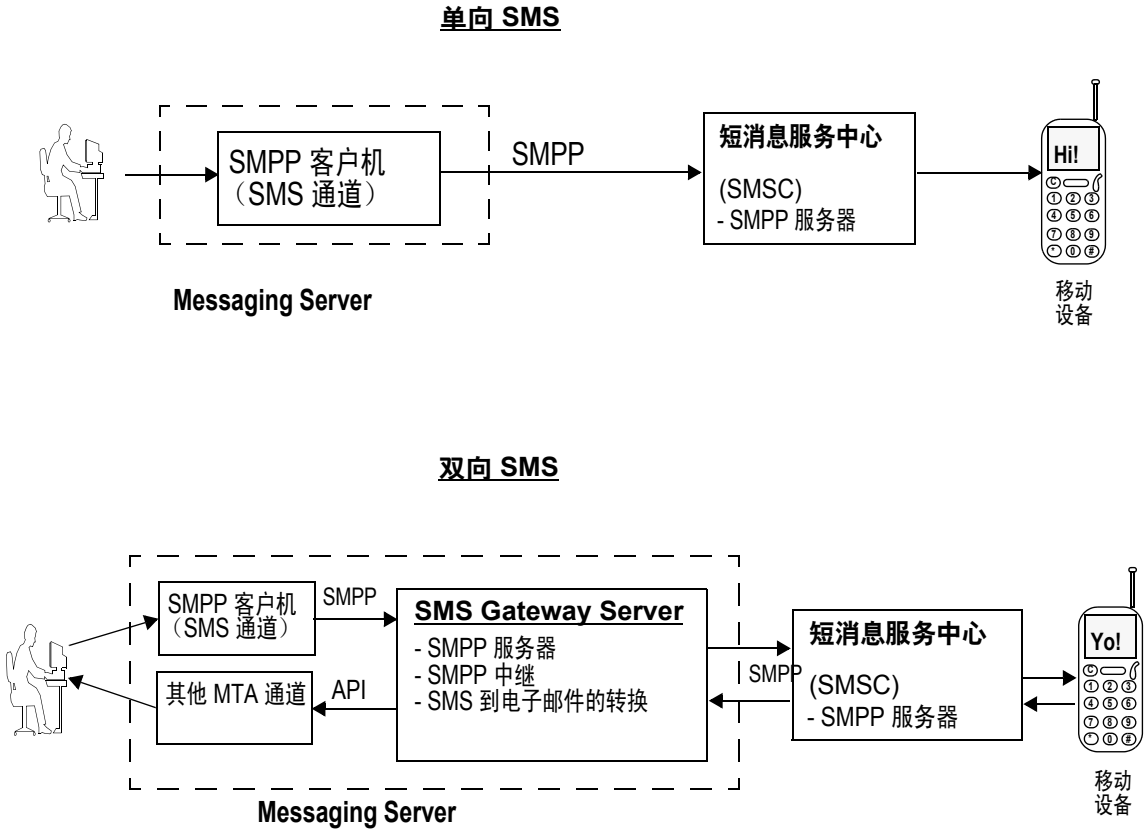
介绍

Sun Java System Messaging Server 通过短消息服务 (SMS) 实现从电子邮件到移动设备和从移动设备到电子邮件的消息传送。SMS 可配置为单向 （只从电子邮件到移动设备）或双向 （从电子邮件到移动设备和从移动设备到电子邮件）。要只启用单向服务，您必须添加和配置 SMS 通道。要启用双向服务，除了必须添加和配置 SMS 通道外，还必须配置 SMS Gateway Server。

单向和双向 SMS 都使用短消息点对点 (SMPP) 协议将已生成的 SMS 消息提交到短消息服务中心 (SMSC)。特别是， SMSC 必须提供支持 TCP/IP 的 V3.4 或更高版本的 SMPP 服务器。

图 D-1 说明了单向和双向 SMS 所采用的消息的逻辑流。

图 D-1 单向和双向 SMS 逻辑流



单向 SMS

要启用单向服务，Messaging Server 应使用与远程 SMSC 进行通信的 SMPP 客户机（MTA SMS 通道）。SMS 通道将已排入队列的电子邮件消息转换成 SMS 消息（如第 775 页的 “电子邮件到 SMS 的转换过程”中所述）。这一转换过程包括处理多个部分的 MIME 消息以及字符集的转换问题。

执行此功能时，SMS 通道起到了 (SMPP) 外部短消息实体 (ESME) 的作用。

双向 SMS

双向 SMS 使邮件服务器不仅可以向远程设备发送电子邮件，还允许从远程设备接收邮件回复，以及为远程设备电子邮件组织启用邮件服务器。

启用双向 SMS 服务器不仅需要 MTA SMS 通道 （SMPP 客户机）（如前一主题中所述），还需要 SMS Gateway Server。 Sun Java System Messaging Server 将 SMS Gateway Server 作为其常规安装过程的一部分进行安装，之后您还必须对其进行配置。 SMS Gateway Server 执行两项功能：

- SMPP 中继

  SMS Gateway Server 充当 MTA SMS 通道和 SMSC 之间的透明 SMPP 客户机。不过，除此之外，如果作为中继， SMS Gateway Server 还会为已中继的消息生成一个唯一的 SMS 源地址，并保存远程 SMSC 返回的消息 ID，以便以后与 SMS 通知消息建立关联。

- SMPP 服务器

  SMS Gateway Server 充当一个 SMPP 服务器，以接收移动设备始发的 SMS 消息、回复以前的电子邮件消息和 SMS 通知。 SMS Gateway Server 使用定义转换过程的配置文件从 SMS 消息中提取目标电子邮件地址。配置文件还介绍如何处理远程 SMSC 为响应以前从电子邮件发送到移动设备的消息而返回的通知消息。

注 Sun Java System Messaging Server 不支持 Windows 平台上的双向 SMS。

要求

本手册假定您已阅读了 LogicaCMG 的 SMPP 规范和适用于您的 SMSC 的 SMPP 文档。

为了实现 SMS，必须具备以下条件：

- Sun Java System Messaging Server 6 或更高版本。（iPlanet Messaging Server 5.2 中还实现了单向 SMS。）
- 基于 TCP/IP 的 SMSC 必须支持 SMPP V3.4 或更高版本，而且在运行 Messaging Server 的主机与 SMSC 之间必须具备 TCP/IP 连通性。

有关 SMS Gateway Server 存储规划的信息，请参见第 841 页的 “SMS Gateway Server 存储要求”。

SMS 通道操作原理

SMS 通道是一个多线程通道，它将已排队的电子邮件消息转换成 SMS 消息，然后提交转换后的消息以将其传送到 SMSC。

本节包含以下通道操作主题：

- 第 774 页的 “将电子邮件定向到通道”。
- 第 775 页的 “电子邮件到 SMS 的转换过程”。
- 第 779 页的 “SMS 消息提交过程”。
- 第 782 页的 “站点定义的地址有效性检查和转换”
- 第 783 页的 “站点定义的文本转换”

将电子邮件定向到通道

按照第 788 页的 “SMS 通道配置” 配置 SMS 通道时，将有一个或多个主机名与该通道相关联。为便于讨论，我们假定主机名 sms.siroe.com 是一个与该通道相关联的主机名。在这种情况下，将用以下形式的地址将电子邮件定向到通道：

```
local-part@sms.siroe.com
```

其中 local-part 或者是 SMS 目标地址 （例如，无绳电话号码、寻呼机 ID 等），或者是以下格式的属性 - 值对列表：

```
/attribute1=value1/attribute2=value2/.../@sms.siroe.com
```

表 D-1 中介绍了识别的属性名称及其用法。这些属性允许按收件人控制某些通道选项。

表 D-1 SMS 属性

属性名称	属性值和用法
ID	将 SMS 消息定向到的 SMS 目标地址 （例如，无绳电话号码、寻呼机 ID 等）。必须提交该属性及其相关值。
FROM	SMS 源地址。选项 USE_HEADER_FROM=0 时忽略。
FROM_NPI	NPI. 使用指定的 NPI 值。选项 USE_HEADER_FROM=0 时忽略。
FROM_TON	TON. 使用指定的 TON 值。选项 USE_HEADER_FROM=0 时忽略。
MAXLEN	对于该收件人，已生成的 SMS 消息中可容纳的最大字节总数 （即，八位字节）。使用 MAXLEN 和 MAX_MESSAGE_SIZE 通道选项所指定的值中的较小值。
MAXPAGES	对于该收件人，能够将电子邮件消息分割成的 SMS 消息的最大数目。使用 MAXPAGES 和 MAX_PAGES_PER_MESSAGE 通道选项所指定的值中的较小值。

表 D-1 SMS 属性

属性名称	属性值和用法
NPI	为使用 ID 属性指定的目标 SMS 地址指定一个数字规划指标 (NPI) 值。有关此属性接受的值的说明，请参见 DEFAULT_DESTINATION_NPI 通道选项的说明。使用此属性时，属性值将覆盖 DEFAULT_DESTINATION_NPI 通道选项所给定的值。
PAGELEN	对于该收件人，一条 SMS 消息中可容纳的最大字节数。使用该值与 MAX_PAGE_SIZE 通道选项所指定值中的最小值。
TO	ID 的同义词。
TO_NPI	NPI 的同义词。
TO_TON	TON 的同义词。
TON	为使用 ID 属性给定的目标 SMS 地址指定数字类型 (TON) 值。有关此属性接受的值的说明，请参见 DEFAULT_DESTINATION_TON 通道选项的说明。使用此属性时，属性值将覆盖 DEFAULT_DESTINATION_TON 通道选项给定的值。

下面是一些地址示例：

```
123456@sms.siroe.com
/id=123456/@sms.siroe.com
/id=123456/maxlen=100/@sms.siroe.com
/id=123456/maxpages=1/@sms.siroe.com
```

有关在电子邮件地址的 SMS 目标地址部分中执行转换、有效性检查和其他操作的信息，请参见第 782 页的 “站点定义的地址有效性检查和转换”。

电子邮件到 SMS 的转换过程

为了将电子邮件发送到远程站点，必须将电子邮件转换成能被远程 SMSC 所理解的 SMS 消息。本节说明将 SMS 通道中排队的电子邮件消息转换成一个或多个 SMS 消息的过程。如下文所述，选项可以控制生成的 SMS 消息的最大数目、这些 SMS 消息的最大总长度和任意一条 SMS 消息的最大大小。只有电子邮件消息的文本部分（即， MIME 文本内容类型）会被使用，并且还可以控制已转换部分的最大数目。

电子邮件消息标题行和文本部分中所使用的字符集均将被转换为统一字符编码，然后再转换为相应的 SMS 字符集。

如果没有 SMS_TEXT 映射表 （请参见第 783 页的 “站点定义的文本转换”），已排入 SMS 通道的电子邮件消息将按图 D-2 中的说明进行处理。

图 D-2 SMS 通道的电子邮件处理

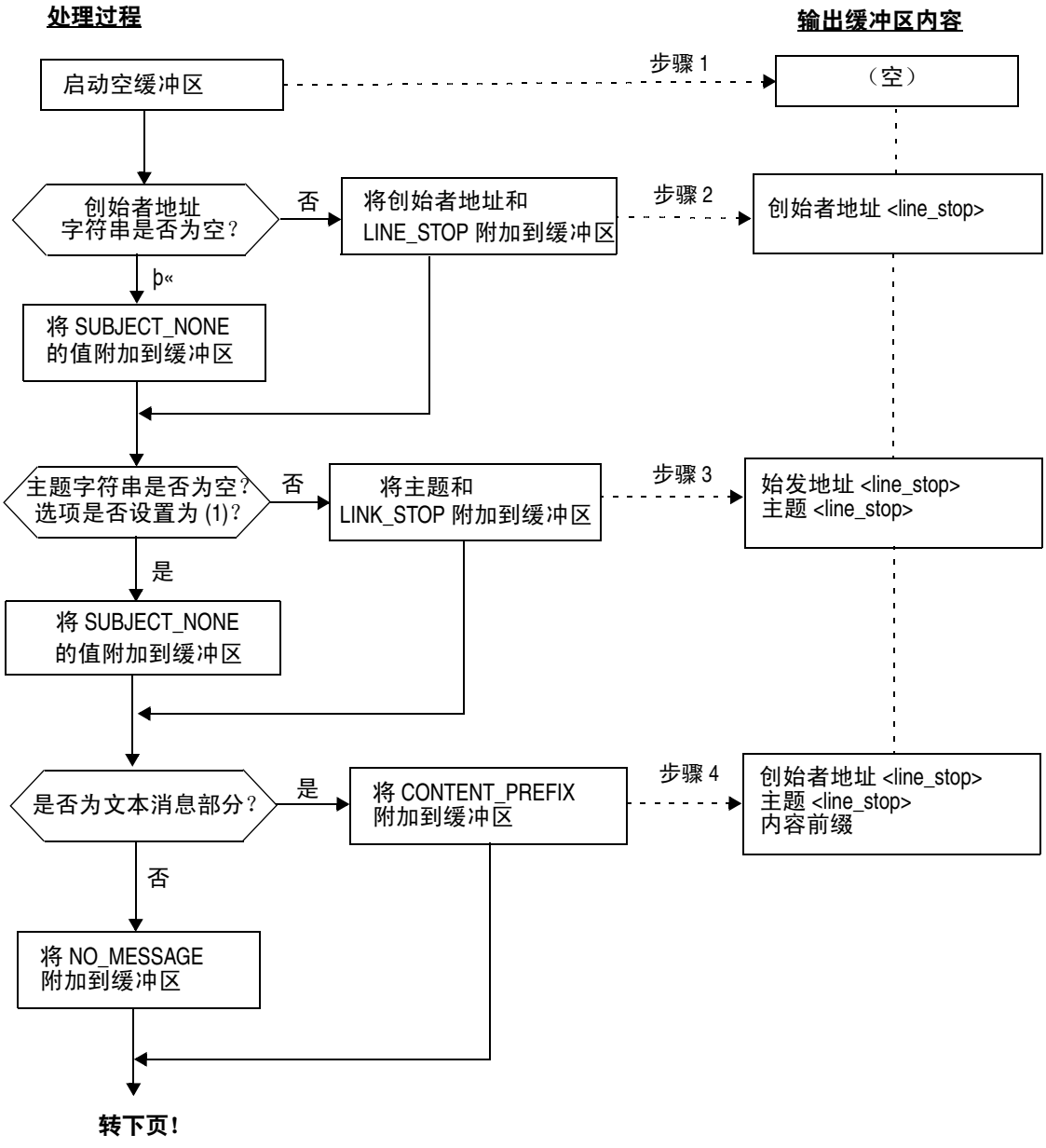
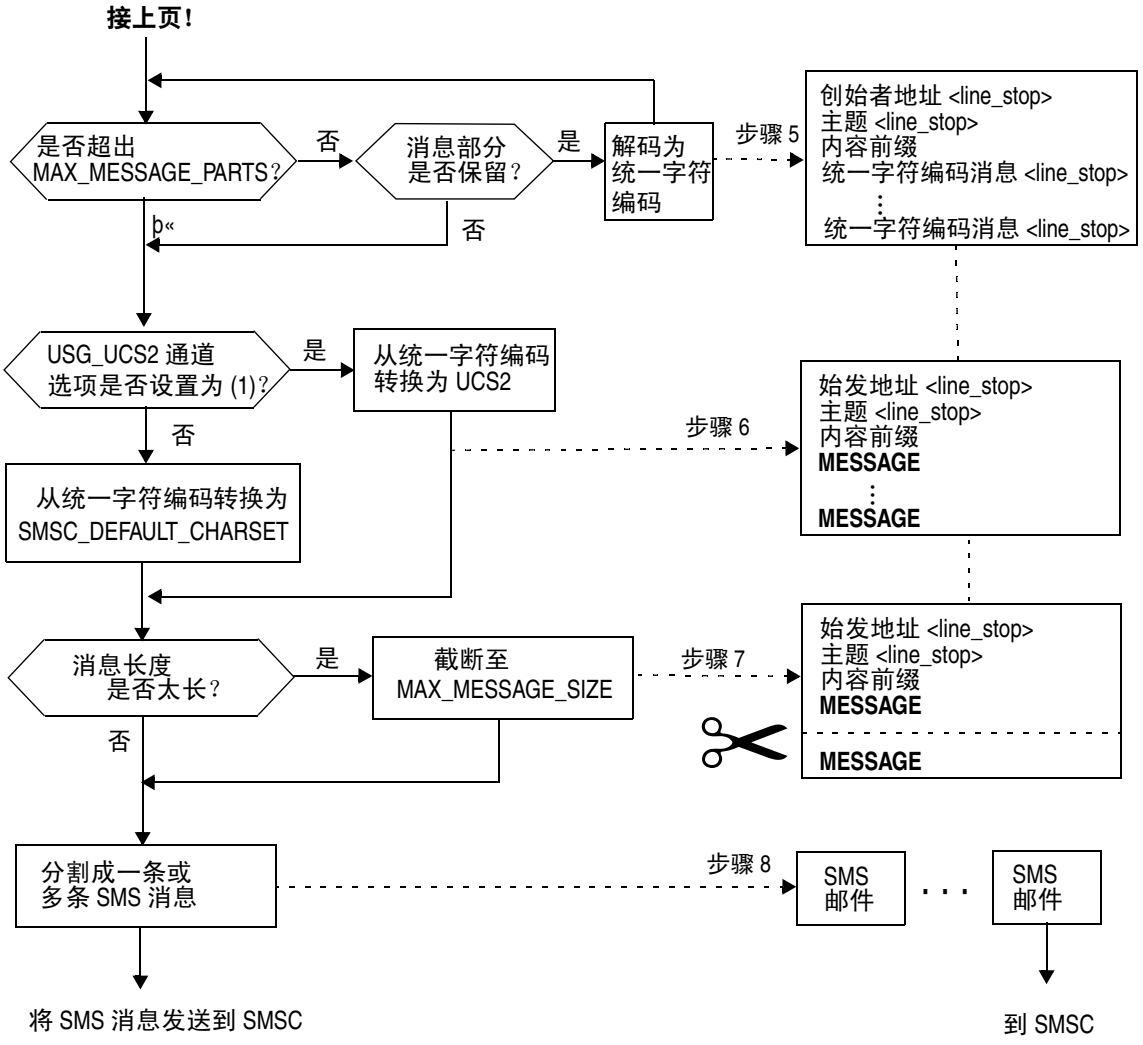


图 D-3 SMS 通道的电子邮件处理 （续）



以下步骤对应于图 D-2 中的编号框：

1. 启动一个空输出缓冲区。该缓冲区所使用的字符集是统一字符编码。
2. 电子邮件消息的创始者地址来自以下五个源 （按首选项降序显示）之一：

   1. Resent-from:
   2. From:
   3. Resent-sender:
   4. Sender:
   5. Envelope From:

   如果创始者地址是空字符串，则 FROM_NONE 通道选项的值就会附加到该缓冲区。

   但是，如果创始者地址是一个非空字符串，则 FROM_FORMAT 通道选项的处理结果和 LINE_STOP 通道选项的值就会附加到输出缓冲区。

   请注意，只有 USE_HEADER_RESENT 选项值为 1 时才能考虑 Resent-from: 和 Resent-sender: 标题行。否则，将忽略 Resent- 标题行。
3. 如果 Subject: 标题行不存在或为空，则 SUBJECT_NONE 选项的值就会附加到输出缓冲区。

   否则， SUBJECT_FORMAT 选项的处理结果和 LINE_STOP 通道选项的值就会附加到输出缓冲区。
4. 如果没有文本消息部分，则 NO_MESSAGE 通道选项的值就会附加到输出缓冲区。

   若有文本消息部分，则 CONTENT_PREFIX 通道选项的值就会附加到输出缓冲区。

   非文本消息部分则被放弃。
5. 对于每个文本部分，如果未达到 MAX_MESSAGE_PARTS 限制，文本部分就会被解码为统一字符编码并与 LINE_STOP 通道选项的值一起被附加到该缓冲区。
6. 然后，所得到的输出缓冲区将从统一字符编码转换为 SMSC 的默认字符集或 UCS2 (UTF-16)。将用 SMSC_DEFAULT_CHARSET 选项指定 SMSC 的默认字符集。
7. 转换完毕后，所得到的结果将被截断，以使之不超过 MAX_MESSAGE_SIZE 个字节。
8. 然后，步骤 6 中转换得到的字符串将被分割成一条或多条 SMS 消息，其中任何一条 SMS 消息都不长于 MAX_PAGE_SIZE 个字节。最多将生成 MAX_PAGES_PER_MESSAGE 条 SMS 消息。

注 由于一条电子邮件消息可能发送给多个收件人，因此，可能需要对使用 MAXLEN、 MAXPAGES 或 PAGELEN 属性 （如第 4 页的 “将电子邮件定向到通道” 所述）的每个收件人地址执行步骤 6 至步骤 8。

电子邮件消息处理样例

例如，使用通道的默认设置的电子邮件消息：

```
From:John Doe
To: 1234567@sms.siroe.com
Subject: Today's meeting
Date: Fri, 26 March 2001 08:17

The staff meeting is at 14:30 today in the big conference room.
```

将转换成 SMS 消息：

```
jdoe@siroe.com (Today担 meeting) The staff meeting is at 14:30 today in the big
conference room.
```

如下所示的另一组选项设置：

```
CONTENT_PREFIX=Msg:
FROM_FORMAT=From:${pa}
SUBJECT_FORMAT=Subj:$s
```

将会生成以下 SMS 消息：

```
From:John Doe Subj:Today担 meeting Msg:The staff meeting is at 14:30 today in
the big conference room.
```

SMS 消息提交过程

电子邮件消息转换成一条或多条 SMS 消息 （可能每个收件人的设置不同）后，SMS 消息将被提交到目标 SMSC。提交过程是使用基于 TCP/IP 的 SMPP V3.4 完成的。SMPP 服务器的主机名 (SMPP_SERVER) 将用作与 SMS 通道相关联的正式主机名；要使用的 TCP 端口 (SMPP_PORT) 将用 port 通道关键字指定。

当有消息需要处理时，通道就会被启动。通道将作为发送器绑定到 SMPP 服务器，递交使用第 803 页的 “SMPP 选项”中所述的 ESME_ 通道选项指定的证书。表 D-2 列出了 BIND_TRANSMITTER PDU （协议数据单元）中的字段集，并给出了它们的值：

表 D-2 生成的 BIND_TRANSMITTER PDU 中的字段

字段	值
system_id	ESME_SYSTEM_ID 通道选项；默认值为空字符串
password	ESME_PASSWORD 通道选项；默认值为空字符串
system_type	ESME_SYSTEM_TYPE 通道选项；默认值为空字符串
interface_version	0x34 表示 SMPP V3.4

表 D-2 生成的 BIND_TRANSMITTER PDU 中的字段

字段	值
addr_ton	ESME_ADDRESS_TON：默认值为表示未知 TON 的 0x00
addr_npi	ESME_ADDRESS_NPI：默认值为表示未知 NPL 的 0x00
addr_range	ESME_IP_ADDRESS 通道选项；默认值为空字符串

请注意，通道是多线程的。通道可以运行多个出队列线程，具体取决于要发送邮件的数量。（甚至可能会运行多个通道进程。）每个线程执行一次 BIND_TRANSMITTER，然后在该 TCP/IP 连接上发送所有必须发送的 SMS 消息，随后发送一个 UNBIND 命令，最后关闭连接。系统不会为了将来可能会重新使用某个连接而将其以开放状态闲置一段时间。如果远程 SMPP 服务器发送回一个限制错误，系统就会执行一次 UNBIND 操作，而 TCP/IP 连接将关闭并建立一个新的连接和 BIND。如果远程 SMPP 服务器在发送完其 SMS 消息之前发送了 UNBIND 命令，也会发生类似情况。

然后，将使用 SMPP SUBMIT_SM PDU 提交 SMS 消息。如果返回一个永久性错误（例如 ESME_RINVDSTADR），则电子邮件消息将会作为不可传送的消息而被返回。如果返回一个临时性错误，电子邮件消息就会重新入队，以尝试以后传送。要说明的是，对于永久性错误，条件可能永远不存在而重复尝试传送也不会有实际结果，例如无效的 SMS 目标地址。而对于临时性错误，条件在近期可能不存在，如服务器关闭或服务器拥塞的情况。

如果 USE_HEADER_FROM 选项的值为 1，则将为提交的 SMS 消息设置源地址。所使用的值将从始发电子邮件消息中导出，并选定为所有回复最有可能被定向到的 （电子邮件）地址。相应地，源地址从以下七种来源 （按首选项降序显示）之一中选出：

1. Resent-reply-to:
2. Resent-from:
3. Reply-to:
4. From:
5. Resent-sender:
6. Sender:
7. Envelope From:

请注意，仅在 USE_HEADER_REPLY_TO 选项的值为 1 时，才考虑 Resent-reply-to: 和 Reply-to: 标题行。而且，只有 USE_HEADER_RESENT 选项的值为 1 时才能考虑 Resent-reply-to:、 Resent-from: 和 Resent-sender: 标题行。（请注意，这就意味着只有这两个选项的值都必须为 1 时才能考虑 Resent-reply-to: 标题行。）这两个选项的默认值都为值 0。同样，默认配置仅考虑第 4、第 6 和第 7 项。最后，由于 SMS 消息中的源地址被限制为 20 个字节，所以如果选定的源地址超过该限制，该地址就会被截断。

表 D-3 列出了 SUBMIT_SM PDU 中的强制性字段集：

表 D-3 生成的 SUBMIT_SM PDU 中的强制性字段

字段	值
service_type	DEFAULT_SERVICE_TYPE 通道选项；默认值为空字符串。
source_addr_ton	DEFAULT_SOURCE_TON 通道选项；如果 USE_HEADER_FROM=1，则该字段通常被强制赋予表示字母数字 TON 的值 0x05；否则，默认值为表示国际 TON 的 0x01。
source_addr_npi	DEFAULT_SOURCE_NPI 通道选项；默认值为 0x00。
source_addr	DEFAULT_SOURCE_ADDRESS 通道选项 （如果 USE_HEADER_FROM=0）；否则为表示电子邮件消息创始者的字母数字字符串。
dest_addr_ton	TON 寻址属性或 DEFAULT_DESTINATION_TON 通道选项；默认值为表示国际 TON 的 0x01。
dest_addr_npi	NPI 寻址属性或 DEFAULT_SOURCE_NPI 通道选项；默认值为表示未知 NPI 的 0x00。
dest_addr	从电子邮件信封 To: 地址的本地部分导出的目标 SMS 地址；请参见第 774 页的“将电子邮件定向到通道”。
esm_class	对于单向 SMS，设置为 0x03，表示存储和转发模式、默认的 SMSC 消息类型，且不设置回复路径。对于双向 MSM 消息，则设置为 0x83。
protocol_id	0x00；不适用于 CDMA 和 TDMA；对 GSM 来说， 0x00 表示不使用 Internet，但使用 SME 对 SME 协议。
priority_flag	对于 GSM 和 CDMA 为 0x00，对于 TDMA 为 0x01，所有这些都表示正常优先级；请参见 DEFAULT_PRIORITY 通道选项的说明。
schedule_delivery_time	表示立即传送的空字符串。
validity_period	DEFAULT_VALIDITY_PERIOD 通道选项；默认值为表示应使用 SMSC 的默认值的空字符串。
registered_delivery	0x00，表示不使用已注册的传送。
replace_if_present_flag	0x00，表示不应替换以前的任何 SMS 消息。
data_coding	对于 SMSC 的默认字符集为 0x00；对于 UCS2 字符集则为 0x08。
sm_default_msg_id	0x00，表示不使用预定义的消息。
sm_length	SMS 消息的长度和内容；有关详细信息，请参见第 775 页的 “电子邮件到 SMS 的转换过程”。
short_message	SMS 消息的长度和内容；有关详细信息，请参见第 775 页的 “电子邮件到 SMS 的转换过程”。

表 D-4 显示了 SUBMIT_SM PDU 中的可选字段：

表 D-4 生成的 SUBMIT_SM PDU 中的可选字段

字段	值
privacy	请参见 DEFAULT_PRIVACY 通道关键字中的说明；除非电子邮件消息有 Sensitivity: 标题行，否则默认设置为不提供替换
sar_refnum	请参见 USE_SAR 通道关键字的说明；默认设置为不提供这些字段
sar_total	请参见上面的 sar_refnum。
sar_seqnum	请参见上面的 sar_refnum。

通道将一直绑定到 SMPP 服务器，直到它再没有要提交的 SMS 消息 （消息队列为空）或者已超过 MAX_PAGES_PER_BIND 时为止。在后一种情况下，如果仍有需要发送的 SMS 消息，就会建立新的连接并绑定已执行的操作。

请注意， SMS 通道是多线程的。通道中的每个处理线程均保持自身与 SMPP 服务器的 TCP 连接。例如，如果有三个处理线程有要提交的 SMS 消息，则通道与 SMPP 服务器就有三个开放的 TCP 连接。每个连接均将作为发送器绑定到 SMPP 服务器。而且，任何给定的处理线程一次只能有一个等待提交的 SMS。即，一个给定线程将提交一条 SMS 消息，然后等待，直至收到提交响应 （即 SUBMIT_SM_RESP PDU）之后，才提交另一条 SMS 消息。

站点定义的地址有效性检查和转换

站点可能希望将有效性检查和转换应用于收件人电子邮件地址 （在第 774 页的 “将电子邮件定向到通道”中进行了介绍）中记录的 SMS 目标地址中。例如，站点可能希望：

- 去除非数字字符 （例如，将 800.555.1212 转换成 8005551212）
- 添加前缀 （例如，将 8005551212 转换成 +18005551212）
- 验证正确性 （例如， 123 为太短）

前两项任务可使用 DESTINATION_ADDRESS_NUMERIC 和 DESTINATION_ADDRESS_PREFIX 通道选项来完成。一般情况下，所有这三项任务和其他任务都可使用映射表实现：使用重写规则中的映射表调用或使用 FORWARD 映射表。使用重写规则中的映射表调用具有很强的灵活性，包括能够拒绝带有站点定义的错误响应的地址。本节其余部分将只集中介绍这种方法 - 使用重写规则中的映射表调用的方法。

假设目标地址只能是数字格式，长度只能为 10 或 11 位并以字符串 “+1”为前缀，则其可使用以下重写规则实现

```
sms.siroe.com     ${X-REWRITE-SMS-ADDRESS,$U}@sms.siroe.com
sms.siroe.com     $?Invalid SMS address
```

上述第一条重写规则调出到名为 X-REWRITE-SMS-ADDRESS 的站点定义的映射表中。该映射表传递电子邮件地址的本地部分，以便进行检查。如果映射进程确定本地部分可接受，则该地址将被接收并重写到 SMS 通道中。如果映射进程不接受本地部分，将应用下一条重写规则。由于它是一条 $? 重写规则，所以该地址将被拒绝，并发送错误文本 “无效的 SMS 地址”。

X-REWRITE-SMS-ADDRESS 映射表如下所示。它以属性 - 值对列表格式或仅按原始 SMS 目标地址执行必要的本地部分验证步骤。

```
X-VALIDATE-SMS-ADDRESS

! Iteratively strip any non-numeric characters
    $_*$[$ -/:-~]%*  $0$2$R
! Accept the address if it is of the form 1nnnnnnnnnn or nnnnnnnnnn
! In accepting it, ensure that we output +1nnnnnnnnnn
   1%%%%%%%%%%      +1$0$1$2$3$4$5$6$7$8$9$Y
   %%%%%%%%%%       +1$0$1$2$3$4$5$6$7$8$9$Y
! We didn't accept it and consequently it's invalid
   *                 $N

X-REWRITE-SMS-ADDRESS

    */id=$_*/*       $C$0/id=$|X-VALIDATE-SMS-ADDRESS;$1|/$2$Y$E
    */id=$_*/*       $N
    *                $C$|X-VALIDATE-SMS-ADDRESS;$0|$Y$E
    *                $N
```

对于上述设置，请确保 DESTINATION_ADDRESS_NUMERIC 选项的值为 0 （默认值）。否则，将从 SMS 目标地址中去除 “+”。

站点定义的文本转换

站点可使用转换规则表自定义第 775 页的 “电子邮件到 SMS 的转换过程”中所述的步骤 1 至 6。这些规则通过 MTA 映射文件中的映射表指定。

映射表应被命名为 *SMS_Channel*_TEXT，其中的 *SMS_Channel* 是 SMS 通道的名称；例如，如果通道被命名为 sms，则映射表名为 SMS_TEXT，或者如果通道被命名为 sms_mway，则映射表名为 SMS_MWAY_TEXT。

该映射表中可包含两种类型的条目。然而，在解释这些条目的格式之前，请务必清楚地了解如何使用映射表，以便了解如何构造和使用这些条目。在这两种条目的说明之后给出了一个映射表示例。

此时，两种类型的条目是：

- 消息标题条目
- 消息主体条目

消息标题条目

这些条目指定了 SMS 消息中应包含哪些消息标题行，以及应如何缩写这些标题行或应如何转换这些标题行 （在不能缩写时）。只有当其中一个条目将一个标题行成功映射到一个非零长度的字符串时，该标题行才能包含到将要生成的 SMS 消息中。每个条目都具有以下格式

H|*pattern*　　*replacement-text*

如果消息标题行与该模式匹配，将会使用映射文件的模式匹配和字符串替换功能将标题行替换为替代文本 replacement-text。然后，标题行的最终映射结果将会包含在 SMS 消息中，该消息中提供了在替代文本中指定的元字符 $Y。如果某个标题行与任何模式字符串都不匹配，而且如果其映射到一个零长度的字符串或者在替代文本中未指定 $Y 元字符，则 SMS 消息中将忽略该标题行。两个条目

```
H|From:*  F:$0$Y
H|Subject:*   S:$0$Y
```

会使 `From:` 和 `Subject:` 标题行包含在 SMS 消息中，并且 `From:` 和 `Subject:` 被缩写为 `F:` 和 `S:`。条目：

```
H|Date:*  H|D:$0$R$Y
H|D:*,*%19%*:*:*  H|D:$0$ $5:$6$R$Y
```

会使 `Date:` 标题行被接受和映射，以便将标题行示例

```
Date:Wed, 16 Dec 1992 16:13:27 -0700 (PDT)
```

转换成

```
D:Wed 16:13
```

可能会生成非常复杂的重复映射。希望设置定制过滤器的站点将首先需要了解映射文件的工作原理。在必要时可将条目右侧的 H| 忽略。允许在该侧出现 H|，以便减小重复映射集所需的表条目数量。

消息主体条目

这些条目建立了适用于每行消息主体的映射。每行消息主体将在并入被生成的 SMS 消息中之前，通过这些映射进行传送。这些条目的格式为：

`B|`*pattern*　　`B|`*replacement-text*

如果某行消息主体与 *pattern* 模式匹配，就会用替代文本 *replacement-text* 替换该行消息主体。使用这种功能还会构造非常复杂的重复映射。在必要时可省略条目右侧的 B| 。

SMS 映射表示例

代码示例 D-1 中显示了一个 `SMS_TEXT` 映射表示例。每行末尾括号内的数字与该表后面标题为 " 说明文本 " 一节中的条目编号相对应。

代码示例 D-1　　SMS_TEXT 映射表示例。

```
SMS_TEXT

   H|From:*          H|F:$0$R$Y  (1.)
   H|Subject:*       H|S:$0$R$Y  (1.)
   H|F:*<*>*         H|F:$1$R$Y  ()
   H|F:*(*)*         H|F:$0$2$R$Y  (2.)
   H|F:*"*"*         H|F:$0$2$R$Y  (3.)
   H|F:*@*           H|F:$0$R$Y  (4.)
   H|%:$ *           H|$0:$1$R$Y  (5.)
   H|%:*$            H|$0:$1$R$Y  (5.)
   H|%:*$ $ *        H|$0:$1$ $2$R$Y  (6.)
   B|*--*            B|$0-$1$R  (7.)
   B|*..*            B|$0.$1$R  (7.)
   B|*!!*            B|$0!$1$R  (7.)
   B|*??*            B|$0?$1$R  (7.)
   B|*$ $ *          B|$0$ $1$R  (6.)
   B|$ *             B|$0$R  (5.)
   B|*$              B|$0$R  (5.)
```

说明文本

上面 `SMS_TEXT` 映射表示例中的条目的说明如下：

上例中，元字符 $R 用于实现和控制映射的重复应用。通过在这些映射上迭代，可获得强大的过滤功能。例如，要清除单个前导或后缀空格 (6) 或将两个空格缩减为一个空格 (7) 的简单映射在作为整体采用时会成为一个过滤器，能够去除全部前导和后缀空格并将多个连续空格缩减为一个空格。这种过滤有助于减少每条 SMS 消息的长度。

1. 这两个条目会将 From: 和 Subject: 标题行包含在一条 SMS 消息中。从：和 Subject: 可分别缩写为 F: 和 S:。某些其他条目会进一步影响 From: 和 Subject: 标题行。

   此条目将把包含 <...> 模式的 From: 标题行缩减为只包含尖括号内的文本。例如：

   ```
   F:"John C. Doe" <jdoe@siroe.com> (Hello)
   ```

   将被替换为：

   ```
   F:jdoe@siroe.com
   ```

2. 此条目将删除 From: 标题行中 (...) 模式内包含的所有内容。例如：

   ```
   F:"John C. Doe" <jdoe@siroe.com> (Hello)
   ```

   将被替换为：

   ```
   F:"John C. Doe" <jdoe@siroe.com>
   ```

3. 此条目将删除 From: 标题行中 "..." 模式内包含的所有内容。例如：

   ```
   F:"John C. Doe" <jdoe@siroe.com> (Hello)
   ```

   将被替换为：

   ```
   F:<jdoe@siroe.com> (Hello)
   ```

4. 此条目将删除 From: 标题行中 at 符号 (@) 右侧包含的所有内容。例如：

   ```
   F:"John C. Doe" <jdoe@siroe.com> (Hello)
   ```

   将被替换为：

   ```
   F:"John C. Doe" <jdoe@
   ```

5. 这四个条目将从消息标题和主体行中删除前导和后缀空格。

6. 这两个条目会将消息标题和主体行中的两个空格缩减为一个空格。

7. 这四个条目会将双字节短划线、句号、感叹号和问号转变成匹配字符的单字节形式。这样还有助于缩减 SMS 消息中的字节数。

条目的顺序是非常重要的。例如，按照给定顺序，消息 From: 标题行开始：

```
From:"John C. Doe"  (Hello)
```

将缩减为：

```
jdoe
```

实现这一目的的操作步骤如下：

1. 我们以 From: 标题行开始：

   ```
   From:"John C. Doe"  (Hello)
   ```

   第一个映射条目中的模式将与之匹配并生成以下结果：

   ```
   F:"John C. Doe"  (Hello)
   ```

   结果字符串中的 $R 元字符将使结果字符串被重新映射。

2. 此映射将应用到上一步的结果字符串中。这将生成：

   ```
   F:jdoe@siroe.com
   ```

   映射中的 $R 会把整个映射集重新应用到此步骤的结果中。

3. 接下来，将应用映射生成：

   ```
   F:jdoe
   ```

   映射中的 $R 会把整个映射集重新应用到此步骤的结果中。

4. 接下来，将应用映射生成：

   ```
   F:jdoe
   ```

   映射中的 $R 会把整个映射集重新应用到此步骤的结果中。

5. 由于其他条目都不匹配，所以最后将得到以下字符串：

   ```
   F:jdoe
   ```

   该字符串被并入到 SMS 消息中。

注 可使用 `imsimta` 测试映射实用程序测试映射表。例如，

```
# imsimta test -mapping -noimage_file -mapping_file=test.txt
Enter table name: SMS_TEXT
Input string: H|From: "John C. Doe"  (Hello)
Output string: H|F:jdoe
Output flags: [0,1,2,89]
Input string: ^D
#
```

有关 `imsimta` 实用程序的详细信息，请参见 Sun Java System Messaging Server 管理指南 (http://docs.sun.com/doc/819-1056)。

SMS 通道配置

本节介绍如何为单向 （电子邮件到移动设备）和双向 （电子邮件到移动设备和移动设备到电子邮件）功能设置 SMS 通道。除第 814 页的 “为双向 SMS 配置 SMS 通道”主题中说明的例外情况外，为单向和双向功能设置 SMS 通道的方法相同。

本节包含以下主题：

- 第 788 页的 “添加 SMS 通道”
- 第 790 页的 “创建 SMS 通道选项文件”
- 第 791 页的 “可用选项”
- 第 811 页的 “添加附加 SMS 通道”
- 第 812 页的 “调整传送重试的频率”
- 第 812 页的 “单向配置范例 (MobileWay)”
- 第 814 页的 “为双向 SMS 配置 SMS 通道”

添加 SMS 通道

向 Messaging Server 配置中添加 SMS 通道需要两个步骤：

1. 第 789 页的 “添加通道定义和重写规则”。
2. 第 790 页的 “创建 SMS 通道选项文件”。

如果没有在各种情况下均必须设置的通道选项，可能需要设置以下一个或多个选项：`ESME_PASSWORD`、`ESME_SYSTEM_ID`、`MAX_PAGE_SIZE`、`DEFAULT_SOURCE_TON` 和 `DEFAULT_DESTINATION_TON`。而且，如前文所述，SMPP 服务器的主机名或 IP 地址和 TCP 端口必须通过 imta.cnf 文件中的通道定义或通过通道选项文件进行设置。

您可配置多个 SMS 通道，并为不同 SMS 通道赋予不同的特征。有关使用多个 SMS 通道的详细信息，请参见第 811 页的 “添加附加 SMS 通道”。

请注意以下说明：如果更改了 `imta.cnf` 文件，就必须重新编译。如果仅更改了通道选项文件，则不需要重新编译。

还请注意，通道更改生效前的时间因更改内容的不同而不同。许多通道选项更改在作了更改启动的所有通道中都有效，而由于作业控制器通常会启动新通道，所以看起来几乎是即刻发生的。某些更改结果只有在重新编译并重新启动了 SMTP 服务器后才生效。这些选项是在消息排入通道后而不是在通道本身运行时得到处理的。

添加通道定义和重写规则

要添加通道定义和重写规则，请执行以下操作：

1. 将一个 SMS 通道添加到 MTA 的配置中以前，需要为通道取名。通道的名称可以是 sms 或 sms_x，其中 x 是不分大小写、长度在一至三十六个字节之间的字符串。例如， sms_mway。

2. 要添加通道定义，请编辑位于 *installation-directory*/config/ 目录中的 imta.cnf 文件。在文件末尾于此二行之后添加一个空白行：

   ```
   channel-name port p threaddepth t \
     backoff pt2m pt5m pt10m pt30m notices 1
   smpp-host-name
   ```

   其中 *channel-name* 是您为通道选择的名称， *p* 是 SMPP 服务器所侦听的 TCP 端口， *t* 是每个传送过程中 SMPP 服务器同时连接的最大数目，而 *smpp-host-name* 则是运行 SMPP 服务器的系统的主机名。

   例如，您可以将通道定义指定为如下内容：

   ```
   sms_mway port 55555 threaddepth 20 \
     backoff pt2m pt5m pt10m pt30m notices 1
   smpp.siroe.com
   ```

   有关如何计算 threaddepth 的说明，请参见第 790 页的 “控制同时连接数目”。

   有关 backoff 和 notices 通道关键字的讨论，请参见第 812 页的 “调整传送重试的频率”。

   如果希望为 *smpp-host-name* 指定 IP 地址而不是主机名，请指定域文字。例如，如果 IP 地址为 127.0.0.1，则应为 *smpp-host-name* 指定 [127.0.0.1]。或者，应考虑使用 SMPP_SERVER 通道选项。

注 对于 Sun Java System Messaging Server 6.1，反对使用 master 通道关键字。如果其存在，则应忽略。

3. 添加了通道定义后，就请跳至文件的上半部分，并按以下格式添加一条重写规则：

   ```
   smpp-host-name $u@smpp-host-name
   ```

   例如，

   ```
   smpp.siroe.com $u@smpp.siroe.com
   ```

4. 保存 imta.cnf 文件。

5. 用 imsimta cnbuild 命令重新编译配置。

6. 用 imsimta restart dispatcher 命令重新启动 SMTP 服务器。
7. 对于上述配置，通过将电子邮件消息寻址为 id@smpp-host-name （例如 123456@smpp.siroe.com）可以将其定向到通道。有关寻址的详细信息，请参见第 775 页的 “电子邮件到 SMS 的转换过程”。
8. 或者，如果希望对用户隐藏 SMPP 服务器的主机名，或者希望把其他主机名与同一通道相关联，则可添加其他重写规则。例如，要将 host-name-1 和 host-name-2 与通道相关联，请将以下内容添加到重写规则中：

   ```
   host-name-1 $U%host-name-1@smpp-host-name
   host-name-2 $U%host-name-2@smpp-host-name
   ```

   例如，如果 SMPP 服务器的主机名是 smpp.siroe.com，但是您希望用户将电子邮件寻址为 id@sms.sesta.com，则请添加重写规则：

   ```
   sms.sesta.com $U%sms.sesta.com@smpp.siroe.com
   ```

请注意， SMPP_SERVER 和 SMPP_PORT 通道选项将覆盖通道的正式主机名和 port 通道关键字设置。当使用 SMPP_PORT 选项时，没有必要也使用 port 关键字。采用这两个选项的好处在于，它们能够在不需要重新编译配置的情况下得到实现并在实现后进行更改。附加使用 SMPP_SERVER 选项的信息在第 811 页的 “添加附加 SMS 通道”中进行了介绍。

控制同时连接数目

threaddepth 通道关键字控制一个传送过程内要指定给每个传送线程的消息数目。要计算允许同时连接的总数目，请将以下两个选项的值相乘：SMPP_MAX_CONNECTIONS 和 job_limit (SMPP_MAX_CONNECTIONS * job_limit)。SMPP_MAX_CONNECTIONS 选项控制一个传送过程内传送线程的最大数目。而 job_limit 选项对在其中运行通道的作业控制器处理池而言，则控制同时传送过程的最大数目。

要限制同时连接的总数，您必须适当调节其中一个选项或这两个选项。例如，如果远程 SMPP 服务器只允许单个连接，则 SMPP_MAX_CONNECTIONS 和 job_limit 都必须设置为 1。在调节值时，最好允许 job_limit 大于 1。

创建 SMS 通道选项文件

一般情况下，通道选项文件包含通道操作所需的、站点特定的参数。 SMS 不需要通道选项文件。如果确定您的安装需要一个通道选项文件，则请将该文件以文本文件的形式保存在 *installation-directory*/config/ 目录中。与其他通道选项文件一样，该文件的文件名也应采用如下格式：

*channel_name*_option

例如，如果通道被命名为 sms_mway，则通道选项文件就应是：

installation-directory/config/sms_mway_option

每个选项都放置在使用如下格式的文件的单一行中：

option_name=*option_value*

例如，

```
PROFILE=GSM
SMSC_DEFAULT_CHARSET=iso-8859-1
USE_UCS2=1
```

有关可用 SMS 通道选项及各个选项说明的列表，请参见下文中的 " 可用选项 "。

可用选项

SMS 通道包含许多选项，这些选项分为六大类：

- **电子邮件到 *SMS* 的转换**：控制电子邮件到 SMS 的转换过程的选项。
- *SMS Gateway Server* **选项**：网关配置文件选项。
- *SMS* **字段**：控制已生成 SMS 消息中的 SMS 特定字段的选项。
- *SMPP* **协议**：与使用基于 TCP/IP 的 SMPP 协议相关联的选项。
- **本地化**：允许本地化文本字段插入到 SMS 消息中的选项。
- **其他**：调试选项。

下表中汇总了这些选项，并且以下章节进行了更全面的介绍。

表 D-5 SMS 通道选项

电子邮件到 SMS 转换选项		
选项 （页码）	**说明**	**默认值**
GATEWAY_NOTIFICATIONS	指定是否将电子邮件通知消息转换成 SMS 消息。	0
MAX_MESSAGE_PARTS	从电子邮件消息中提取的消息部分的最大数目	2
MAX_MESSAGE_SIZE	从电子邮件消息中提取的字节的最大数目	960
MAX_PAGE_SIZE	一条 SMS 消息中可容纳的字节的最大数目	160

表 D-5 SMS 通道选项 （续）

MAX_PAGES_PER_MESSAGE	电子邮件消息分割成的 SMS 消息的最大数目	6
ROUTE_TO	将 SMS 消息路由到指定的 IP 主机名。	
SMSC_DEFAULT_CHARSET	SMSC 所使用的默认字符集。	US-ASCII
USE_HEADER_FROM	设置 SMS 源地址	0
USE_HEADER_PRIORITY	控制电子邮件消息标题中优先级信息的使用	1
USE_HEADER_REPLY_TO	生成 SMS 源地址时控制 Reply-to: 标题行的使用	0
USE_HEADER_RESENT	生成创始者信息时控制 Resent-*: 标题行的使用	0
USE_HEADER_SENSITIVITY	控制电子邮件消息标题中保密性信息的使用	1
USE_UCS2	在 SMS 消息中使用 UCS2 字符集 （如果可用）	1
SMS Gateway Server 选项		
GATEWAY_PROFILE	匹配在 SMS Gateway Server 的配置文件 sms_gateway.cnf 中配置的网关配置文件名	N/A
SMS 字段选项		
DEFAULT_DESTINATION_NPI	默认 SMS 目标地址为 NPI	0x00
DEFAULT_DESTINATION_TON	默认 SMS 目标地址为 TON	0x01
DEFAULT_PRIORITY	SMS 消息的默认优先级设置	0=GSM、 CDMA 1=TDMA
DEFAULT_PRIVACY	SMS 消息的默认保密性值标志	-1
DEFAULT_SERVICE_TYPE	与提交的 SMS 消息相关联的 SMS 应用服务	N/A
DEFAULT_SOURCE_ADDRESS	默认 SMS 源地址	0
DEFAULT_SOURCE_NPI	默认的 SMS 源地址为 NPI	0x00
DEFAULT_SOURCE_TON	默认的 SMS 源地址为 TON	0x01
DEFAULT_VALIDITY_PERIOD	SMS 消息的默认有效期	N/A
DESTINATION_ADDRESS_NUMERIC	将 SMS 目标地址缩减为仅包含 0 至 9 个字符	0
DESTINATION_ADDRESS_PREFIX	目标 SMS 地址带有前缀的文本字符串	N/A
PROFILE	要使用的 SMS 配置文件	GSM
USE_SAR	使用 SMS sar_ 字段排列多条 SMS 消息	0

表 D-5 SMS 通道选项 （续）

SMPP 协议选项		
ESME_ADDRESS_NPI	绑定到 SMTP 服务器时要指定的 ESME NPI	0x00
ESME_ADDRESS_TON	绑定到 SMPP 服务器时要指定的 ESME TON	0x00
ESME_IP_ADDRESS	运行 Sun Java System Messaging Server 的主机的 IP 地址	N/A
ESME_PASSWORD	绑定到 SMPP 服务器时要递交的密码	N/A
ESME_SYSTEM_ID	绑定时要递交到 SMSC 的系统标识	N/A
ESME_SYSTEM_TYPE	绑定时要递交到 SMSC 的系统类型	N/A
MAX_PAGES_PER_BIND	与 SMPP 服务器进行单个会话期间要提交的 SMS 消息的最大数目	1024
REVERSE_ORDER	多部分 SMS 消息的传输顺序	0
SMPP_MAX_CONNECTIONS	SMPP 服务器同时连接的最大数目	20
SMPP_PORT	对于单向 SMS，指 SMPP 服务器将侦听的 TCP 端口。 对于双向 SMS，指用于 LISTEN_PORT 以进行 SMPP 中继的同一 TCP 端口。	N/A
SMPP_SERVER	对于单向 SMS，指 SMPP 服务器要连接到的主机的名称。 对于双向 SMS，设置为指 SMS Gateway Server 的主机名或 IP 地址。如果使用 SMPP 中继的 LISTEN_INTERFACE_ADDRESS 选项，则请确保使用与指定的网络接口地址相关联的主机名或 IP 地址。	N/A
TIMEOUT	用 SMPP 服务器完成读写操作超时	30
本地化选项		
CONTENT_PREFIX	引入电子邮件消息内容的文本	Msg:
DSN_DELAYED_FORMAT	用于传送延迟通知的格式化字符串	空字符串
DSN_FAILED_FORMAT	用于传送失败通知的格式化字符串	参见说明
DSN_RELAYED_FORMAT	用于中继通知的格式化字符串。	参见说明
DSN_SUCCESS_FORMAT	要成功传送通知的格式化字符串。	参见说明
FROM_FORMAT	指示电子邮件消息创始者时显示的文本	$a
FROM_NONE	没有创始者时显示的文本	N/A

表 D-5 SMS 通道选项 （续）

LANGUAGE	要从其选择文本字段的语言组 (i-default)	i-default
LINE_STOP	从电子邮件消息中提取的、放置在各行末尾的文本	空格字符
NO_MESSAGE	表示消息无内容的文本	]no message]
SUBJECT_FORMAT	指示电子邮件消息的主题时显示的文本	$s
SUBJECT_NONE	电子邮件消息无主题时显示的文本	N/A
其他选项		
DEBUG	启用详细调试输出	-1

电子邮件到 SMS 转换选项

以下选项控制电子邮件消息到 SMS 消息的转换。选项值的范围列在括号中。一般情况下，给定电子邮件消息可转换成一条或多条 SMS 消息。有关此转换过程的说明，请参见第 775 页的 “电子邮件到 SMS 的转换过程”。

GATEWAY_NOTIFICATIONS

（*0* 或 *1*）指定是否将电子邮件通知转换成 SMS 通知。电子邮件通知消息必须符合 RFC 1892、 1893 和 1894。默认值为 0。

当 GATEWAY_NOTIFICATIONS=0 时，这些通知将被放弃，不会转换成 SMS 通知。

要将这些通知转换成 SMS 通知，则应设置 GATEWAY_NOTIFICATIONS=1。当此选项设置为 1 时，这些本地化选项 (DSN_*_FORMAT) 控制将哪些通知类型 （成功、失败、延迟、已中继）转换成 SMS 消息并通过网关进行发送。（如果通知类型的值是一个空字符串，则该类型通知将不转换成 SMS 消息。）

MAX_MESSAGE_PARTS

（**整数**）将多个部分的电子邮件消息转换成 SMS 消息时，将只转换前 MAX_MESSAGE_PARTS 个文本部分。其余部分将被放弃。默认情况下，MAX_MESSAGE_PARTS 为 2。要使消息部分数量无限，应将值指定为 -1。当值指定为 0 时，则不会将任何消息内容置于 SMS 消息中。这就只会使用电子邮件消息的标题行（例如 Subject:）以生成 SMS 消息。

请注意，包含文本和附件的电子邮件消息一般由两部分组成。还请注意，只有纯文本消息部分才可转换。所有其他 MIME 内容类型都将被放弃。

MAX_MESSAGE_SIZE

（**整数**， >= *10*）使用此选项可以设置电子邮件消息所生成的 SMS 消息中容纳的总字节数上限。特别是，将用于一条或多条生成的 SMS 消息的最大 MAX_MESSAGE_SIZE 字节数。任何超出此限值的字节将被放弃。

默认情况下，上限强制为 960 个字节。这一限制对应于 MAX_MESSAGE_SIZE=960。要使字节数不受限制，应将值指定为零。

将电子邮件消息从统一字符编码转换为 SMSC 的默认字符集或 UCS2 之后，才确定所使用的字节数。这意味着，在转换为 UCS2 的情况下， 960 个字节的 MAX_MESSAGE_SIZE 将让步，因为每个 UCS2 字符至少两个字节长，所以最多为 480 个字符。

请注意， MAX_MESSAGE_SIZE 和 MAX_PAGES_PER_MESSAGE 选项都服务于同一目的：限制所得的 SMS 消息的总大小。事实上， MAX_PAGE_SIZE=960 和 MAX_PAGE_SIZE=160 隐含了 MAX_PAGES_PER_MESSAGE=6。那么为什么存在两种不同的选项呢？这样就可以控制页面的总大小或总页数，而无需考虑一条 SMS 消息的最大大小 MAX_PAGE_SIZE。这一点在通道选项文件中可能并不重要，但在使用第 774 页的 “将电子邮件定向到通道”中所述的 MAXPAGES 或 MAXLEN 寻址属性时则很重要。

最后请注意，应使用 MAX_MESSAGE_SIZE 和 MAX_PAGE_SIZE * MAX_PAGES_PER_MESSAGE 两个限值中较小的值。

MAX_PAGE_SIZE

（**整数**， >= *10*）一条 SMS 消息中允许的最大字节数用 MAX_PAGE_SIZE 选项控制。默认情况下，使用的字节数值为 160。此字节数对应于 MAX_PAGE_SIZE=160。

MAX_PAGES_PER_MESSAGE

（**整数**， *1* **至** *255*）要用此选项控制为给定电子邮件消息生成的 SMS 消息的最大数目。事实上，此选项将截断电子邮件消息，从而只把适合 MAX_PAGES_PER_MESSAGE SMS 消息的那部分电子邮件消息转换成 SMS 消息。有关进一步的讨论，请参见 MAX_PAGE_SIZE 选项的说明。

默认情况下，将 MAX_PAGES_PER_MESSAGE 设置为 1 或 MAX_MESSAGE_SIZE 除以 MAX_PAGE_SIZE 所得商中的较大值。

ROUTE_TO

（**字符串**、 *IP* **主机名**、 *1* **至** *64* **个字节**）使用如下格式的电子邮件地址将定向到配置文件的所有 SMS 消息重新路由到指定的 IP 主机名：

```
SMS-destination-address@route-to
```

其中 SMS-destination-address 是 SMS 消息的目标地址，而 route-to 则是用此选项指定的 IP 主机名。这条 SMS 消息的全部内容将作为所得的电子邮件消息的内容进行发送。 PARSE_RE_* 选项将被忽略。

注 PARSE_RE_* 和 ROUTE_TO 选项应相互独立使用。在同一网关配置文件中同时使用这两个选项将导致配置错误。

SMSC_DEFAULT_CHARSET

（**字符串**）使用此选项，就可以指定 SMSC 的默认字符集。请使用以下文件中给定的字符集名称

installation-directory/config/charsets.txt

如果未指定此选项，就假设使用 US-ASCII。请注意， charsets.txt 中使用的助记名称是在同一目录中的 charnames.txt 中定义的。

处理电子邮件消息时，首先对标题行和文本消息部分进行解码，然后将其转换为统一字符编码。接下来，数据将会转换为 SMSC 的默认字符集或 UCS2，这取决于 USE_UCS2 选项的值以及 SMS 消息是否至少包含一个默认 SMSCC 字符集中所没有的符号。请注意， UCS2 字符集是 16 位统一字符编码，通常称作 UTF-16。

USE_HEADER_FROM

（**整数， *0* 至 *2***）设置此选项，以允许将 From: 地址传递到 SMSC。该值指示 From: 地址的来源及其具备的格式。表 D-6 显示了允许的值及其含义。

表 D-6 USE_HEADER_FROM 值

值	说明
0	SMS 源地址绝不可依据 From: 地址。使用已找到的属性 - 值对
1	SMS 源地址设置为 from-local@from-domain，其中 From: 地址为：@from-route:from-local@from-domain
2	SMS 源地址设置为 from-local，其中 From: 地址为：@from-route:from-local@from-domain

USE_HEADER_PRIORITY

（*0* 或 *1*）此选项控制 RFC 822 Priority: 标题行的处理标题行。默认情况下，Priority: 标题行中的信息用于设置所得到的 SMS 消息的优先级标志，以覆盖用 DEFAULT_PRIORITY 选项指定的默认 SMS 优先级。这种情况对应于 USE_HEADER_PRIORITY=1。要禁用 RFC 822 Priority: 标题行，请指定 USE_HEADER_PRIORITY=0。

有关处理 SMS 优先级标志的详细信息，请参见 DEFAULT_PRIORITY 选项的说明。

USE_HEADER_REPLY_TO

（*0* 或 *1*）当 USE_HEADER_FROM =1 时，此选项控制是否考虑将 Reply-to: 或 Resent-reply-to: 标题行用作 SMS 源地址。默认情况下， Reply-to: 和 Resent-reply-to: 标题行标题行被忽略。这对应于选项值 0。要想启用这些标题行，请使用选项值 1。

请注意， RFC 2822 反对使用 Reply-to: 和 Resent-reply-to: 标题行标题行。

USE_HEADER_RESENT

（*0* 或 *1*）当 USE_HEADER_FROM =1 时，此选项控制是否将 Resent- 标题行用作 SMS 源地址。默认情况下， Resent- 标题行被忽略。这对应于选项值 0。要想启用这些标题行，请使用选项值 1。

请注意， RFC 2822 反对使用 Resent- 标题行。

USE_HEADER_SENSITIVITY

（*0* 或 *1*）USE_HEADER_SENSITIVITY 选项控制 RFC 822 Sensitivity: 标题行的处理。默认情况下， Sensitivity: 标题行中的信息用于设置所得到的 SMS 消息的保密性标志，以覆盖用 DEFAULT_PRIVACY 选项指定的默认 SMS 保密性。这种情况 （默认情况）对应于 USE_HEADER_SENSITIVITY=1。要启用 RFC 822 Sensitivity: 标题行，请指定 USE_HEADER_SENSITIVITY=0。

有关处理 SMS 保密性标志的详细信息，请参见 DEFAULT_PRIVACY 选项的说明。

USE_UCS2

（*0* 或 *1*）适当时，通道将在该选项所生成的 SMS 消息中使用 UCS2 字符集。这是一个默认性能，对应于 USE_UCS2=1。要禁用 UCS2 字符集，请指定 USE_UCS2=0。有关字符集问题的详细信息，请参见 SMSC_DEFAULT_CHARSET 选项的说明。

表 D-7 USE_UCS2 有效值

USE_UCS2 值	结果
1 （默认值）	将尽可能使用 SMSC 默认字符集。如果始发电子邮件消息中包含 SMSC 默认字符集所没有的符号，就会使用 UCS2 字符集。
0	将始终使用 SMSC 默认字符集。该字符集中所没有的符号将由助记符号表示（例如用 “AE” 表示 AE 连字符）。

SMS Gateway Server 选项

GATEWAY_PROFILE

SMS Gateway Server 配置文件 `sms_gateway.cnf` 中网关配置文件的名称。

SMS 选项

以下选项允许在生成的 SMS 消息中指定 SMS 字段。

DEFAULT_DESTINATION_NPI

（**整数**， *0* **至** *255*）默认情况下，将指定目标地址的 NPI （数字规划指标）值为零。使用此选项，可指定一个范围在 0 至 255 之间的替代整数值。典型 NPI 值包含下文的表 D-8 中所找到的值：

表 D-8 数字规划指标值

值	说明
0	未知
1	ISDN 类 （E.163、 E.164）
3	数据 (X.121)
4	电传 (F.69)
6	陆地移动设备 (E.212)
8	全国
9	Private
10	ERMES
14	IP 地址 (Internet)
18	WAP 客户机 ID
>= 19	未定义

可以将此选项的值指定为以下三种形式之一：

- 十进制值 （例如 10）。
- 带前缀 “0x” 的十六进制值 （例如 0x0a）。
- 以下任何一种不区分大小写的文本字符串 （相关联的十进制值显示在括号中）：数据 (3)、默认值 (0)、 e.163 (1)、 e.164 (1)、 e.212 (6)、 ermes (10)、 f.69 (4)、Internet (14)、 IP (14)、 ISDN (1)、陆地移动设备 (6)、全国 (8)、专用 (9)、电传 (4)、未知 (0)、 wap (18)、 x.121 (3)。

DEFAULT_DESTINATION_TON

（**整数**， *0* **至** *255*）默认情况下，将指定目标地址的 TON （数字类型）指标值为零。使用此选项，可指定一个范围在 0 至 255 之间的替代整数值。典型 TON 值包含下文的表 D-9 中所找到的值：

表 D-9 典型 TON 值

值	说明
0	未知
1	国际
2	全国
3	网络特定
4	用户号码
5	字母数字
6	缩写
>=7	未定义

可以将此选项的值指定为以下三种形式之一：

- 十进制值 （例如 10）
- 带前缀 "0x" 的十六进制值 （例如 0x0a）
- 以下任何一种不区分大小写的文本字符串 （相关联的十进制值显示在括号中）：缩写 (6)、字母数字 (5)、默认值 (0)、国际 (1)、全国 (2)、网络特定 (3)、用户 (4)、未知 (0)。

DEFAULT_PRIORITY

（**整数**， *0* **至** *255*） SMS 消息有一个强制性优先级字段。 SMS 优先级值的解释显示在下文的表 D-10 中：

表 D-10 针对每个 SMS 配置文件类型解释的 SMS 优先级值

值	GSM	TDMA	CDMA
0	非优先级	大量	正常
1	优先级	正常	交互
2	优先级	Urgent	Urgent
3	优先级	特急	紧急

使用此选项，可以指定赋予 SMS 消息的默认优先级。如果没有指定优先级，PROFILE=GSM 和 CDMA 使用默认优先级 0， PROFILE=TDMA 使用优先级 1。

请注意，如果 USE_HEADER_PRIORITY=1 且电子邮件消息具有 RFC 822 Priority: 标题行，则改用该标题行中指定的优先级设置所得到的 SMS 消息的优先级。特别是，如果 USE_HEADER_PRIORITY=0，则会始终根据 DEFAULT_PRIORITY 选项设置 SMS 优先级标志，并且始终忽略 RFC 822 Priority: 标题行。如果 USE_HEADER_PRIORITY=1，则会使用始发电子邮件消息的 RFC 822 Priority: 标题行设置 SMS 消息的优先级标志。如果该标题行不存在，则会使用 DEFAULT_PRIORITY 选项设置 SMS 优先级标志。

用于将 RFC 822 Priority: 标题行值转换成 SMS 优先级标志的映射显示在下文的表格中：

表 D-11 将 Priority: 标题转换成 SMS 优先级标志的映射

RFC 822	SMS 优先级标志		
优先级：value	**GSM**	**TDMA**	**CDMA**
第三级	非优先级 (0)	大量 (0)	正常 (0)
第二级	非优先级 (0)	大量 (0)	正常 (0)
非急	非优先级 (0)	大量 (0)	正常 (0)
正常	非优先级 (0)	正常 (1)	正常 (0)
Urgent	优先级 (1)	急 (2)	急 (2)

DEFAULT_PRIVACY

（整数， *-1*、 *0* 至 *255*）是否要在 SMS 消息中设置保密性标志，并且使用 DEFAULT_PRIVACY 和 USE_HEADER_SENSITIVITY 选项控制要使用哪一个值。默认情况下，DEFAULT_PRIVACY 使用值 -1。下文的表 D-12 显示了将 DEFAULT_PRIVACY 和 USE_HEADER_SENSITIVITY 选项设置为各种值的结果。

表 D-12 DEFAULT_PRIVACY 和 USE_HEADER_SENSITIVITY 的值的结果

DEFAULT_PRIVACY	USE_HEADER_SENSITIVITY	结果
-1	0	SMS 消息中从不设置 SMS 保密性标志。
n >= 0	0	SMS 保密性标志的值始终设置为 n。将始终忽略 RFC 822 Sensitivity: 标题行。
-1 （默认值）	1 （默认值）	SMS 消息的保密性标志仅在始发电子邮件消息具有 RFC 822 Sensitivity: 标题行时才设置。在这种情况下，将 SMS 保密性标志设置为对应于 Sensitivity: 标题行的值。该值为默认值。

表 D-12 DEFAULT_PRIVACY 和 USE_HEADER_SENSITIVITY 的值的结果

DEFAULT_PRIVACY	USE_HEADER_SENSITIVITY	结果
n >= 0	1	将 SMS 消息的保密性标志设置为对应于始发电子邮件消息的 RFC 822 Sensitivity: 标题行。如果电子邮件消息不具有 Sensitivity: 标题行，则将 SMS 保密性标志的值设置为 n。

SMS 保密性值的解释显示在下文的表 D-13 中：

表 D-13 SMS 保密性值解释

值	说明
0	无限制
1	有限制
2	机密
3	秘密
>= 4	未定义

用于将 RFC 822 Sensitivity: 标题行值转换成 SMS 优先级值的映射显示在下文的表 D-14 中：

表 D-14 将 Sensitivity: 标题转换成 SMS 保密性值的映射

RFC 822 Sensitivity:value	SMS 保密性值
Personal	1 （有限制）
Private	2 （机密）
公司机密	3 （秘密）

DEFAULT_SERVICE_TYPE

（**字符串，** *0* **至** *5* **个字节**）要与通道所生成的 SMS 消息相关联的服务类型。默认情况下，不指定服务类型 （即，零长度字符串）。某些通用的服务类型包括：CMT （蜂窝式消息传送）、CPT （蜂窝式呼叫）、VMN （语音邮件通知）、VMA （语音邮件报警）、WAP （无线应用协议）和 USSD （无特定结构的辅助数据服务）。

DEFAULT_SOURCE_ADDRESS

（**字符串**，*0* **至** *20* **个字节**）用作由电子邮件消息生成的 SMS 消息的源地址。请注意，当 USE_HEADER_FROM=1 时，用此选项指定的值将被电子邮件消息的创始者地址所覆盖。默认情况下，该值被启用，即值为 0。

DEFAULT_SOURCE_NPI

（**整数**，*0* **至** *255*）默认情况下，将指定源地址的 NPI 值为零。使用此选项，可指定一个范围在 0 至 255 之间的替代整数值。有关 NPI 典型值表，请参见 DEFAULT_DESTINATION_NPI 选项的说明。

DEFAULT_SOURCE_TON

（**整数**，*0* **至** *255*）默认情况下，将指定源地址的 TON 指标值为零。使用此选项，可指定一个范围在 0 至 255 之间的替代整数值。有关典型 TON 值表，请参见 DEFAULT_DESTINATION_TON 选项的说明。

DEFAULT_VALIDITY_PERIOD

（**字符串**，*0* **至** *252* **个字节**）默认情况下， SMS 消息不给定相对有效期，而是使用 SMSC 的默认值。使用此选项可以指定不同的相对有效期。可以以单位秒、分钟、小时或天指定值。下文的表 D-15 指定了此选项各种值的格式和说明：

表 D-15 DEFAULT_VALIDITY_PERIOD 格式和值

格式	说明
nnn	隐含单位为秒 （例如 604800）
*nnn*s	单位为秒 （例如 604800s）
*nnn*m	单位为分钟 （例如 10080m）
*nnn*h	单位为小时 （例如 168h）
*nnn*d	单位为天 （例如 7d）

可以使用指定的 0、0s、0m、0h 或 0d 来选择 SMSC 的默认有效期。即，如果使用指定的 0、0s、0m、0h 或 0d，就会为已生成的 SMS 消息的有效期指定一个空字符串。

请注意，此选项不接受 UTC 格式的值。

DESTINATION_ADDRESS_NUMERIC

（*0* **或** *1*）使用此选项可从电子邮件信封 To: 地址所提取的 SMS 目标地址中去除所有非数字字符。例如，如果信封 To: 地址为：

```
"(800) 555-1212"@sms.siroe.com
```

则该地址将被减少为：

```
8005551212@sms.siroe.com
```

要启用此去除操作，请为此选项指定值 1。默认情况下，此去除操作被禁用，这对应于选项值 0。请注意，如果启用去除操作，将会在通过 DESTINATION_ADDRESS_PREFIX 选项添加任何目标地址前缀之前完成去除操作。

DESTINATION_ADDRESS_PREFIX

（**字符串**）在某些实例中，可能需要确保在所有 SMS 目标地址前都加一个固定的文本字符串前缀 （例如 "+"）。可以使用此选项指定这样一个前缀。然后，此前缀将被添加到任何没有指定前缀的 SMS 目标地址中。要避免被 DESTINATION_ADDRESS_NUMERIC 选项去除，请在 DESTINATION_ADDRESS_NUMERIC 选项之后使用此选项。

PROFILE

（**字符串**）指定要与 SMSC 配合使用的 SMS 配置。可能的值包括 GSM、 TDMA 和 CDMA。如果没有指定，则假设为 GSM。此选项仅用于为诸如 DEFAULT_PRIORITY 和 DEFAULT_PRIVACY 之类的其他通道选项选择默认值。

USE_SAR

（*0* **或** *1*）可能需要将足够大的电子邮件消息分割成多条 SMS 消息。如果发生这种情况，就可以使用 SMS sar_ 字段有选择地为一条 SMS 消息添加排序信息。这样将生成 “片段” SMS 消息，此消息可由接收终端重新组合成一条 SMS 消息。指定 USE_SAR=1，以表示可在适当时添加此排序信息。默认设置是不添加排序信息，并且对应于 USE_SAR=0。

当指定了 USE_SAR=1 时， REVERSE_ORDER 选项将被忽略。

SMPP 选项

以下选项可用于指定 SMPP 协议参数。当 MTA 用作外部短消息实体 (ESME) （即，把 MTA 绑定到 SMPP 服务器上，以便向服务器的相关 SMSC 提交 SMS 消息）时，使用以字符串 "ESME_" 开头的名称的选项用于标识 MTA。

ESME_ADDRESS_NPI

（**整数，** *0* **至** *255*）默认情况下，绑定操作将指定 ESME NPI 的值为零，该值表示未知 NPI。使用此选项，可指定一个范围在 0 至 255 之间的替代整数值。有关 NPI 典型值表，请参见 DEFAULT_DESTINATION_NPI 选项的说明。

ESME_ADDRESS_TON

（**整数**，*0* **至** *255*）默认情况下，绑定操作将指定 ESME TON 值为 0。使用此选项，可指定一个范围在 0 至 255 之间的替代整数值。有关典型 TON 值表，请参见 DEFAULT_DESTINATION_TON 选项的说明。

ESME_IP_ADDRESS

（**字符串**，*0* **至** *15* **个字节**）当绑定到 SMPP 服务器时，BIND PDU 表示客户的 （即 ESME 的）地址范围是一个 IP 地址。这一操作将通过将 TON 指定为 0x00 并将 NPI 指定为 0x0d 来完成。然后，地址范围字段的值将被设置为运行 SMS 通道的主机的 IP 地址。指定 IP 地址为点分十进制格式 （例如 127.0.0.1）。

ESME_PASSWORD

（**字符串**，*0* **至** *8* **个字节**）当绑定到 SMPP 服务器时，可能需要密码。如果需要密码，请使用此选项指定密码。默认情况下，存在长度为零的密码字符串。

ESME_SYSTEM_ID

（**字符串**，*0* **至** *15* **个字节**）绑定到 SMPP 服务器时，可能需要为 MTA 提供系统 ID。默认情况下，不指定系统 ID （即，使用零长度的字符串）。要指定系统 ID，请使用此选项。

ESME_SYSTEM_TYPE

（**字符串**，*0* **至** *12* **个字节**）当绑定到 SMPP 服务器时，可能需要为 MTA 提供系统类型。默认情况下，不指定系统类型 （即，使用零长度的字符串）。

MAX_PAGES_PER_BIND

（**整数**，>= *0*）某些 SMPP 服务器可能限制单个绑定会话期间提交的 SMS 消息的最大数目。认识到这一点后，就可使用此选项指定单个会话期间可提交的 SMS 消息的最大数目。达到此限制后，通道将解开，并关闭 TCP/IP 连接，然后再重新连接并重新绑定。

默认情况下，MAX_PAGES_PER_BIND 使用的值为 1024。请注意，通道还将检测 ESME_RTHROTTLED 错误并在单个通道运行期间相应地调整 MAX_PAGES_PER_BIND。

REVERSE_ORDER

（*0* **或** *1*）当一条电子邮件消息生成多条 SMS 消息时，所生成的那些 SMS 消息就可按顺序 (REVERSE_ORDER=0) 或倒序 (REVERSE_ORDER=1) 提交到 SMSC。倒序可用于接收终端首先显示最后接收到的消息的情况。在这种情况下，最后接收到的消息将成为电子邮件消息的第一部分而不是最后一部分。默认情况下，将使用 REVERSE_ORDER=1。

请注意，当指定 USE_SAR=1 时，此选项将被忽略。

SMPP_MAX_CONNECTIONS

（**整数**，*1* **至** *50*）该选项控制每个过程同时连接 SMPP 的最大数目。由于每个连接都有一个相关联的线程，所以此选项还可用于限制每个过程的 “辅助”线程的最大数目。默认情况下， SMPP_MAX_CONNECTIONS=20。

SMPP_PORT

（**整数**，*1* **至** *65535*） SMPP 服务器将侦听的 TCP 端口可使用此选项或 port 通道关键字来指定。此端口号必须通过这两种机制之一进行指定。如果同时用这两种机制指定了此端口号，则优先采用 SMPP_PORT 选项所作的设置。请注意，此选项没有默认值。

对于双向 SMS，请确保该端口与用于 SMPP 中继的 LISTEN_PORT 端口相同。

SMPP_SERVER

（**字符串**，*1* **至** *252* **个字节**）默认情况下，对于单向 SMS，要连接到 SMPP 服务器的 IP 主机名为与通道相关联的正式主机名 （即， MTA 配置中通道定义的第二行中所显示的主机名）。此选项可用于指定不同的主机名或 IP 地址，该主机名或 IP 地址将覆盖通道定义中所指定的主机名或 IP 地址。在指定 IP 地址时，请使用点分十进制表示法 （例如 127.0.0.1）。

对于双向 SMS，请设置为指向 SMS Gateway Server 的主机名或 IP 地址。如果使用 SMPP 中继的 LISTEN_INTERFACE_ADDRESS 选项，则请确保使用与指定的网络接口地址相关联的主机名或 IP 地址。

TIMEOUT

（**整数**， >= 2）默认情况下，当等待数据完成到 SMPP 服务器的写入或等待从 SMPP 服务器接收数据操作时，使用的超时时间为 30 秒。使用 TIMEOUT 选项可指定一个不同的超时值 （以秒为单位）。指定值应至少为 1 秒。

本地化选项

在构造 SMS 消息时， SMS 通道有许多其放置到这些消息中的固定文本字符串。例如，引入电子邮件的 From: 地址和 Subject: 标题行的这些字符串。使用本节所述的通道选项，可为不同的语言指定这些字符串的版本，然后为该通道指定默认语言。代码示例 D-2 显示了选项文件的语言部分：

代码示例 D-2 通道选项文件的语言说明部分

```
LANGUAGE=default-language

[language=i-default]
FROM_PREFIX=From:
SUBJECT_PREFIX=Subj:
CONTENT_PREFIX=Msg:
LINE_STOP=
NO_MESSAGE=[no message]
REPLY_PREFIX=Re:

[language=en]
FROM_PREFIX=From:
SUBJECT_PREFIX=Subj:
CONTENT_PREFIX=Msg:
LINE_STOP=
NO_MESSAGE=[no message]
REPLY_PREFIX=Re:
 ...
```

在每一个 [language=x] 块中，可指定与该语言相关的本地化选项。如果块中未指定特定选项，则请使用该选项的全局值。在 [language=x] 块之外所指定的本地化选项设置该选项的全局值。

对于下文列出的选项，必须使用 US-ASCII 或 UTF-8 字符集指定字符串值。请注意， US-ASCII 字符集是 UTF-8 字符集的特例。

CONTENT_PREFIX

（**字符串**， *0* **至** *252* **个字节**）放置于 SMS 消息中、位于电子邮件消息内容之前的文本字符串。默认全局值为 US-ASCII 字符串 “Msg:”。

DSN_DELAYED_FORMAT

（**字符串**， *0* **至** *256* **个字符**）用于传送延迟通知的格式化字符串。默认情况下，此选项使用一个空字符串，从而禁止将延迟通知转换成 SMS。请注意，必须将 GATEWAY_NOTIFICATIONS 设置为 1 才能使此选项有效。 GATEWAY_NOTIFICATIONS=0 时，将忽略此选项。

DSN_FAILED_FORMAT

（**字符串**，*0* **至** *256* **个字符**）用于永久性传送失败通知的格式化字符串。此选项的默认值为字符串：

```
Unable to deliver your message to $a; no further delivery attempts will be made.
```

要禁止失败通知的转换，请为此选项指定一个空字符串。请注意，必须将 GATEWAY_NOTIFICATIONS 设置为 1 才能使此选项有效。GATEWAY_NOTIFICATIONS=0 时，将忽略此选项。

DSN_RELAYED_FORMAT

（**字符串**，*0* **至** *256* **个字符**）用于中继通知的格式化字符串。默认值为字符串：

```
Your message to $a has been relayed to a messaging system which may not provide a final delivery confirmation
```

要禁止中继通知的转换，请为此选项指定一个空字符串。请注意，必须将 GATEWAY_NOTIFICATIONS 设置为 1 才能使此选项有效。GATEWAY_NOTIFICATIONS=0 时，将忽略此选项。

DSN_SUCCESS_FORMAT

（**字符串**，*0* **至** *256* **个字符**）用于成功传送通知的格式化字符串。默认值为字符串：

```
Your message to $a has been delivered
```

要禁止成功的传送通知的转换，请为此选项指定一个空字符串。请注意，必须将 GATEWAY_NOTIFICATIONS 设置为 1 才能使此选项有效。GATEWAY_NOTIFICATIONS=0 时，将忽略此选项。

FROM_FORMAT

（**字符串**，*0* **至** *252* **个字节**）将创始者信息格式化以插入到 SMS 消息中的格式化模板。默认全局值是 US-ASCII 字符串 "$a"，该字符串替换创始者的电子邮件地址。有关详细信息，请参见第 809 页的 “格式化模板”。

FROM_NONE

（**字符串**，*0* **至** *252* **个字节**）不显示创始者地址时放置在 SMS 消息中的文本字符串。默认全局值是一个空字符串。

请注意，由于站点一般都会拒绝没有任何创始者地址的电子邮件消息，所以通常将永远不会使用此选项。

LANGUAGE

（**字符串，** *0* **至** *40* **个字节**）从其中选择文本字符串的默认语言组。如果未指定，则会从主机的默认语言环境规范中导出语言。如果主机的语言环境规范不可用或对应于 “C”，则会使用 i-default。（i-default 对应于 “国际读者通用英文文本”。）

LINE_STOP

（**字符串，** *0* **至** *252* **个字节**）要放置在从电子邮件消息中提取的 SMS 消息行之间的文本字符串。默认全局值是 US-ASCII 空格字符 “ ”。

NO_MESSAGE

（**字符串，** *0* **至** *252* **个字节**）要放置在 SMS 消息中以表示电子邮件消息无内容的文本字符串。默认全局值是 US-ASCII 字符串 “[no message]”。

SUBJECT_FORMAT

（**字符串，** *0* **至** *252* **个字节**）要对显示在 SMS 消息中的 Subject: 标题行内容进行格式化的格式化模板。此选项的默认全局值是 US-ASCII 字符串 “($s)”。有关详细信息，请参见第 809 页的 “格式化模板”。

有关在不具有 Subject: 标题行或该标题行的内容为空字符串时的处理说明，请参见 SUBJECT_NONE 选项。

SUBJECT_NONE

（**字符串，** *0* **至** *252* **个字节**）原始电子邮件消息没有 Subject: 标题行或 Subject: 标题行的值为空字符串时所显示的文本字符串。此选项的默认全局值是空字符串。

DEBUG

（**整数，位掩码**）启用调试输出。默认值为 6，表示选择警告和错误消息。任何非零值都可为通道本身启用调试输出，与通道定义中指定的 master_debug 相同。表 D-16 定义了 DEBUG 位掩码的位值。

表 D-16 DEBUG 位掩码

位	值	说明
0-31	-1	极其详细的输出
0	1	提示性消息
1	2	警告消息
3	4	错误消息
3	8	子例行程序调用跟踪
4	16	散列表诊断

表 D-16 DEBUG 位掩码 （续）

位	值	说明
5	32	I/O 诊断，接收
6	64	I/O 诊断，传输
7	128	SMS 到电子邮件转换的诊断 （移动设备始发和 SMS 通知）
8	256	PDU 诊断，标题数据
9	512	PDU 诊断，主体数据
10	1024	PDU 诊断，类型 — 长度 — 值数据
11	2048	选项处理；将所有选项设置发送到日志文件。

格式化模板

使用 FROM_FORMAT、 SUBJECT_FORMAT 和所有 DSN_* 通道选项指定的格式化模板都是 UTF-8 字符串，这些字符串可能包含文字文本与替换序列的组合。假设电子邮件地址样例为

```
Jane Doe <user@siroe>
```

已识别的替换序列显示在下文的表 D-17 中：

表 D-17 替换序列

序列	说明
$a	用创始者电子邮件地址的本地和域部分替换 （例如 “user@siroe”）
$d	用创始者电子邮件地址的域部分替换 （例如 “domain”）
$p	用创始者电子邮件地址的短语部分 （如果有）替换 （例如 “Jane Doe”）
$s	用 Subject: 标题行的内容替换
$u	用创始者电子邮件地址的本地部分替换 （例如 “user”）
\x	用文字字符 “x” 替换

例如，格式化模板

```
From:$a
```

将生成文本字符串

```
From:user@siroe
```

构造

```
${xy:alternate text}
```

可用于替换与序列 x 相关联的文本。如果该文本是空字符串，则会改用与序列 y 相关联的文本。而且，如果该文本为空字符串，则会替换替代文本。例如，假设将格式化模板

```
From:${pa:unknown sender}
```

用于创始者电子邮件地址

```
John Doe <jdoe@siroe.com>
```

（其中有一个短语部分），该模板将生成：

```
From:John Doe
```

但是，对于地址

```
jdoe@siroe.com
```

（其中没有短语），该模板将生成

```
From:jdoe@siroe.com
```

而对于空创始者地址，该模板将生成

```
From:unknown sender
```

添加附加 SMS 通道

您可以配置 MTA，使之具有多个 SMS 通道。执行此操作的典型原因有两个：

1. 为了与不同 SMPP 服务器进行通信。

   这是显而易见的：仅向配置中添加附加 SMS 通道，确保 (a) 为其取一个不同的通道名并且 (b) 使不同的主机名与其相关联。例如，

   ```
   sms_mway port 55555 threaddepth 20
   smpp.siroe.com

   sms_ace port 777 threaddepth 20
   sms.ace.net
   ```

   请注意，不需要新的重写规则。如果没有直接匹配的重写规则， Messaging Sever 就查找带有相关联主机名的通道。例如，如果用 `user@host.domain` 表示服务器，它就将查找名为 "host.domain" 的通道。如果它找到这样的通道，就在该通道中路由消息。否则，它将开始查找 ".domain" 重写规则，如果没有该规则，则查找点 (".") 规则。有关重写规则的更多信息，请参见第 255 页的第 11 章 “配置重写规则”。

2. 为了使用不同的通道选项与同一 SMPP 服务器进行通信。

   为了使用不同的通道选项与同一 SMPP 服务器进行通信，请在每个通道定义中的 `SMPP_SERVER` 通道选项中指定同一 SMPP 服务器。

   由于两个不同的通道不能有相同的正式主机名 （即，列在通道定义第二行中的主机名），所以有必要使用此机制。为了使它们能够与同一 SMPP 服务器进行通信，请定义两个独立的通道，并请在其通道选项文件的 `SMPP_SERVER` 中指定同一 SMPP 服务器。

   例如，您可以给出以下通道定义

   ```
   sms_mway_1 port 55555 threaddepth 20
   SMS-DAEMON-1

   sms_mway_2 port 55555 threaddepth 20
   SMS-DAEMON-2
   ```

   和重写规则

   ```
   sms-1.siroe.com $u%sms-1.siroe.com@SMS-DAEMON-1
   sms-2.siroe.com $U%sms-2.siroe.com@SMS-DAEMON-2
   ```

   然后，为了使它们都能使用同一 SMPP 服务器，这两个通道中的任何一个通道都应在其通道选项文件中指定 `SMPP_SERVER=smpp.siroe.com`。

调整传送重试的频率

如果某条 SMS 消息因为临时性错误 （例如，无法到达 SMPP 服务器）而无法传送，电子邮件消息将保留在传送队列中，并在以后再重试。除非另有配置，否则作业控制器将在一个小时后才进行重试。对于 SMS 消息传送来说，这一等待时间好像太长。在这种情况下，建议将 backoff 通道关键字与 SMS 通道配合使用，以为传送尝试指定一个更主动的安排。例如，

```
sms_mway port 55555 threaddepth 20 \
  backoff pt2m pt5m pt10m pt30m notices 1
smpp.siroe.com
```

对于上述设置，将在第一次尝试结束后两分钟进行一次重新传送尝试。如果再次失败，则请在第二次尝试后五分钟再次尝试。然后在十分钟后再试，此后每隔三十分钟重试一次。如果在一天之后仍不能传送， `notices 1` 通道关键字将会把该消息作为不可传送的消息予以返回。

单向配置范例 (MobileWay)

MTA SMS 通道可与任何 SMPP V3.4 兼容 SMPP 服务器配合使用。为便于说明配置示例，本节将解释如何配置 SMS 通道，以使其与 MobileWay SMPP 服务器配合使用。MobileWay (http://www.mobileway.com/) 是领先的全局数据和 SMS 连接性提供商。通过 MobileWay 路由您的 SMS 通信，您就可以实现与全球范围内大多数主要 SMS 网络上的 SMS 用户的通信。

如果用 MobileWay 申请 SMPP 帐户，系统可能会要求您回答以下问题：

- 您的 SMPP 客户机的 IP 地址：请提供 Internet 上其他域可见的您的 Messaging Server 系统的 IP 地址。
- 默认有效期：这是 MobileWay 将使用的 SMS 有效期，在您提交的 SMS 消息中不应指定有效期。在该有效期过期前不能传送的 SMS 消息将被放弃。请提供一个合理的有效期值 （例如 2 天、 7 天等）。
- 窗口大小：这个值是 SMPP 服务器在提交任何其他 SMS 消息前，您的 SMPP 客户机将停止并等待 SMPP 服务器响应之前将提交的 SMS 消息的最大数目。您必须提供一个至少能容纳 1 条消息的值。
- 时区：指定您的 Messaging Server 系统运行的时区。应将时区指定为一个 GMT 偏移。
- 超时：与单向 SMS 消息传送无关。
- 用于外挂请求的 IP 地址和 TCP 端口：与单向 SMS 消息传送无关。

对 MobileWay 提供了上述问题的答案以后，您将得到一个 SMPP 帐户以及与其 SMPP 服务器进行通信所必需的信息。此信息包括

```
Account Address: a.b.c.d:p
Account Login: system-id
Account Passwd: secret
```

Account Address 字段是将连接到的 MobileWay SMPP 服务器的 IP 地址 `a.b.c.d` 和 TCP 端口号 p。请将这些值用于 `SMPP_SERVER` 和 `SMPP_PORT` 通道选项。 Account Login 和 Passwd 是分别用于 `ESME_SYSTEM_ID` 和 `ESME_PASSWORD` 通道选项的值。使用此信息时，您的通道的选项文件应包括

```
SMPP_SERVER=a.b.c.d
SMPP_PORT=p
ESME_SYSTEM_ID=system-id
ESME_PASSWORD=secret
```

此时，要与 MobileWay 交互操作，就需要作两项附加选项设置

```
ESME_ADDRESS_TON=0x01
DEFAULT_DESTINATION_TON=0x01
```

`imta.cnf` 文件中的重写规则可以显示为

```
sms.your-domain $u@sms.your-domain
```

而 `imta.cnf` 文件中的通道定义可以显示为

```
sms_mobileway
sms.your-domain
```

通道选项文件、重写规则和通道定义适当显示后，就可以发送一条测试消息。MobileWay 要求国际寻址为以下格式

```
+<country-code><subscriber-number>
```

例如，要向用户编号为 (800) 555-1212 的北美用户发送一条测试消息，就应将您的电子邮件消息寄到

```
+18005551212@sms.your-domain
```

调试

要调试通道，请在通道的定义中指定 `master_debug` 通道关键字。例如，

```
sms_mway port 55555 threaddepth 20 \
  backoff pt2m pt5m pt10m pt30m notices 1 master_debug
```

使用 master_debug 通道关键字，有关通道操作的基本诊断信息将被输出到通道的日志文件中。要获得有关通道所承担的 SMPP 事务的详细诊断信息，还请在通道的选项文件中指定

```
DEBUG=-1
```

。

为双向 SMS 配置 SMS 通道

有关配置 SMS 通道的常规指导，请参见前文中从第 788 页的 “SMS 通道配置”开始的主题。尽管 SMS 通道可直接与远程 SMSC 通话，但除下文的表 D-18 中列出的例外情况之外仍应对 SMS 通道进行配置：

表 D-18 双向配置的例外情况

例外	解释
master 通道关键字	如果存在 master 通道关键字，则应将其删除。 不再需要配置 SMS 通道。
SMPP_SERVER	设置为指向 SMS Gateway Server 的 IP 地址的主机名。如果使用 SMPP 中继的 LISTEN_INTERFACE_ADDRESS 选项（请参见第 825 页的 “配置选项”），则请确保使用与指定的网络接口地址相关联的主机名或 IP 地址。
SMPP_PORT	使用与 LISTEN_PORT 设置所用的端口相同的 TCP 端口为例，说明 SMPP 中继（请参见第 823 页的 “SMPP 中继”）。
DEFAULT_SOURCE_ADDRESS	拾取一个值，然后配置远程 SMSC，以将此地址路由回 Gateway SMPP 服务器。在 SMS 通道的选项文件中，请使用此选项指定选定的值。
GATEWAY_PROFILE	设置为与网关配置文件的名称相匹配。请参见第 822 页的 “网关配置文件”。
USE_HEADER_FROM	设置为 0。

所有其他通道配置都应按照 SMS 通道文档中的介绍执行。

如第 820 页的 “设置双向 SMS 路由选择”中所述，需要对远程 SMSC 进行配置，以便如 DEFAULT_SOURCE_ADDRESS 通道选项中所定义的那样，使用 LISTEN_PORT 选项所指定的 TCP 端口号将 SMS 地址路由到网关的 SMP 服务器。（有关如何指定 LISTEN_PORT 的说明，请参见第 823 页的 “SMPP 服务器”。）

请注意，多个 SMS 通道可使用同一 SMS 中继。同样，只需要一个 SMPP 服务器或网关配置文件就可为多个 SMS 通道处理 SMS 多个回复和通知。存在对多个中继、服务器和网关配置文件进行配置的功能以通过配置选项影响不同的用法特征。

SMS Gateway Server 操作原理

通过使移动设备始发 SMS 消息与正确的电子邮件地址相匹配的机制，SMS Gateway Server 使得双向 SMS 更易于实现。本节包含以下 SMS Gateway Server 主题：

- 第 815 页的 “SMS Gateway Server 功能”
- 第 816 页的 “SMPP 中继和服务器性能”
- 第 818 页的 “SMS 回复和通知的处理”

SMS Gateway Server 功能

SMS Gateway Server 同时作为 SMPP 中继和服务器运行。还可将其配置为每种功能有多个 “实例”。例如，可以将其配置为拥有三种不同的 SMPP 中继，每种中继侦听不同的 TCP 端口或网络接口，并中继到不同的远程 SMPP 服务器。与此类似，还可以将其配置为拥有四个不同的 SMPP 服务器，每个服务器侦听不同组合的 TCP 端口和网络接口。

可以将 SMS Gateway Server 配置为拥有零个或多个向电子邮件地址发送 SMS 消息的网关配置文件。每个网关配置文件说明了哪个目标 SMS 地址与该配置文件相匹配，说明了如何从 SMS 消息中提取目标电子邮件地址，并说明了 SMS 到电子邮件转换过程的各种特征。通过 SMPP 中继或服务器递交到 SMS Gateway Server 的每条 SMS 消息都将与各个配置文件相比较。如果找到匹配项，则消息将被路由到电子邮件。

最后，网关配置文件还说明如何处理远程 SMSC 为响应以前的电子邮件到移动设备的消息而返回的通知消息。

SMPP 中继和服务器性能

如果作为 SMPP 中继，SMS Gateway Server 应尝试尽可能地透明，就是将来自本地 SMPP 客户机的全部请求中继到远程 SMPP 服务器，然后再中继回远程服务器的响应。但有两种例外情况：

- 如果本地 SMPP 客户机提交一条消息，此消息的 SMS 目标地址与已配置的网关配置文件之一相匹配，已提交的 SMS 消息就会直接返回到电子邮件；而该 SMS 消息将不会中继到远程 SMPP 服务器。
- 如果本地或远程 SMPP 客户机提交一条消息，此消息的 SMS 目标地址与 SMPP 中继先前所生成的唯一 SMS 源地址相匹配，此 SMS 消息就是对先前已中继的消息的回复。该回复回指向原始邮件的创始者。

请注意，一般可对 SMS Gateway Server 进行配置，以便其所生成的唯一 SMS 源地址与网关配置文件之一相匹配。

注 SMS Gateway Server 的 SMPP 中继仅用于与限定 Sun Java System SMPP 客户机 （即 Sun Java System Messaging Server 的 SMS 通道）配合使用。它不用于与任意 SMPP 客户机配合使用。

以下三种情况下，如果作为 SMPP 服务器， SMS Gateway Server 都将 SMS 消息定向到电子邮件：

- SMS 消息是移动设备始发的并且与网关配置文件相匹配。
- SMS 消息是移动设备始发的，并且 SMS 目标地址与以前生成的唯一 SMS 源地址相匹配。
- SMS 消息是 SMS 通知，它对应于 SMS Gateway Server 的 SMPP 中继以前所中继的电子邮件到移动设备的消息。

所有其他 SMS 消息都将被 SMPP 服务器拒绝。

远程 SMPP 到 Gateway SMPP 的通信

远程 SMPP 客户机使用协议数据单元 (PDU) 与 Gateway SMPP 服务器进行通信。远程 SMPP 客户机发布 Gateway SMPP 服务器所响应的请求 PDU。 Gateway SMPP 服务器同步运行。它在处理来自已连接的远程 SMPP 客户机的下一个请求 PDU 之前，先完成对一个请求 PDU 的响应。

下文的表 D-19 列出了 Gateway SMPP 服务器所处理的请求 PDU，并指定了 Gateway SMPP 服务器的响应。

表 D-19 SMPP 服务器协议数据单元

请求 PDU	SMPP 服务器响应
BIND_TRANSMITTER BIND_TRANSCEIVER UNBIND	与相应的响应 PDU 相对应。将忽略认证证书。
OUTBIND	Gateway SMPP 服务器发送回一个 BIND_RECEIVER PDU。将忽略递交的认证证书。
SUBMIT_SM DATA_SM	尝试将目标 SMS 地址与唯一的 SMS 源地址或网关配置文件的 SELECT_RE 设置相匹配。如果都不匹配， PDU 将被拒绝，并返回 ESME_RINVDSTADR 错误。
DELIVER_SM	尝试在历史记录中查找目标 SMS 地址或已收到的消息 ID。如果都不匹配，则返回错误 ESME_RINVMSGID。
BIND_RECEIVER	不支持。返回 GENERIC_NAK PDU，并返回 ESME_RINVCMDID 错误。
SUBMIT_MULTI	不支持。返回 GENERIC_NAK PDU，并返回 ESME_RINVCMDID 错误。
REPLACE_SM	不支持。返回 GENERIC_NAK PDU，并返回 ESME_RINVCMDID 错误。
CANCEL_SM	不支持。返回 GENERIC_NAK PDU，并返回 ESME_RINVCMDID 错误。
QUERY_SM	不支持。返回 GENERIC_NAK PDU，并返回 ESME_RINVCMDID 错误。
QUERY_LAST_MSGS	不支持。返回 GENERIC_NAK PDU，并返回 ESME_RINVCMDID 错误。
QUERY_MSG_DETAILS	不支持。返回 GENERIC_NAK PDU，并返回 ESME_RINVCMDID 错误。
ENQUIRE_LINK	返回 ENQUIRE_LINK_RESP PDU。
ALERT_NOTIFICATION	已接受但被忽略。

SMS 回复和通知的处理

SMS Gateway Server 保留通过其 SMPP 中继转发的每条 SMS 消息的历史记录。之所以需要使用历史数据，是因为这样的事实：在向 SMS 提交电子邮件消息时，通常不可能将消息发起人的电子邮件地址转换成 SMS 源地址。由于任何 SMS 回复和通知都将被定向到该 SMS 源地址，所以往往会出现问题。使用已中继消息中自动生成的唯一 SMS 源地址可以解决这一问题。然后，通过对远程 SMSC 进行配置，就可把这些 SMS 源地址路由回 Gateway SMPP 服务器。

历史数据将表示为消息 ID 和已生成的唯一 SMS 源地址的内存中散列表。这些信息还与相关联的电子邮件始发数据一起保存在磁盘上。基于磁盘的存储是一系列文件，每个文件表示长 `HASH_FILE_ROLLOVER_PERIOD` 秒的事务 （默认时间为 30 分钟）。每个文件将保留 `RECORD_LIFETIME` 秒钟 （默认时间为 3 天）。有关历史数据的内存中和磁盘上资源要求的讨论，请参见 Sun Java System Messaging Server Deployment Planning Guide (`http://docs.sun.com/doc/819-0063`)。

每条记录由三个部分组成：

- 电子邮件始发数据（例如信封 From: 和 To: 地址，地址）。此数据由 MTA SMS 通道在其提交消息时提供。
- 唯一的 SMS 源地址由 SMPP 中继生成并插入到已中继 SMS 消息中。
- 远程 SMSC 的 SMPP 服务器在其接收某项提交任务时返回的、最后收到的消息 ID。

SMS 回复的路由选择过程

Gateway SMPP 中继和服务器使用历史记录处理 SMS 回复、通知和移动设备始发的消息。当某条 SMS 消息递交到 SMPP 中继或服务器时，将进行以下路由选择过程：

1. 将 SMS 目标地址与历史记录相比较，以查看是否有由 SMPP 中继以前生成的、与之匹配的唯一 SMS 源地址。如果找到匹配地址，请参见步骤 6。
2. 如果没有匹配地址，而该消息是一个 SMS 通知 (SMPP `DELIVER_SM` PDU)，则会将接收到的消息 ID （如果有）与历史记录相比较。如果找到匹配地址，请转至步骤 8。 [实际上， SMS Gateway Server 允许将这些地址递交到 SMPP 中继或 SMPP 服务器。]
3. 如果没有匹配地址，则会将目标 SMS 地址与每个已配置网关配置文件的 `SELECT_RE` 选项表达式相比较。如果找到匹配地址，则请转至步骤 9。
4. 如果没有匹配地址并且 SMS 消息被递交到 Gateway SMPP 中继，则该消息就会被中继到远程 SMPP 服务器。

5. 如果没有匹配地址并且 SMS 消息被递交到 Gateway SMPP 服务器，则会确定该消息为无效消息，并在 SMPP 响应 PDU 中返回一个错误响应。对于电子邮件到 SMS，最终将生成一个非传送通知 (NDN)。
6. 如果找到匹配的唯一一个 SMS 源地址，则会进一步检查该 SMS 消息，以查看其是否是一个回复或一条通知消息。要成为通知消息，该消息就必须是一个带有已收到消息 ID 的 `SUBMIT_SM` PDU。否则，应将其看作是一个回复。
7. 如果其为回复，则会使用历史记录中的始发电子邮件信息将该 SMS 消息转换成电子邮件消息。
8. 如果其为通知，则会根据 RFC 1892-1894 将该 SMS 消息转换成电子邮件传送状态通知 (DSN)。请注意，将接受原始电子邮件消息的 ESMTP `NOTIFY` 标志 (RFC 1891)（例如，如果 SMS 消息是“成功的” DSN 而原始电子邮件消息仅需要“失败”通知，则该 SMS 通知就会被放弃）。
9. 如果目标 SMS 地址与已配置网关配置文件中的 `SELECT_RE` 选项相匹配，则该 SMS 消息就会被看作是一条移动设备发起的消息，并按照该网关配置文件的 `PARSE_RE_n` 规则将其转换回电子邮件消息。如果转换失败，则该 SMS 消息将无效并返回一个错误响应。

SMS Gateway Server 配置

本节介绍如何为电子邮件到移动设备和移动设备到电子邮件这两项功能设置 SMS Gateway Server。本节包含以下主题：

- 第 820 页的“设置双向 SMS 路由选择”
- 第 821 页的“启用和禁用 SMS Gateway Server”
- 第 821 页的“启动和停止 SMS Gateway Server”
- 第 821 页的“SMS Gateway Server 配置文件”
- 第 822 页的“配置网关服务器上的电子邮件到移动设备”
- 第 824 页的“配置移动设备到电子邮件的操作”
- 第 825 页的“配置选项”
- 第 838 页的“双向 SMS 配置示例”

设置双向 SMS 路由选择

在 MTA 和 SMSC 之间设置双向电子邮件和 SMS 路由选择所推荐的方法有三步过程：

- 设置 SMS 地址前缀 — 选择 SMS 地址前缀。可以使用任何长度不超过十个字符的前缀。
- 设置网关配置文件 — 保留与 SMS Gateway Server 配合使用的前缀 （通过设置网关配置文件）。
- 配置 SMSC — 配置 SMSC，以将 SMS 目标地址路由到以此前缀开头的 SMS Gateway SMPP 服务器。移动设备始发的电子邮件将只有前缀。回复和通知将不仅有前缀，其前缀后面还跟有十位十进制数。

设置 SMS 地址前缀

由 MTA SMS 通道生成的源 SMS 地址应被设置为与所选定的 SMS 地址前缀相匹配。通过设置以下几项即可完成此操作：

- MTA SMS 通道选项：

  `USE_HEADER_FROM=0`

  `DEFAULT_SOURCE_ADDRESS=`*`prefix`*

  第一个设置使通道无法尝试使用电子邮件消息中包含的信息设置 SMS 源地址。第二个设置使 SMS 源地址在未通过任何其他来源进行设置时对其进行设置 （设置成选定的前缀）。

- 将前缀识别为要接受并路由到电子邮件的 SMS 目标地址。通过指定如下 `SELECT_RE` 网关配置文件选项可完成此操作：

  `SELECT_RE=`*prefix*

设置网关配置文件

然后，应设置 SMS Gateway Server 的网关配置文件，以使所有已中继的 SMS 源地址都是唯一的地址。此设置是默认设置，但可通过指定网关配置文件选项 `MAKE_SOURCE_ADDRESSES_UNIQUE=1` 来进行显式设置。这样将得到如下格式的已中继 SMS 源地址：

prefixnnnnnnnnnn

其中 *nnnnnnnnnn* 是一个唯一的十位数十进制数字。

配置 SMSC

最后，应将 SMSC 配置为将所有与前缀 （或仅为前缀，或为前缀加一个十位数数字）相匹配的 SMS 目标地址路由到 SMS Gateway Server 的 SMPP 服务器。这种路由选择的正则表达式将类似于：

prefix([0-9]{10,10}){0,1}

其中 *prefix* 是 DEFAULT_SOURCE_ADDRESS 的值， [0-9] 指定可用于十位数数字的值，{10, 10} 指定将有十位数的最小和最大值，而 {0, 1} 指定可有零或一个十位数数字。

启用和禁用 SMS Gateway Server

- 要启用 SMS Gateway Server，必须将配置参数 local.smsgateway.enable 的值设置为 1。使用以下配置实用程序命令设置该值：

  ```
  # configutil -o local.smsgateway.enable -v 1
  ```

- 要禁用网关服务器，请使用以下命令将 local.smsgateway.enable 的值设置为 0：

  ```
  # configutil -o local.smsgateway.enable -v 0
  ```

启动和停止 SMS Gateway Server

启用了 SMS Gateway Server 后，可使用以下命令启动和停止它：

```
# start-msg sms
```

和

```
# stop-msg sms
```

SMS Gateway Server 配置文件

为了运行，SMS Gateway Server 需要一个配置文件。该配置文件是一个使用 UTF-8 记录的统一字符编码文本文件，该文件可以是一个 ASCII 文本文件。该文件的名称必须为：

installation-directory/config/sms_gateway.cnf

文件中的各选项设置的格式如下：

```
option-name=option-value
```

作为选项组一部分的选项以如下格式显示：

```
[group-type=group-name]
option-name-1=option-value-1
option-name-2=option-value-2
...
option-name-n=option-value-n
```

配置网关服务器上的电子邮件到移动设备

要实现双向 SMS 的电子邮件到移动设备部分，您必须完成以下配置：

- 第 822 页的 “网关配置文件”
- 第 823 页的 “SMPP 中继”
- 第 823 页的 “SMPP 服务器”

网关配置文件

要配置电子邮件到移动设备网关配置文件，请执行以下步骤：

1. 向 SMS Gateway Server 配置文件添加一个网关配置文件。

   要添加选项组，请使用以下格式：

   ```
   [GATEWAY_PROFILE=profile_name]
   option-name-1=option-value-1
   option-name-2=option-value-2a
   ...
   option-name-n=option-value-n
   ```

   网关配置文件名的长度 （前述格式的 `profile_name`）不得超过 11 个字节。文件名必须与 SMS 通道选项文件中的 `GATEWAY_PROFILE` 通道选项同名。文件名不区分大小写。有关有效通道选项的列表，请参见第 791 页的 “可用选项”。

2. 设置网关配置文件选项 （例如 `SMSC_DEFAULT_CHARSET`），以符合远程 SMSC 的特征。

3. 设置其他网关配置文件选项，以符合 SMS 通道的电子邮件特征。

   有关网关配置文件选项的完整说明，请参见第 833 页的 “网关配置文件选项”。

4. 设置 `CHANNEL` 选项。

   将其值设置为 MTA SMS 通道的名称。

   通过网关向电子邮件发送通知后，所得的电子邮件消息将被排入到使用该通道名称的 MTA 中。

SMPP 中继

要配置 SMPP 中继，请完成以下步骤：

1. 向 SMS Gateway Server 的配置文件中添加一个 SMPP 中继实例 （选项组）。

   要添加选项组，请使用以下格式：

   ```
   [SMPP_RELAY=relay_name]
   option-name-1=option-value-1
   option-name-2=option-value-2
   ...
   option-name-n=option-value-n
   ```

   任何名称都可用作中继的名称。重要的是，该中继名不得用于同一配置文件中的任何其他 SMPP 中继实例。

2. 设置 `LISTEN_PORT` 选项。

   用于 SMS 通道的 `SMPP_PORT` 选项的值必须与用于中继的 `LISTEN_PORT` 选项的值相匹配。对于 `LISTEN_PORT`，请选择一个未被任何其他 SMPP 中继或服务器实例所使用，也未被同一计算机上运行的任何其他服务器所使用的 TCP 端口号。

3. 设置 `SERVER_HOST` 选项。

   中继的 `SERVER_HOST` 选项应提供远程 SMSC 的 SMPP 服务器的主机名。可以使用 IP 地址代替主机名。

4. 设置 `SERVER_PORT` 选项。

   中继的 `SERVER_PORT` 选项应提供远程 SMSC 的 SMPP 服务器的 TCP 端口。

有关所有 SMPP 中继选项的完整说明，请参见第 829 页的 “SMPP 中继选项”。

SMPP 服务器

要配置 SMPP 服务器，请完成以下步骤：

1. 向 SMS Gateway Server 的配置文件中添加一个 SMPP 服务器实例（选项组）。

   要添加选项组，请使用以下格式：

   ```
   [SMPP_SERVER=server_name]
   option-name-1=option-value-1
   option-name-2=option-value-2
   ...
   option-name-n=option-value-n
   ```

   任何名称都可用作服务器的名称。重要的是，该服务器名不得用于同一配置文件中的任何其他 SMPP 服务器实例。

2. 设置 LISTEN_PORT 选项。

   选择一个任何其他服务器或中继实例没有使用的 TCP 端口号。此外，该端口号也未被同一计算机上的任何其他任何服务器所使用。

   需要将远程 SMSC 配置为通过 SMPP 将通知路由到使用此 TCP 端口的 SMS Gateway Server 系统。

有关所有 SMPP 服务器选项的完整说明，请参见第 831 页的“SMPP 服务器选项”。

配置移动设备到电子邮件的操作

要配置移动设备到电子邮件功能，则必须执行两个配置步骤：

- 第 824 页的 “配置移动设备到电子邮件网关配置文件”
- 第 825 页的 “配置移动设备到电子邮件 SMPP 服务器”

请注意，多个网关配置文件可使用同一个 SMPP 服务器实例。实际上，同一个 SMPP 服务器实例可同时用于电子邮件到移动设备和移动设备到电子邮件应用程序。

配置移动设备到电子邮件网关配置文件

对于由移动设备始发的消息，网关配置文件将提供两类关键信息：如何标识用于该配置文件的 SMS 消息和如何将这些消息转换成电子邮件消息。请注意，此配置文件可以与用于电子邮件到移动设备的配置文件相同，只不过增加了 SELECT_RE 选项。

要配置网关配置文件，请执行以下步骤：

1. 向 SMS Gateway Server 的配置文件添加一个网关配置文件 （选项组）。

   要添加选项组，请使用以下格式：

   ```
   [GATEWAY_PROFILE=profile_name]
   option-name-1=option-value-1
   option-name-2=option-value-2
   ...
   option-name-n=option-value-n
   ```

   配置文件的名称可使用长为 11 个字符或少于 11 个字符的任何名称。重要的是，它不能是已用于同一个配置文件中另一个网关配置文件的文件名。

2. 设置 SELECT_RE 选项，必须为每个网关配置文件指定该选项。

   此选项的值是一个 ASCII 正则表达式，可用于比较 SMS 目标地址。如果 SMS 目标地址与该正则表达式相匹配，则会通过网关将 SMS 消息发送到使用匹配配置文件所述的特征的电子邮件中。

   注意可以配置具有 SMS 地址的重叠集的多个网关配置文件 （例如，与地址 000 相匹配的配置文件和与任何其他三位数地址相匹配的其他配置文件）是重要的。但是，当 SMS 消息仅传送给一个网关配置文件 （第一个匹配文件）时，应避免执行此操作。而且，未定义比较的顺序。

3. 设置 CHANNEL 选项。

   其值应是 MTA 的 SMS 通道名。

有关所有移动设备始发选项的完整说明，请参见第 833 页的 “网关配置文件选项”。

配置移动设备到电子邮件 SMPP 服务器

添加的 SMPP 服务器与为电子邮件到移动设备添加的 SMPP 服务器相同（请参见第 823 页的 “SMPP 服务器”）。

需要将远程 SMSC 配置为将 SMS 通信路由到 Gateway SMPP 服务器。要执行此操作， SMSC 用于路由移动设备到电子邮件通信的 SMS 目标地址应是为网关配置文件选项 SELECT_RE 设置的值。

例如，如果要将 SMS 地址 000 用于移动设备到电子邮件通信，就需要配置 SMSC，以便将 SMS 目标地址 000 的通信路由到 Gateway SMPP 服务器。网关配置文件应使用选项设置 SELECT_RE=000。

配置选项

本节将详细说明 SMS Gateway Server 配置文件选项。下文各表列出了全部可用的配置选项以及各选项的简要说明。全局选项、 SMPP 中继选项、 SMPP 服务器选项和 SMS Gateway Server 配置文件选项各有一个表。

在以下小节中，给出了所有可用配置选项的完整说明。这些小节包括：

- 第 826 页的 “全局选项”

  全局选项必须放置在配置文件的顶部和所有选项组之前。其余选项必须显示在选项组中。

- 第 829 页的 “SMPP 中继选项”
- 第 831 页的 “SMPP 服务器选项”
- 第 833 页的 “网关配置文件选项”

全局选项

SMS Gateway Server 目前有三类全局选项：

- 线程调整选项
- 历史数据调整
- 其他

在指定任何选项组之前，必须将所有全局选项指定于配置文件的顶部。表 D-20 列出了所有全局配置选项。

表 D-20 全局选项

选项	默认值	说明
DEBUG	6	选择已生成的诊断输出的类型
HISTORY_FILE_DIRECTORY		历史数据文件的绝对目录路径
HISTORY_FILE_MODE	0770	历史文件的权限
HISTORY_FILE_ROLLOVER_PERIOD	30 分钟	向同一历史数据文件写入数据的最长时间
LISTEN_CONNECTION_MAX		所有 SMPP 中继和服务器实例上并行外来连接的最大数目
RECORD_LIFETIME	3 天	历史数据归档文件中记录的有效期
THREAD_COUNT_INITIAL	10 个线程	工作人员线程的初始数目
THREAD_COUNT_MAXIMUM	50 个线程	工作人员线程的最大数目
THREAD_STACK_SIZE	64 Kb	各工作人员线程的堆栈大小

线程调整选项

各外来 TCP 连接代表一个 SMPP 会话。会话处理由线程池中的工作人员线程处理。当会话处理需要等待 I/O 请求的完成时，工作人员线程停止会话并给出其他要执行的工作。 I/O 请求完成后，池中的可用工作人员线程就会恢复会话。

以下选项可用于调整此工作人员线程进程池：THREAD_COUNT_INITIAL, THREAD_COUNT_MAXIMUM, THREAD_STACK_SIZE.

THREAD_COUNT_INITIAL

（**整数，** *> 0*）为工作人员线程池初始创建的线程数目。该数目不包括用于管理内存中的历史数据的专用线程 （2 个线程），也不包括用于侦听外来 TCP 连接的专用线程 （SMS Gateway Server 所侦听的每个 TCP 端口 / 接口地址对各有一个线程）。THREAD_COUNT_INITIAL 的默认值为 10 个线程。

THREAD_COUNT_MAXIMUM

（**整数，** *>= THREAD_COUNT_INITIAL*）工作人员线程池中允许的线程的最大数目。默认值为 50 个线程。

THREAD_STACK_SIZE

（**整数，** *> 0*）工作人员线程池中各工作人员线程的堆栈大小 （字节）。默认值为 65536 个字节 (64 Kb)。

历史数据调整

如果一条 SMS 消息被中继，由接收的远程 SMPP 服务器生成的消息 ID 将保存在一个内存中的散列表中。还保存了该消息 ID 以及有关原始电子邮件消息的信息。如果该消息 ID 以后要被某 SMS 通知所引用，此信息就可以被检索出来。然后可以使用检索出来的信息将 SMS 通知发送给相应的电子邮件收件人。

内存中的散列表可通过专用线程返回到磁盘中。所得的磁盘文件被称为 “历史文件”。这些历史文件有两个用途：用于以非易失性形式保存在重新启动 SMS Gateway Server 后恢复内存中散列表所需的数据，并用于通过在磁盘上保存可能过长的数据来节省虚拟内存。每个历史文件的数据写入操作只能持续 HASH_FILE_ROLLOVER_PERIOD 秒，超过这个时间后，历史文件就会关闭并创建一个新的历史文件。如果历史文件超过 RECORD_LIFETIME 秒的周期，就会将其从磁盘中删除。

以下选项用于调整历史文件：HISTORY_FILE_DIRECTORY, HISTORY_FILE_MODE, HISTORY_FILE_ROLLOVER_PERIOD, RECORD_LIFETIME.

HISTORY_FILE_DIRECTORY

（**字符串，绝对目录路径**）用于将历史文件写入到的目录的绝对路径。如果路径不存在，将新建此目录路径。此选项的默认值为：

msg_svr_base/data/sms_gateway_cache/

所使用的目录应位于一个合理的快速磁盘系统中，并应有足够的可用空间用于预期的存储；有关存储规划的信息，请参见第 841 页的 “SMS Gateway Server 存储要求”。鼓励站点将此选项更改为更合适的值。

HISTORY_FILE_MODE

（**整数，八进制值**）与历史文件相关的文件权限。默认情况下，将使用值 0770 （八进制）。

HISTORY_FILE_ROLLOVER_PERIOD

（**整数，秒**）当前历史文件将关闭，并且每隔 HASH_FILE_ROLLOVER_PERIOD 秒创建一个新的历史文件。默认情况下，使用的秒数值为 1800 秒 （30 分钟）。

RECORD_LIFETIME

（**整数，秒数** > *0*）历史记录以秒为单位的有效期。超过这个有效期的记录将从内存中清除；超过这个有效期的历史文件则将从磁盘上删除。默认情况下，使用的值为 259,200 秒 （3 天）。保存在内中的记录将由专用来管理内存中数据的线程彻底清除。这些清除操作每 HASH_FILE_ROLLOVER_PERIOD 秒执行一次。磁盘上的文件在必须打开新的历史记录时被清除。

其他

另外还有两个选项：DEBUG 和 LISTEN_CONNECTION_MAX。

DEBUG

（**整数，位掩码**）启用调试输出。默认值为 6，表示选择警告和错误消息。

表 D-21 定义了 DEBUG 位掩码的位值。

表 D-21 DEBUG 位掩码

位	值	说明
0-31	-1	极其详细的输出
0	1	提示性消息
1	2	警告消息
3	4	错误消息
3	8	子例行程序调用跟踪
4	16	散列表诊断
5	32	I/O 诊断，接收
6	64	I/O 诊断，传输
7	128	SMS 到电子邮件转换的诊断 （移动设备始发和 SMS 通知）
8	256	PDU 诊断，标题数据
9	512	PDU 诊断，主体数据

表 D-21 DEBUG 位掩码 （续）

位	值	说明
10	1024	PDU 诊断，类型 - 长度 - 值数据
11	2048	选项处理；将所有选项设置发送到日志文件。

LISTEN_CONNECTION_MAX

（**整数，** >= *0*）所有 SMPP 中继和服务器实例上允许的并行外来 TCP 连接的最大数目。值 0 （零）指示对连接数目没有全局限制。但是，给定中继或服务器实例可能会给每个中继或服务器强加限制。

SMPP 中继选项

SMS Gateway Server 可以有其 SMPP 中继的多个实例，每个实例都有不同的特征，首要的特征将是所侦听的 TCP 端口和接口。为 SMPP 中继所侦听的每个网络接口和 TCP 接口对进行不同放置时，可能归因于不同的特征。将使用本节中所述的选项来指定这些特征。

每个实例都应放置在以下格式的选项组中：

```
[SMPP_RELAY=relay-name]
option-name-1=option-value-1
option-name-2=option-value-2
...
option-name-n=option-value-n
```

字符串 `relay-name` 仅用于将此实例与其他实例区分开。

表 D-22 列出了 SMPP 中继的配置选项。

表 D-22 SMPP 中继选项

选项	默认值	说明
LISTEN_BACKLOG	255	外来 SMPP 客户机连接的连接待办事项
LISTEN_CONNECTION_MAX		并行外来连接的最大数目
LISTEN_INTERFACE_ADDRESS		外来 SMPP 客户机连接的网络接口
LISTEN_PORT		外来 SMPP 客户机连接的 TCP 端口
LISTEN_RECEIVE_TIMEOUT	600 秒	读取 SMPP 的外来连接超时
LISTEN_TRANSMIT_TIMEOUT	120 秒	写入 SMPP 客户机的外来连接超时

表 D-22 SMPP 中继选项 （续）

选项	默认值	说明
MAKE_SOURCE_ADDRESSES_UNIQUE	1	使已中继 SMS 源地址成为唯一的地址并能作为回复地址
SERVER_HOST		要中继到的 SMPP 服务器的主机名或 IP 地址
SERVER_PORT		要中继到的 SMPP 服务器的 TCP 端口
SERVER_RECEIVE_TIMEOUT	600 秒	读取外发 SMPP 服务器连接超时
SERVER_TRANSMIT_TIMEOUT	120 秒	写入外发 SMPP 服务器连接超时

LISTEN_BACKLOG

（整数，范围在 *[0,255]* 之间）TCP 堆栈允许外来 SMPP 客户机连接拥有的连接待办事项。默认值为 255。

LISTEN_CONNECTION_MAX

（整数， >= *0*）允许该 SMPP 中继实例拥有的并行外来 TCP 连接的最大数目。请注意，如果该值超出全局 LISTEN_CONNECTION_MAX 的设置，将会忽略该值。

LISTEN_INTERFACE_ADDRESS

（字符串， *"INADDR_ANY"* 或点分十进制的 *IP* 地址）外来 SMPP 客户机连接要侦听的网络接口的 IP 地址。可以是字符串 “INADDR_ANY”（全部可用的接口）或是一个点分十进制形式的 IP 地址。（例如 193.168.100.1）。默认值为 “INADDR_ANY”。成簇的 HA 配置将需要将此值设置为对应于 HA 逻辑 IP 地址。

LISTEN_PORT

（整数， *TCP* 端口号）为接受外来 SMPP 客户机连接而绑定的 TCP 端口。必须指定此选项；此选项没有默认值。还请注意，此服务不赋予 Internet 指定的数字授权 (IANA)。

LISTEN_RECEIVE_TIMEOUT

（整数，秒数 > *0*）等待从 SMPP 客户机读取数据时所允许的超时。默认值为 600 秒（10 分钟）。

LISTEN_TRANSMIT_TIMEOUT

（整数，秒数 > *0*）向 SMPP 客户机发送数据时所允许的超时。默认值为 120 秒 （2 分钟）。

MAKE_SOURCE_ADDRESSES_UNIQUE

（*0* 或 *1*）默认情况下，SMPP 中继将向每个 SMS 源地址附加一个唯一的十位数字符串。然后，所得的 SMS 源地址将与其他历史数据一起保存。该结果则是 SMS 用户可以回复到的唯一 SMS 地址。如果用作 SMS 目标地址， SMPP 服务器将检测此地址，然后将 SMS 消息发送给正确的电子邮件创始者。

要禁止生成这种唯一的 SMS 源地址 （对于单向 SMS），请将此选项的值指定为 0（零）。

SERVER_HOST

（字符串， *TCP* 主机名或点分十进制 *IP* 地址）要将 SMPP 客户机通信中继到的 SMPP 服务器。可以指定一个主机名或 IP 地址。必须指定此选项；此选项没有默认值。

SERVER_PORT

（整数， *TCP* 端口号）要中继到的远程 SMPP 服务器的 TCP 端口。必须指定此选项；此选项没有默认值。没有为此服务指定的 IANA ； 不要与为 SNPP 指定的 IANA 相混淆。

SERVER_RECEIVE_TIMEOUT

（整数，秒数 > *0*）等待从 SMPP 服务器读取数据时所允许的超时。默认值为 600 秒（10 分钟）。

SERVER_TRANSMIT_TIMEOUT

（整数，秒数 > *0*）向 SMPP 客户机发送数据时所允许的超时。默认值为 120 秒 （2 分钟）。

SMPP 服务器选项

SMS Gateway Server 可以有其 SMPP 服务器的多个实例，每个实例都有不同的特征，首要的特征将是所侦听的 TCP 端口和接口。为 SMPP 服务器所侦听的每个网络接口和 TCP 接口对进行不同放置时，可能归因于不同的特征。将使用本节中所述的选项来指定这些特征。

每个实例都应放置在以下格式的选项组中：

```
[SMPP_SERVER=server-name]
option-value-1=option-value-1
option-value-2=option-value-2
...
option-name-n=option-value-n
```

字符串 server-name 仅用于将此实例同其他实例区分开。

表 D-23 列出了 SMPP 服务器的配置选项。

表 D-23 SMPP 服务器选项

选项	默认值	说明
LISTEN_BACKLOG	255	外来 SMPP 服务器连接的连接待办事项
LISTEN_CONNECTION_MAX		并行外来连接的最大数目
LISTEN_INTERFACE_ADDRESS		外来 SMPP 服务器连接的网络接口
LISTEN_PORT		外来 SMPP 服务器连接的 TCP 端口
LISTEN_RECEIVE_TIMEOUT	600 秒	外来 SMPP 服务器连接的读取超时
LISTEN_TRANSMIT_TIMEOUT	120 秒	外来 SMPP 服务器连接的写入超时

LISTEN_BACKLOG

（**整数，范围在** *[0,255]* **之间**） TCP 堆栈允许外来 SMPP 客户机连接拥有的连接待办事项。默认值为 255。

LISTEN_CONNECTION_MAX

（**整数** >= *0*）允许该 SMPP 服务器实例拥有的并行外来 TCP 连接的最大数目。请注意，如果该值超出全局 LISTEN_CONNECTION_MAX 的设置，将会忽略该值。

LISTEN_INTERFACE_ADDRESS

（**字符串，** *"INADDR_ANY"* **或点分十进制** *IP* **地址**）外来 SMPP 客户机连接要侦听的网络接口的 IP 地址。可以是字符串 "INADDR_ANY"（全部可用的接口）或是一个点分十进制形式的 IP 地址。（例如 193.168.100.1。）默认值为 "INADDR_ANY"。

LISTEN_PORT

（**整数，** *TCP* **端口号**）为接受外来 SMPP 客户机连接而绑定的 TCP 端口。必须指定此选项；此选项没有默认值。请注意，没有为此服务指定的 IANA。

LISTEN_RECEIVE_TIMEOUT

（**整数，秒数** > *0*）等待从 SMPP 客户机读取数据时所允许的超时。默认值为 600 秒（10 分钟）。

LISTEN_TRANSMIT_TIMEOUT

（**整数，秒数** > *0*）向 SMPP 客户机发送数据时所允许的超时。默认值为 120 秒 （2 分钟）。

网关配置文件选项

可能没有或有多个网关配置文件。在 SMS Gateway Sever 的配置文件中，每个网关配置文件都按以下格式在选项组中进行声明：

```
[GATEWAY_PROFILE=profile-name]
option-name-1=option-value-1
option-name-2=option-value-2
...
option-name-n=option-value-n
```

字符串 `profile-name` 仅用于将配置文件同其他始发配置文件区分开。

表 D-24 列出了 SMS Gateway Server 配置文件选项。

表 D-24 SMS Gateway Server 配置文件选项

选项	默认值	说明
CHANNEL	sms	用于对消息进行排入的通道
EMAIL_BODY_CHARSET	US-ASCII	电子邮件消息主体字符集
EMAIL_HEADER_CHARSET	US-ASCII	电子邮件消息标题字符集
FROM_DOMAIN		用于将电子邮件路由回 SMS 的域名
PARSE_RE_0, PARSE_RE_1, ..., PARSE_RE_9		用于解析 SMS 消息文本的正则表达式
PROFILE	GSM	在以下系统中运行的 SMS 配置文件：GSM、 TDMA 或 CDMA
SELECT_RE		用于选择插件的正则表达式
SMSC_DEFAULT_CHARSET	US-ASCII	SMSC 的默认字符集
USE_SMS_PRIORITY	0	Gateway SMS 的电子邮件优先级标志
USE_SMS_PRIVACY	0	Gateway SMS 的电子邮件保密性指示符

CHANNEL

（**字符串，** *1* **至** *40* **个字符**）用于对电子邮件消息进行排入的 MTA 通道的名称。如果未指定，则假设为 “sms”。指定的通道必须定义在 MTA 的配置中。

EMAIL_BODY_CHARSET

（**字符串，字符集名称**） SMS 文本在插入到电子邮件消息的主体之前要转换为的字符集。如果有必要，将对已转换的文本进行 MIME 编码。默认值为 US-ASCII。如果 SMS 消息包含字符集中所没有的符号，这些符号将被转换为助记字符，转换后的字符对收件人可能有意义，也可能没有。

MTA 认可的字符集的列表可在以下文件中找到：

installation-directory/config/charsets.txt

EMAIL_HEADER_CHARSET

（**字符串，字符集名称**）将 SMS 文本插入到 RFC 822 Subject: 标题行之前， SMS 文本要转换为的字符集。如果有必要，将对已转换的字符串进行 MIME 编码。默认值为 US-ASCII。如果 SMS 消息包含字符集中所没有的符号，这些符号将被转换为助记字符，转换后的字符对收件人可能有也可能没有意义

FROM_DOMAIN

（**字符串，** *IP* **主机名，** *1* **至** *64* **个字符**）在为电子邮件消息构造信封 From: 地址时要附加到 SMS 源地址中的域名。指定的主机名应是能将电子邮件路由回 SMS 的正确名称。（例如，与 MTA SMS 通道相关联的主机名。）如果未指定，则将使用利用 CHANNEL 选项指定的通道的正式主机名。

PARSE_RE_0, PARSE_RE_1, ..., PARSE_RE_9

（**字符串，** *UTF-8* **正则表达式**）对于电子邮件由移动设备始发的情况，网关配置文件需要从 SMS 消息的文本中提取目标电子邮件地址。此操作是通过一个或多个 POSIX 兼容的正则表达式 (RE) 来实现的。每个正则表达式都将计算 SMS 消息的文本，直到找到一个生成目标电子邮件地址的匹配项或正规表达式的列表用完为止。

注 PARSE_RE_* 和 ROUTE_TO 选项应相互独立使用。在同一网关配置文件中同时使用这两个选项将导致配置错误。

每个正则表达式都必须是 POSIX 兼容的，而且必须使用 UTF-8 字符集编码。正则表达式必须以字符串 0 的形式输出目标地址。它们可以随意输出要在 Subject: 标题行中用作字符串 1 的文本，以及要在消息主体中用作字符串 2 的文本。任何不被正则表达式所 “消耗的”文本还将用在消息主体中，其后跟随用字符串 2 的任何文本输出。

应以 PARSE_RE_0、PARSE_RE_1、... 至多到 PARSE_RE_9 的顺序尝试使用正则表达式。如果没有指定正则表达式，则将使用以下默认正则表达式：

```
[ \t]*([^\( ]*)[ \t]*(?:\(([^\)]*\))?[\t]*(.*)
```

这个默认正则表达式可分为以下几个成分：

```
[ \t]*
```

忽略前导空格字符 （SPACE 和 TAB）。

```
([^\( ]*)
```

目标电子邮件地址。这是首先报告的字符串。

```
[ \t]*
```

忽略空格字符。

```
(?:\(([^\)]*)$1\))?
```

包含在括号中的可选主题文本。这是第二次报告的字符串。前导 ?: 会使外围括号不报告字符串。它们只用于将其内容一起编组到一个后缀为 ? 的单一 RE 中。后缀 ? 使此 RE 组件仅匹配零或一次，等效于表达式 {0,1}。

```
[ \t]*
```

忽略空格字符。

```
(.*)
```

消息主体的其余文本。这是第三次报告的字符串。

例如，对于上述正则表达式， SMS 消息样例：

```
dan@sesta.com(Testing)This is a test
```

将产生电子邮件消息：

```
To:dan@sesta.com
Subject: Testing

This is a test
```

另一个示例， SMS 消息：

```
sue@sesta.com This is another test
```

将产生：

```
To:sue@sesta.com

This is another test
```

请注意，在用这些正则表达式进行计算之前，SMS 消息将被转换为统一字符编码的 UTF-16 编码。然后，已转换的文本将用先前已从 UTF-8 转换为 UTF-16 的正则表达式进行计算。然后，计算结果将转换为用于目标电子邮件地址的 US-ASCII、用于 `Subject:` 文本的 `EMAIL_HEADER_CHARSET` （如果有）以及用于邮件主体的 `EMAIL_BODY_CHARSET` （如果有）。

PROFILE

（**字符串，“*GSM*”、“*TDMA*”或“*CDMA*”**）要采用的 SMS 配置文件。目前此信息只用于将 SMS 优先级标志映射到 RFC 822 `Priority:` 标题行标题行。所以，当 `USE_SMS_PRIORITY=0` （这是此选项的默认设置）时，此选项将不会有影响。

SELECT_RE

（**字符串，*US-ASCII* 正则表达式**）要与每个 SMS 消息的 SMS 目标地址进行比较的 US-ASCII POSIX 兼容正则表达式。如果某条 SMS 消息的目标地址与此 RE 相匹配，则该 SMS 消息将通过网关发送到与此网关配置文件相一致的电子邮件中。

请注意，由于 SMS 消息的目标地址是以 US-ASCII 字符集指定的，所以此正则表达式还必须用 US-ASCII 表示。

SMSC_DEFAULT_CHARSET

（**字符串，字符集名称**）远程 SMSC 所使用的默认字符集的名称。此选项的两个通用选项为 US-ASCII 和 UTF-16-BE (USC2)。如果未指定，则假设为 US-ASCII。

USE_SMS_PRIORITY

（**整数，*0* 或 *1***）默认情况下 （当 `USE_SMS_PRIORITY=0` 时），SMS 消息中的优先级标志将被忽略并且不与电子邮件消息一起发送。要与电子邮件一起传送优先级标志，请指定 `USE_SMS_PRIORITY=1`。当与电子邮件一起传送时，从 SMS 到电子邮件的映射如表 D-25 所示。

表 D-25 从 SMS 到电子邮件的优先级标志映射

SMS 配置文件	SMS 优先级标志	电子邮件 Priority: 标题行
GSM	0 （非优先级）	无标题行 （表示 Normal）
	1, 2, 3 （优先级）	Urgent

表 D-25 从 SMS 到电子邮件的优先级标志映射

SMS 配置文件	SMS 优先级标志	电子邮件 Priority: 标题行
TDMA	0（大量）	不急
	1（正常）	无标题行（表示 Normal）
	2（紧急）	Urgent
	3（非常紧急）	Urgent
CDMA	0（正常）	无标题行（表示 Normal）
	1（交互）	Urgent
	2（紧急）	Urgent
	3（紧急）	Urgent

请注意，电子邮件 Priority: 标题行的值包括 Nonurgent、 Normal 和 Urgent。

USE_SMS_PRIVACY

（整数， *0* 或 *1*）默认情况下（当 USE_SMS_PRIVACY=0 时）， SMS 保密性指示被忽略并且不与电子邮件消息一起发送。要将此消息与电子邮件一起传送，请指定 USE_SMS_PRIVACY=1。当与电子邮件一起传送时，从 SMS 到电子邮件的映射如表 D-26 所示。

表 D-26 从 SMS 到电子邮件的优先级标志映射

SMS 保密性标志	电子邮件 Sensitivity: 标题行
0（无限制）	无标题行
1（有限制）	Personal
2（机密）	Private
3（秘密）	Company-confidential

请注意，电子邮件 Sensitivity: 标题行的值包括 Personal、 Private 和 Company-confidential。

双向 SMS 配置示例

性能假设

在方便解释此示例，假设需要以下性能：

- 定址到

  `sms-id@sms.domain.com`

  的电子邮件消息要发送到 SMS 地址

  `sms-id`

  并在范围 `000`*nnnnnnnnnn* 内给定一个唯一的 SMS 源地址。

- 定址到 SMS 地址 `000` 的移动设备 SMS 消息将通过网关发送到带有从 SMS 消息文本开始处提取的电子邮件地址的电子邮件。

  例如，如果 SMS 消息文本为：

  `jdoe@domain.com Interested in a movie?`

  则消息 “Interested in a movie?”将发送至 jdoe@domain.com。

- 发送到 `000`*nnnnnnnnnn* 的 SMS 通知将通过网关发送给电子邮件并定向到接收该消息的创始者。

为了实现此性能，需要进行如下假设和指定

进一步的假设和指定

- MTA 的 SMS 通道使用域名 `sms.domain.com`。
- SMS Gateway Server 在主机 gateway.domain.com 上运行并将：
  - TCP 端口 503 用于其 SMPP 中继
  - TCP 端口 504 用于其 SMPP 服务器
- 远程 SMSC 的 SMPP 服务器在主机 `smpp.domain.com` 上运行并侦听 TCP 端口 377。
- 远程 SMSC 的默认字符集是 UCS2 （亦称 UTF-16）。

SMS 通道配置

要实现上述性能，可以在 imta.cnf 文件中使用以下 SMS 通道配置 （将这些行添加至文件底部）：

```
（空行）
sms
sms.domain.com
```

SMS 通道选项文件

然后，通道的选项配置文件 sms_option 将包含以下设置：

```
SMPP_SERVER=gateway.domain.com
SMPP_PORT=503
USE_HEADER_FROM=0
DEFAULT_SOURCE_ADDRESS=000
GATEWAY_PROFILE=sms1
SMSC_DEFAULT_CHARSET=UCS2
```

SMS Gateway Server 配置

最后， Gateway Server 配置文件 sms_gateway.cnf 应类似于以下内容：

```
HISTORY_FILE_DIRECTORY=/sms_gateway_cache/

[SMPP_RELAY=relay1]
LISTEN_PORT=503
SERVER_HOST=smpp.domain.com
SERVER_PORT=377

[SMPP_SERVER=server1]
LISTEN_PORT=504

[GATEWAY_PROFILE=sms1]
SELECT_RE=000([0-9]{10,10}){0,1}
SMSC_DEFAULT_CHARSET=UCS2
```

测试此配置

如果没有可用于测试的 SMSC，您可能需要执行某些回送测试。使用 sms_option 文件中的某些附加设置可对上述配置执行某些简单的回送测试。

sms_option 文件的附加设置

sms_option 文件的附加设置包括：

```
! So that we don't add text to the body of the SMS message
FROM_FORMAT=
SUBJECT_FORMAT=
CONTENT_PREFIX=
```

没有这些设置，包含以下内容：

```
user@domain.com (Sample subject) Sample text
```

的电子邮件就会转换成 SMS 消息：

```
From:user@domain.com Subject:Sample Subject Msg:Sample text
```

反过来，这将不会是移动设备到电子邮件代码所期望看到的格式：

```
user@domain.com (Sample subject) Sample text
```

因此，需要 （用于回送测试）为 FROM_FORMAT、 SUBJECT_FORMAT 和 CONTENT_PREFIX 选项指定空字符串。

执行回送测试

发送寻址到 000@sms.domain.com 的测试电子邮件消息，例如：

```
user@domain.com (Test message) This is a test message which should loop back
```

结果是，此电子邮件消息应路由回电子邮件收件人 user@domain.com。请确保已将 sms.domain.com 添加至您的 DNS 或主机表中，以进行测试。

SMS Gateway Server 存储要求

要确定 SMS Gateway Server 所需要的资源数量，请使用您从表 D-27 中的要求生成的数字，同时还要使用您预期每秒中继的消息的数目以及 RECORD_LIFETIME 设置。

表 D-27 包含了历史记录、 SMPP 中继和 SMPP 服务器的要求。

表 D-27 SMS Gateway Server 存储要求

组件	要求
内存中历史记录	已中继的每一条消息都要求 33+m+s 个字节的虚拟内存，其中 m 是此消息的 SMS 消息 ID 的长度 (1 <= m <= 64)， s 是此消息的 SMS 源地址的长度 (1 <= s<= 20)。 当 MAKE_SOURCE_ADDRESS_UNIQUE=0 时，则仅使用 16+m 个字节。对于 64 位操作系统，每条记录都将消耗 49+m+s 个字节的虚拟内存 [当 MAKE_SOURCE_ADDRESS_UNIQUE=0 时为 24+m]。 还请注意，堆分配器实际上可能为每条记录分配更大的虚拟内存。 记录的最大数目为 430 亿条 (2**32-1)。记录数目少于 1680 万条 (2**24) 时，散列表将消耗大约 16 Mb ；记录少于 6710 万条 (2**26) 时，散列表将消耗大约 64 Mb ；记录大于 6710 万条时，散列表将消耗大约 256 Mb。 64 位操作系统的内存消耗量加倍。 这些消耗不包括各条消息本身所需的内存消耗。
盘上历史记录	每条已中继的消息所需字节的平均数目如下： 81+m+2s+3a+S+2i 其中： • m 是 SMS 消息 ID 的平均长度，且 1<=m<=64 • s 是 SMS 源地址的平均长度，且 1 <= s <= 20 • a 是电子邮件地址的平均长度，且 3 <= a <= 129 • S 是 Subject: 标题行的的平均长度，且 0 <= S<= 80 • i 是电子邮件消息信封 ID 的平均长度，且 0 <= i <= 129 任何指定记录的大小都受消息的信封 From: 和 To: 地址的长度、信封和消息 ID 的长度以及 Subject: 标题行的长度的影响。 最大记录长度为 910 个字节。 使用 MAKE_SOURCE_ADDRESS_UNIQUE=0 时，每条记录的大小 （以字节为单位）都为： 78+m+3a+S+2i。

表 D-27 SMS Gateway Server 存储要求 （续）

组件	要求
SMPP 中继	每条已中继的 SMPP 会话将消耗两个 TCP 端口：一个与本地 SMPP 客户机连接，另一个与远程 SMPP 服务器连接。在 32 位操作系统中，每条连接将消耗大约 1 Kb 的虚拟内存；在 64 位操作系统中则要消耗 2 Kb。
SMPP 服务器	每条外来连接都消耗一个 TCP 插槽。在 32 位操作系统中，每条连接将消耗大约 1 Kb 的虚拟内存；在 64 位操作系统中则要消耗 2 Kb。

例如，如果每秒中平均有 50 条消息需要中继， SMS 源地址的长度为 13 个字节，SMS 消息 ID 的一般长度为 12 个字节，电子邮件地址则为 24 个字节，`Subject:` 行为 40 个字节，电子邮件消息和信封 ID 各为 40 个字节，而历史记录则需要保留 7 天，则：

- 将有 3024 万条历史记录需要保存，每条平均要消耗内存 58 个字节并且消耗磁盘空间 311 个字节；
- 历史记录的内存中消耗将大约为 1.70 Gb (1.63 Gb + 64 Mb) ；并且
- 消耗的盘上存储大约为 8.76 Gb。

如果可以提供足够的磁盘空间以处理任何磁盘要求，将严格限制 32 位计算机上的虚拟内存要求大约为 2Gb。要减少虚拟内存或磁盘存储所需的数量，请使用 `RECORD_LIFETIME` 选项较少记录保留时间长度。

安装工作单

本附录提供了可以用来规划安装的工作单。将介绍以下工作单：

- Directory Server 安装
- Administration Server 初始运行时配置
- Directory Server 安装程序脚本 (comm_dssetup.pl)
- Messaging Server 初始运行时配置

Directory Server 安装

您可以通过 Java Enterprise System 安装程序或通过以前的安装来安装 Directory Server。请将您的 Directory Server 安装和配置参数记录到表 E-1 （它是显示在 Messaging Server Deployment Planning Guide 中的工作单副本）中。安装和配置 Administration Server 和 Messaging Server 时将需要这些参数。

表 E-1 Directory Server 安装参数

参数：	说明：	示例：	用于：	您的答案：
Directory Server 安装根目录	Directory Server 计算机上专用于保存服务器程序文件、配置文件、维护文件和信息文件的目录。	`/var/mps/serverroot/`	`comm_dssetup.pl` Perl 脚本 请参见第 39 页的“为 Messaging Server 配置准备 Directory Server”。	
主机	此主机名为 IP 主机名，它可以是“简捷形式”主机名（例如 `fiddle`），也可以是全限定主机名。全限定主机名由两部分组成：主机名和域名。	`fiddle.west.sesta.com`	Administration Server 配置 请参见第 39 页的“为 Messaging Server 配置准备 Directory Server”。	
LDAP Directory 端口号	用于 LDAP Directory Server 的默认端口号是 `389`。	`389`	Administration Server 配置和 Messaging Server 配置 请参见第 39 页的“为 Messaging Server 配置准备 Directory Server”和第 49 页的“创建初始 Messaging Server 运行时配置”	
管理员 ID 和密码	管理或负责配置信息的管理员。 管理员密码	`Admin` PaSsWoRd	Administration Server 配置 请参见第 39 页的“为 Messaging Server 配置准备 Directory Server”。	

参数：	说明：	示例：	用于：	您的答案：
用户和组树后缀	目录树顶部的 LDAP 条目的标识名，该条目的下面存储了用户和组数据。	`o=usergroup`	`comm_dssetup.pl` Perl 脚本 请参见第 39 页的“为 Messaging Server 配置准备 Directory Server”。	
目录管理员 DN 和密码	具有特权的目录管理员，类似 UNIX 中的超级用户。通常此管理员负责用户和组数据。 目录管理员的密码。	`cn=Directory Manager` `pAsSwOrD`	`comm_dssetup.pl` Perl 脚本和 Messaging Server 配置 请参见第 39 页的“为 Messaging Server 配置准备 Directory Server”和第 49 页的“创建初始 Messaging Server 运行时配置”。	
管理域	管理控制的区域。	`System Lab`	Administration Server 配置 请参见第 39 页的“为 Messaging Server 配置准备 Directory Server”。	

Administration Server 初始运行时配置

在执行 Java Enterprise System 安装程序过程中，当运行 Administration Server 初始运行时配置程序时，请将您的安装参数记录到表 E-2（它是显示在 Messaging Server Deployment Planning Guide 中的工作单副本）。您需要将其中的某些参数用于 Messaging Server 初始运行配置。您还可以参考 第 844 页的 “Directory Server 安装”核对表来回答某些问题。

表 E-2 Administration Server 初始运行时配置程序参数

参数	说明	示例	您的答案：
全限定域名	主机计算机的全限定域。	`fiddle.west.sesta.com`	
服务器根目录定义	Administration Server 的安装根目录，专用于保存服务器程序文件、配置文件、维护文件和信息文件。	`/var/mps/serverroot`	
UNIX 系统用户	指定给系统用户的特定权限，以确保他们对所运行的进程具有适当的权限。	`inetuser`	
UNIX 系统组	特定 UNIX 系统用户所属的组。	`inetgroup`	
Configuration Directory Server	第 844 页的 “Directory Server 安装”期间指定的主机和端口。	主机 `fiddle.west.sesta.com` 端口 `389`	
配置 Directory Server 管理员和密码	第 844 页的 “Directory Server 安装”期间指定的管理员 ID。 管理员 ID 的密码	`Admin` PaSsWoRd	
管理域	管理控制的区域。 如果将 Messaging Server 和 Directory Server 安装在同一计算机上，则应在第 844 页的 “Directory Server 安装”中选择相同的管理域。	System Lab2	
Administrative Server 端口	专用于 Administration Server 的唯一端口号。	`5555`	

Directory Server 安装程序脚本 (comm_dssetup.pl)

运行 Directory Server 安装程序脚本 (comm_dssetup.pl) 以准备用于 Messaging Server 配置的 Directory Server 时，请将安装参数记录在表 E-3 中。您需要将其中的某些参数用于 Messaging Server 初始运行配置。

表 E-3 comm_dssetup.pl 脚本参数

参数	说明	示例	您的答案：
服务器根目录	Directory Server 的安装根目录，专用于保存服务器程序文件、配置文件、维护文件和信息文件。	/var/mps/serverroot/	
服务器实例	负责大多数功能的 LDAP Directory Server 守护程序或服务。在某些部署中，可以将某个实例专用于维护用户和组，而保留另一个实例用于配置。	slapd-varrius	
DC 根目录	如果您希望拥有两个树的 DIT 置备模型 （Sun LDAP Schema 1 或 Sun ONE LDAP Schema 2 [兼容模式]）， DC Tree 将镜像本地 DNS 结构，系统将使用它作为组织树 （包含用户和组的数据条目）的索引。	o=internet	
用户和组基本后缀	组织树顶层的条目，包含用于用户和组的条目的名称空间。	o=usergroup	
目录管理员 DN 和密码	组织树中负责用户和组数据的管理员。应该与 Sun Java Enterprise System 安装程序中指定的管理员相同。 目录管理员 DN 的密码	cn=Directory Manager pAsSwOrD	

Messaging Server 初始运行时配置

运行 Messaging Server 初始运行时配置程序时，请将安装参数记录在表 E-4 中。您还可以参考 第 844 页的 “Directory Server 安装”核对表来回答某些问题。

表 E-4 Messaging Server 初始运行时配置程序参数

参数	说明	示例	您的答案：
配置和数据目录	包含所有 Messaging Server 配置文件。 *msg_svr_base*/data 目录已符号链接到此目录。	/var/opt/SUNWmsgsr	
UNIX 系统用户	指定给系统用户的特定权限，以确保他们对所运行的进程具有适当的权限。此系统用户不应该与您在 Administration Server 初始运行配置中指定的用户相同。	mailsrv	
UNIX 系统组	特定 UNIX System 用户所属的组。此系统组不应该与您在 Administration Server 初始运行配置中指定的组相同。	mail	
配置目录 LDAP URL、目录管理员和密码	配置 Directory Server、LDAP URL、绑定 DN 和密码	ldap://fiddle.west.sesta.com:389 cn=Directory Manager PaSsWoRd	
用户和组目录 LDAP URL、目录管理员和密码	用户和组 Directory Server、LDAP URL、绑定 DN 和密码。 建议您使用独立与配置目录的用户和组目录。	ldap://fiddle.west.sesta.com:389 cn=Directory Manager PaSsWoRd	
邮寄主管电子邮件地址	将监视邮寄主管邮件的管理员的电子邮件地址。该地址必须是全限定地址而且必须有效，其中带有与地址关联的邮箱。	pma@siroe.com	
管理员帐户的密码	将用作服务管理员密码、用户 / 组管理员密码、最终用户管理员权限密码以及 PAB 管理员密码和 SSL 密码的密码。	paSSwoRD	

表 E-4 Messaging Server 初始运行时配置程序参数 （续）

参数	说明	示例	您的答案：
默认电子邮件域	未指定域时使用的默认电子邮件	siroe.com	
默认电子邮件域的组织名	组织名，您的组织将位于其下，并将用它构造组织树。	例如，如果组织名为 Engineering，则 siroe.com（默认电子邮件域）中的所有用户将被放置在 LDAP DN（o=Engineering、o=usergroup）之下。 用户和组目录后缀是在 comm_dssetup.pl 中指定的。	

词汇表

有关此文档集中使用的术语的完整列表，请参见 Sun Java Enterprise System 词汇表 (http://docs.sun.com/doc/819-1935)。

索引

符号

! （感叹号）
  作为注释指示符 207
$? 277
$A 276
$B 276
$C 275，277
$E 276
$F 276
$M 275，277
$N 275，277
$P 276
$Q 275，277
$R 187，276
$S 276
$T 277
$U substitution sequence 267
$V 182
$V 元字符 186
$X 276
$Z 182
% （百分比符号） 275
(A\!B)((-))C 329
* 567
*.CHANGES 文件 68
*.MERGED 文件 68
+ 116
.HELD 邮件 700
/ 匹配 213
/etc/nsswitch.conf 696
? （at 符号） 277
\! （感叹号）
  在地址中 264
\| 垂直条 260

数字

220 标题 696
733 328
8 位字符 703
822 328

英文

A!B%C 329
A!B?C 329
A@B@C 330
A\!(B((-))C) 329
Access Manager 129
ACCESS_ORCPT 460，462
ACL 500
addheader 415
addreturnpath 333
addrsperfile 350

Administration Server
工作单 846
after 通道关键字 319
alarm.diskavail 735
alarm.diskavail.msgalarmdescription 714
alarm.diskavail.msgalarmstatinterval 714，735
alarm.diskavail.msgalarmthreshold 714，735
alarm.diskavail.msgalarmthresholddirection 736
alarm.diskavail.msgalarmwarninginterval 714，736
alarm.msgalarmnoticehost 735
alarm.msgalarmnoticeport 735
alarm.msgalarmnoticercpt 715，735
alarm.msgalarmnoticesender 735
alarm.serverresponse 736
alarm.serverresponse.msgalarmstatinterval 736
alarm.serverresponse.msgalarmthreshold 736
alarm.serverresponse.msgalarmthresholddirection 736
alarm.serverresponse.msgalarmwarninginterval 736
ALIAS_DOMAINS 336
ALIAS_ENTRY_CACHE_SIZE 201
ALIAS_ENTRY_CACHE_TIMEOUT 201
ALIAS_MAGIC 185，204
ALIAS_URL0 185，204
ALIAS_URL1 185，204
ALIAS_URL2 185，204
aliasdetourhost 355
aliasedObjectName 183
aliaslocal 336
aliaspostmaster 250
ALLOW_RECIPIENTS_PER_TRANSACTION 300
ALLOW_REJECTIONS_BEFORE_DEFERRAL 359
ALLOW_TRANSACTIONS_PER_SESSION 300
allowetrn 303
allowetrn 通道关键字 304
allowswitchchannel 通道关键字 314
alternateblocklimit 347
alternatechannel 347
alternatelinelimit 347
alternaterecipientlimit 347
alwaysencrypt 618
alwayssign 618
AMSDK 131
APOP 575
appid 140
Arabic 字符检测 379
associatedDomain 184
at 符号 264，275，277
authrewrite 316
auto_ef 379
backoff 321
backoff 通道关键字 319
bang 式样 (UUCP) 地址 259
bang 式样地址约定 264
bangoverpercent 329
bangoverpercent 关键字 264
bangstyle 328
bidirectional 320
BLOCK_SIZE 344，346
blocketrn 303
blocketrn 通道关键字 304
blocklimit 346
blSWClientDesintationForeign 409
blSWClientDestinationDefault 408
blSWClientDestinationLocal 409
blswcServerAddress 409
blSWLocalDomain 408
blSWPrecedence 408
blSWUseClientOptin 409
Brightmail
MTA 通道关键字 400
部署 407
配置文件选项 408
体系结构 405
要求和性能 407
CA 证书
安装 581
管理 582
cacheeverything 通道关键字 311
cachefailures 通道关键字 311
cachesuccesses 通道关键字 311

cert8.db 147，153
certmap.conf 587
certutil 618
certutil 588
charset7 通道关键字 306
charset8 通道关键字 306
CHARSET-CONVERSION 343
charsetesc 通道关键字 306
checkehlo 303
checkehlo 通道关键字 303
checkoverssl 619
cmsutil 588
comm_dssetup.pl 39
  工作单 40，847
  交互模式 41
  无提示模式 47
  要求 40
commadmin domain delete 96
commadmin domain purge 95，96
commadmin user delete 95
COMMENT_STRINGS 映射表 334
commentinc 334
commentomit 334
commentstrip 334
commenttotal 334
Communications Express
  故障排除 567
Communications Express Mail 605
Communications Services
  文档 34
configutil
  alarm.diskavail 735
  alarm.msgalarmnoticehost 735
  alarm.msgalarmnoticeport 735
  alarm.msgalarmnoticercpt 735
  alarm.msgalarmnoticesender 735
  alarm.serverresponse 736
  encryption.nsssl3ciphers 586
  encryption.rsa 586
  gen.newuserforms 104
  gen.sitelanguage 108
  local.service.http.proxy 163
  local.service.pab 110
  local.sso 140
  local.store.notifyplugin 752
  local.ugldapbasedn 110
  local.ugldapbindcred 162
  local.ugldapbinddn 110，162
  local.ugldaphost 110，162
  local.ugldapport 110
  local.ugldapuselocal 110
  local.webmail.sso 141
  logfile.service 676
  nsserversecurity 586
  sasl.default 576
  sasl.default.ldap 576
  service.dcroot 162
  service.defaultdomai 163
  service.http 127
  service.http.plaintextmincipher 124
  service.imap 124
  service.imap.banner 116
  service.loginseparator 116，163
  service.pop 122
  service.pop.banner 116
  service.service 599
  store.admins 497
  store.defaultmailboxquota 513
  store.partition 530
  store.quotaenforcement 516
  store.quotaexceedmsginterval 515
  store.quotagraceperiod 518
  store.quotanotification 514
  store.quotawarn 515
conn_throttle.so 467
connectalias 330
connectcanonical 330
Console 96
conversions 文件 368
copysendpost 247
copywarnpost 248
counterutil 725，733
  db_lock 722
  diskusage 727
  POP，IMAP，HTTP 726
  serverresponse 727
  警报统计数据 725

输出 725
counterutil -l 724
CRAM-MD5 575
crdb 219，479
crlaccessfail 619
crldir 619
crlenable 619
crlmappingurl 620
crlurllogindn 620
crlurlloginpw 620
crlusepastnextupdate 620
crontab 103
daemon 通道关键字 314
datefour 340
datetwo 340
dayofweek 340
dcroot
Messenger Express Multiplexor 162
defaultmx 通道关键字 313
defaultnameservers 通道关键字 313
DEFER_GROUP_PROCESSING 199
deferralrejectlimit 359
deferred 319，320
defragment 343
Delegated Administrator 55
Delegated Administrator for Messaging 95
deleted 523
DELIVERY_OPTIONS 195，450，451
dequeue_removeroute 337
destinationfilter 354，483
destinationnosolicit 358
destinationspamfilterXoptin 282，355，400
DIAGNOSTIC_CODE 245
DIGEST-MD5 575
Directory Server 108
工作单 844
配置目录 108
配置设置 108
要求 108
用户目录 95，108
Directory Server 拷贝 54
dirsync 181
disableetrn 303
disconnectbadauthlimit 346
disconnectbadcommandlimit 351
disconnectrecipientlimit 351
disconnectrejectlimit 351
disconnecttransactionlimit 351
dispatcher.cnf 文件 667
disposition_option.dat 245
dispositionchannel 353
DNS
IDENT 协议 311
MX 记录 313
反向查找 311
域验证 306
DNS 查找 476
DNS 问题
MTA 故障排除 709
dns_verify 476
do_the_upgrade.sh 72
domain
DNS 验证 306
停止外来处理 688
DOMAIN_FAILURE 184
DOMAIN_MATCH_URL 183，204
DOMAIN_UPLEVEL 182，186，188
domainetrn 303
domainetrn 通道关键字 304
domainUidSeparator 186
domainvrfy 305
dropblank 332
EHLO 300
ehlo 303
EHLO 命令 303
ehlo 通道关键字 303
eightbit 通道关键字 307
eightnegotiate 通道关键字 307
eightstrict 通道关键字 307
encryption.nsssl3ciphers 586
encryption.rsa 586
ENS 749

管理 751
配置参数 752
启动和停止 751
启用 750
样例程序 750
envelope To: 地址 275
errsendpost 247
errwarnpost 248
ETRN 命令 303
ETRN 命令支持 303
exclusive 522
expandchannel 326
expandchannel 通道关键字 319
expandlimit 326
expandlimit 通道关键字 319
expire_exclude_list 519，528
expnallow 305
expndefault 305
expndisable 305
exproute 329
EXPROUTE_FORWARD 选项 330
field 420，426
fileinto 354
filesperjob 322
filesperjob 通道关键字 319
filter 354
FILTER_DISCARD 通道 485
FILTER_JETTISON 486
folderpattern 522
foldersize 522
FORWARD 地址映射 237
forwardcheckdelete 通道关键字 311
forwardchecknone 通道关键字 311
forwardchecktag 通道关键字 311
FROM_ACCESS 映射表 457，463
gen.newuserforms 104
gen.sitelanguage 108
hashdir 536
HAStoragePlus 84
header_733 328
header_822 328
HEADER_LIMIT 350
header_uucp 328
headerlabelalign 341
headerlimit 350
headerlinelength 341
headerread 339
headerread 关键字 339
headertrim 339
HELD 邮件队列文件 700
HIDE_VERIFY 305
hold 通道 364
holdexquota 348
holdlimit 326
holdlimit 通道关键字 319
host 420，427
http
//www.cyrusoft.com/sieve 401
//www.mozilla.org/projects/security/pki/nss/tools/certutil.html 588
//www.spamassassin.org 411
HTTP 服务
MTA 设置 126
SSL 端口 115
安全性 573
代理验证 600
登录要求 116
端口号 114
访问控制过滤器 599
会话 ID 573
基于密码的登录 126
基于证书的登录 117
进程设置 126
进程数量 118
禁用 126
客户机访问控制 120
连接设置 126
每个进程的连接 118
每个进程的线程 119
配置 125
启动和停止 97
启用 126

切断空闲连接 120
性能参数 118
邮件设置 126
注销客户机 120
专用的 Web Server 125
http 日志记录，禁用 676
HTTP 邮件访问，**请参见**邮件访问
iBiff 配置参数 752
ICAP 394
选项文件 426
iddenttcpsymbolic 通道关键字 311
IDENT 查找 311
identd 596
identnone 通道关键字 312
identnonelimited 通道关键字 312
identnonenumeric 通道关键字 312
identnonesymbolic 通道关键字 312
identtcp 通道关键字 311
identtcplimited 通道关键字 312
identtcpnumeric 通道关键字 311
ignorencoding 343
iii_res* 函数
慢速 SMTP 服务器 696
IMAP 服务
readership 实用程序 537
SSL 115，578
SSL 端口 115
标题 115，123
登录要求 116
端口号 114，115
访问控制过滤器 599
共享文件夹 537
基于密码的登录 123，577
基于证书的登录 117，586
监视用户访问 556
进程设置 123
进程数量 118
禁用 123
客户机调试 558
客户机访问控制 120
连接设置 123
每个进程的连接 118
每个进程的线程 119
配置 123
启动和停止 97
启用 123
切断空闲连接 120
性能参数 118
IMAP，**请参见**
邮件访问
imesrestore 550
imexpire
部署 519
操作原理 519
imexpire，**请参见** “自动删除邮件”
immnonurgent 283，292，320
immnonurgent 通道关键字 318
immonitor-access 724
improute 329
IMPROUTE_FORWARD 330
imquotacheck 493，516，732
imqutoacheck 537
ims50 187，190
imsbackup 实用程序 547
imsched 103，519，527
imsconnutil 556
imsimta cache -view 698
imsimta crdb 479
imsimta process 686
imsimta qm 685，717
`imsimta qm` 365
imsimta qm counters 731
imsimta qm 停止和启动 688
imsimta refresh 206，220
imsimta reload 206
imsimta run 688
imsimta test -exp 487，488，489
imsimta test -rewrite 486，685，709
MTA 故障排除 684
imsimta test -rewrite -filter 486
imsimta 计数器 729

imsrestore 实用程序 547，548
imta.cnf 184，206
imta.cnf 配置文件
结构 206
IMTA_LANG 240
IMTA_MAPPING_FILE 选项 209
IMTA_QUEUE 177
IMTA_REVERSE_DATABASE 234
INBOX，默认邮箱 535
includefinal 247，251
inetCanonicalDomainName 186
inetDomainStatus 186
inner 338
innertrim 339
INTERFACE_ADDRESS 310
interfaceaddress 通道关键字 310
INTERNAL_IP 映射表 58
Internet Content Adaptation Protocol 393
interpretencoding 343
IP 地址
停止外来处理 688
IP 地址过滤 467
iPlanetDirectoryPro 131
IPv4 匹配 213
jettison 486
JOB_LIMIT 323
JOB_LIMIT 作业控制器选项 179，228
language 342
lastresort 通道关键字 313
LDAP
MTA 接口 181
LDAP 参数
Messenger Express Multiplexor 162
LDAP 错误，处理 188
LDAP 服务器故障转移 111
LDAP 目录
MTA 179
查看配置目录中的设置 109
配置目录 108
要求 108
用户目录 95，108
在用户目录中配置查找 108
自定义查找 108
LDAP 置备工具 57
LDAP_ADD_HEADER 201
LDAP_ADD_TAG 201
LDAP_ALIAS_ADDRESSES 192
LDAP_ATTR_DOMAIN1_SCHEMA2 184
LDAP_ATTR_DOMAIN2_SCHEMA2 184
LDAP_ATTR_MAXIMUM_MESSAGE_SIZE 200
LDAP_AUTH_DOMAIN 199
LDAP_AUTH_PASSWORD 200
LDAP_AUTH_POLICY 199
LDAP_AUTH_URL 200
LDAP_AUTOREPLY_TEXT 454
LDAP_CANT_DOMAIN 200
LDAP_CANT_URL 200
LDAP_CONVERSION_TAG 195，373
LDAP_DELIVERY_FILE 194
LDAP_DELIVERY_OPTION 195
LDAP_DISK_QUOTA 194
LDAP_DOMAIN_ATTR_ALIAS 183
LDAP_DOMAIN_ATTR_AUTOREPLY_TIMEOUT 187
LDAP_DOMAIN_ATTR_BASEDN 183
LDAP_DOMAIN_ATTR_BLOCKLIMIT 186，193
LDAP_DOMAIN_ATTR_CANONICAL 186
LDAP_DOMAIN_ATTR_CATCHALL_ADDRESS 186，188
LDAP_DOMAIN_ATTR_CONVERSION_TAG 186，373
LDAP_DOMAIN_ATTR_DISK_QUOTA 187
LDAP_DOMAIN_ATTR_FILTER 187
LDAP_DOMAIN_ATTR_MAIL_STATUS 186
LDAP_DOMAIN_ATTR_MESSAGE_QUOTA 187
LDAP_DOMAIN_ATTR_OPTIN 187
LDAP_domain_attr_optinX 404
LDAP_DOMAIN_ATTR_RECIPIENTCUTOFF 187，349
LDAP_DOMAIN_ATTR_RECIPIENTLIMIT 187，349

LDAP_DOMAIN_ATTR_REPORT_ADDRESS 186
LDAP_DOMAIN_ATTR_ROUTING_HOSTS 182
LDAP_DOMAIN_ATTR_SMARTHOST 186，188
LDAP_DOMAIN_ATTR_SOURCE_CONVERSION_TAG 373
LDAP_DOMAIN_ATTR_SOURCEBLOCKLIMIT 187，346
LDAP_DOMAIN_ATTR_STATUS 186
LDAP_DOMAIN_ATTR_UID_SEPARATOR 186
LDAP_DOMAIN_FILTER_SCHEMA1 183
LDAP_DOMAIN_ROOT 183
LDAP_END_DATE 198
LDAP_ERRORS_TO 201
LDAP_EXPANDABLE 201
LDAP_GROUP_DN 200
LDAP_GROUP_OBJECT_CLASSES 190
LDAP_GROUP_RFC822 200
LDAP_GROUP_URL1 200
LDAP_GROUP_URL2 200
LDAP_HOST_ALIAS_LIST 182
LDAP_LOCAL_HOST 182
LDAP_MAIL_REVERSES 202
LDAP_MESSAGE_QUOTA 194
LDAP_MODERATOR_URL 200
LDAP_OPTIN 198，396
LDAP_optinX 403，404
LDAP_PERSONAL_NAME 453
LDAP_PREFIX_TEXT 201
LDAP_PRESENCE 198
LDAP_PROGRAM_INFO 194
LDAP_RECIPIENTCUTOFF 349
LDAP_RECIPIENTLIMIT 349
LDAP_REJECT_ACTION 199
LDAP_REJECT_TEXT 199
LDAP_REMOVE_HEADER 201
LDAP_REPROCESS 199
LDAP_SCHEMATAG 187
LDAP_SOURCE_CONVERSION_TAG 373
LDAP_SOURCEBLOCKLIMIT 346
LDAP_SPARE_1 194
LDAP_SPARE_2 194
LDAP_START_DATE 198
LDAP_SUFFIX_TEXT 201
LDAP_USE_ASYNC 203
LDAP_USER_OBJECT_CLASSES 190
LDAP_USER_ROOT 183
Legato 551
lib 文件 64
libspamass.so 410
linelength 345
linelimit 346
Linux，默认基本目录 33
LMTP 431
  传送功能 432
  后端存储，无 MTA 441，443
  配置 437
  配置中继 437
  协议 445
local.auto.restart 101，733
local.autorestart.timeout 103，733
local.enablelastaccess 556
local.ens.enable 100
local.hostname 182
local.http.enableuserlist 556
local.imap.enableuserlist 556
local.imta.enable 100
local.imta.hostnamealiases 182
local.imta.mailaliases 187
local.imta.schematag 187
local.ldaphost 111
local.mmp.enable 100
local.probe.service.timeout 734
local.probe.service.warningthreshold 734
local.probe.warningthreshold 734
local.queuedir 734
local.sched.enable 100
local.schedule.expire 527
local.schedule.msprobe 103，734
local.schedule.purge 527
local.schedule.taskname 103
local.service.http.proxy 163
local.service.http.proxy.port.hostname 165

local.service.pab 110
local.smsgateway.enable 100
local.snmp.enable 100
local.sso 140
local.store.checkdiskusage 715
local.store.expire.loglevel 528
local.store.notifyplugin 752
local.store.overquotastatus 512，516
local.store.quotaoverdraft 511，517，518
local.store.relinker.enabled 543
local.store.relinker.maxage 543
local.store.relinker.minsize 543
local.store.relinker.purgecycle 543
local.store.sharedfolders 505
local.store.snapshotinterval 563
local.store.snapshotpath 563
local.ugldapbasedn 110
local.ugldapbasedn configutil 183
local.ugldapbindcred 162
local.ugldapbinddn 110，162
local.ugldaphost 110，111，162
local.ugldapport 110
local.ugldapuselocal 110，111
local.watcher.enable 101，，102，733
local.webmail.cert.enable 623
local.webmail.cert.port 623
local.webmail.smime.enable 624
local.webmail.sso 141
local.webmail.sso.amcookiename 131，166
local.webmail.sso.amloglevel 131
local.webmail.sso.amnamingurl 131，166
local.webmail.sso.id 141
local.webmail.sso.prefix 141
local.webmail.sso.singlesignoff 131
localvrfy 通道关键字 305
LOG_CONNECTION 650
LOG_CONNECTION 选项 653
LOG_FILENAME 650
LOG_FILENAME 选项 653
LOG_MESSAGE_ID 650
log_message_id 690
LOG_MESSAGE_ID 选项 652
LOG_MESSAGES_SYSLOG 选项 652
LOG_NOTARY 650
LOG_PROCESS 650
LOG_PROCESS 选项 653
LOG_TRANPORTINFO 300
LOG_USERNAME 选项 653
logfile.service 676
logfile.service.loglevel 677
logging 352
logheader 352
logindn 620
loginpw 621
loopcheck 353
mail.log_current 690
MAIL_ACCESS 映射表 457，462
mailAllowedServiceAccess 634
mailAlternateAddress 187
mailAutoReplyMode 453
mailAutoReplyText 454
mailAutoReplyTextInternal 454
mailAutoReplyTimeOut 454
mailConversionTag 195
mailDeferProcessing 199
mailDeliveryOption 195，450
mailDomainCatchallAddress 186
MailDomainConversionTag 373
mailDomainConversionTag 186
mailDomainDiskQuota 511
mailDomainMsgMaxBlocks 186
mailDomainMsgQuota 511
mailDomainReportAddress 186
mailDomainSieveRuleSource 187
mailDomainStatus 186，511
maildomainstatus 517
mailEquivalentAddress 187
mailfromdnsverify 通道关键字 306
mailMessageStore 531
mailMsgMaxBlocks 193
mailMsgQuota 510

mailQuota 194，510
mailRejectText 199
mailRoutingAddress 193
mailRoutingHosts 182
mailRoutingSmartHost 186
MailSieveRuleSource 486
mailSieveRuleSource 198
mailUserStatus 511
mailuserstatus 517
make_backup_config_changes.sh 73
make_configutil_changes.sh 73
make_mboxlistdb_changes.sh 74
make_mta_config_changes.sh 73
master 320
master_command 228
master_debug 352，690
MAX_CLIENT_THREADS 300
max_client_threads 323
MAX_CONNS 442
MAX_CONNS 分发程序选项 173
MAX_HEADER_BLOCK_USE 344
MAX_HEADER_LINE_USE 344
MAX_LIFE_CONNS 442
MAX_LIFE_TIME 442
MAX_MESSAGES 作业控制器选项 180
MAX_PROCS 442
MAX_PROCS 分发程序选项
  分发程序
    MAX_PROCS 选项 173
MAX_PROCS*MAX_CONNS 695
maxblocks 344
maxheaderaddrs 341
maxheaderchars 341
maxjobs 322
maxjobs 通道关键字 179，319
maxlines 344
maxprocchars 342
maysaslserver 315
maytls 586
maytls 通道关键字 317
maytlsclient 通道关键字 317
maytlsserver 通道关键字 317
mboxutil 532
MD5 541
MDN 252
MEM. 请参见 Messenger Express Multiplexor 159
memberURL 200
messagecount 522
messagedays 522
messagesize 522
messagesizedays 522
Messaging Multiplexor
  certmap 插件 147
  DNComps 147
  FilterComps 147
  IMAP 示例 156
  POP 示例 158
  SSL，以使用 153
  vdmap 149
  存储管理员 147
  工作原理 146
  功能 145
  基于证书的验证 148
  加密 147
  配置 151，159
  配置前 151
  启动 / 停止 / 刷新 153
  设置 150
  说明 145
  拓扑示例 155
  虚拟域 148
  预验证 148
Messaging Multiplexor，请参见 MMP
Messaging Server
  工作单 49，848
  文档 33
Messenger Express 51，113
  故障排除 567
  监视用户访问 556
  调试 558
  未知 / 无效分区 568
Messenger Express Multiplexor
  dcroot 162

LDAP 参数 162
SSL 160，164
测试 164
错误消息 164
单点登录 166
登录分隔符 163
多个代理服务器设置 165
访问 Messenger Express 客户机 164
概述 159
工作原理 160
管理 164
管理产品版本 165
建立连接的步骤 161
默认域 163
配置 162
启用 163
设置 161
托管域 160
与 MMP 的相似之处 159
Messenger Express Multiplexor 概述 159
Messenger Express 邮件过滤器 63
mgmanMemberVisibility 201
mgrpAddHeader 201
mgrpAllowedBroadcaster 200
mgrpAllowedDomain 199
mgrpAuthPassword 200
mgrpBroadcasterPolicy 199
mgrpDeliverTo 200
mgrpDisallowedBroadcaster 200
mgrpDisallowedDomain 200
mgrpErrorsTo 201
mgrpModerator 199，200
mgrpMsgMaxSize 200
mgrpMsgPrefixText 201
mgrpMsgRejectAction 199
mgrpMsgSuffixText 201
mgrpRemoveHeader 201
mgrpRFC822MailMember 200
Microsoft Exchange 317
MIME
标题 366
处理 343
概述 366
邮件结构 366
MIN_CONNS 分发程序选项 173
MIN_PROCS 分发程序选项 173
MISSING_RECIPIENT_POLICY 332
missingrecipientpolicy 331
mm_debug 690
调试工具
mm_debug 687
mm_init 704
mm_init 中的错误 704
MMP 51，601
AService.cfg 文件 152
AService-def.cfg 152
ImapMMP.config 152
ImapProxyAService.cfg 文件 152
ImapProxyAService-def.cfg 152
LDAP 服务器故障转移 159
PopProxyAService.cfg 文件 152
PopProxyAService-def.cfg 152
SMTP 代理 150
SmtpProxyAService.cfg 152
SmtpProxyAService-def.cfg 152
修改现有实例 153
MMP 和 Messenger Express Multiplexor 的相似之处 159
MMP。请参见 Messaging Multiplexor。
MobileWay 812
mode 421，427
modutil 588
msexchange 317
msg_svr_base 64，495
msprobe 101，733
MTA 50，704
imta.cnf 重写规则 184
LDAP 接口 181
别名扩展 185
操作原理 181
重写规则 174，182
错误处理 184
错误消息 703
分发程序 172

服务器进程 173
概念 167
故障排除 683
命令行实用程序 233
目录信息 179
配置文件 206，220
日志记录 643，647
设置全局选项 224
数据流 181
体系结构 171
添加中继 470
通道 171，175
问题和解决方案 693
邮件队列 177
邮件流 171
中继阻止 472
MTA 错误消息 704
本地主机太长 706
别名的错误等值 705
初始化 ch_facility 时出错
编译的字符集版本不匹配 705
没有空间进入 706
发现重复的别名 705
发现重复的映射名称 705
没有等值地址 706
通道表中的重复的主机 705
通道没有正式主机名 706
无法打开别名包含文件 705
映射名称太长 705
正式主机名太长 707
MTA 队列 716
MTA 功能
MTA 故障排除
.HELD 邮件 700
imsimta qm 启动 688
imsimta qm 停止 688
imsimta test -rewrite 684
标准过程 684
常见问题
MTA 不能接收外来邮件 694
SMTP 连接超时 695
对配置文件的更改 694
服务器端规则 702
接收到的邮件已编码 701
未传送邮件 698
循环邮件 699
邮件未被排出队列 697
概述 683
检查配置 684
检查邮件队列目录 685
日志文件 687
如何从域或 IP 地址停止外来处理 688
如何手动运行通道程序 688
如何停止和启动各个通道 688，690
识别邮件故障点 692
识别邮件路径中的通道 689
示例 689
网络和 DNS 问题 709
文件拥有权 685
一般错误消息 704
mm_init 704
os_smtp_* 错误 709
版本不匹配 707
非法主机 / 域错误 709
交换空间 708
文件打开或创建错误 708
作业控制器和分发程序 686
MTA 故障排除示例 689
MTA 配置
故障排除 684
MTA 配置文件 206
MTA 示例
启动和停止通道 690
邮件故障 692
MTA 通道
启动和停止 688
MTA 映射文件 208–??
multiple 350
mustsaslserver 315
musttls 586
musttls 通道关键字 317
musttlsclient 通道关键字 317
musttlsserver 通道关键字 317
MX 记录查找 709
MX 记录支持 313

mx 通道关键字 313
myprocmail，使用 Pipe 通道 363
nameparameterlengthlimit 349
nameservers 通道关键字 313
NDAAuth-applicationID 140
netstat 718
nms41 187，190
noaddreturnpath 333
nobangoverpercent 329
nobangoverpercent 关键字 264
noblocklimit 346
nocache 通道关键字 311
nodayofweek 340
nodeferred 319，320
nodefragment 343
nodestinationfilter 354
nodropblank 332
noehlo 303
noehlo 通道关键字 303
noexproute 329
noexquota 348
nofileinto 354
nofilter 354
noheaderread 339
noheadertrim 339
noimproute 329
noinner 338
noinnertrim 339
nolinelimit 346
nologging 352
noloopcheck 353
nomailfromdnsverify 通道关键字 306
nomaster_debug 352
nomsexchange 317
nomx 通道关键字 313
nonrandommx 通道关键字 313
nonurgentbackoff 通道关键字 319，321
nonurgentblocklimit 324
nonurgentblocklimit 通道关键字 319
nonurgentnotices 246
nonurgentnotices 通道关键字 320
noreceivedfor 334
noreceivedfrom 334
noremotehost 331
noreturnpersonal 250
noreverse 235，332
normalbackoff 321
normalbackoff 通道关键字 319
normalblocklimit 324
normalblocklimit 通道关键字 319
normalnotices 246
normalnotices 通道关键字 320
norules 337
norules 通道关键字 275
nosasl 315
nosaslserver 315
nosaslswitchchannel 315
nosendetrn 303，304
nosendpost 247
noservice 326
noslave_debug 352
nosmtp 通道关键字 302
nosourcefilter 354
noswitchchannel 关键字 314
notices 246，321
notices 通道关键字 320
NOTIFICATION_LANGUAGE 映射表 240，242
notificationchannel 353
notls 通道关键字 317
notlsclient 通道关键字 317
notlsserver 通道关键字 317
novrfy 303
nowarnpost 248
nox_env_to 340
nsserversecurity 586
nsswitch.conf 文件 313
optin_user_carryover 405
OR_CLAUSES 199
ORCPT 460
ORIG_MAIL_ACCESS 映射表 457，462

ORIG_SEND_ACCESS 映射表 457，460
ORIGINAL_ADDRESS 245
os_smtp_* 错误 709
os_smtp_open 错误 709
os_smtp_read 错误 709
os_smtp_write 错误 709
parameterlengthlimit 349
PDU 779
percentonly 329
percents 328
personalinc 335
personalomit 335
personalstrip 335
pipe 通道 354，362
pk12util 588
PKCS #11
  内部模块和外部模块 580
platformwin 621
pool 322
pool 通道关键字 319
POP Before SMTP 601
POP 服务
  SSL 578
  标题 115
  登录要求 116
  端口号 114
  访问控制过滤器 599
  基于密码的登录 577
  基于证书的登录 586
  监视用户访问 556
  进程数量 118
  客户机调试 558
  客户机访问控制 120
  每个进程的连接 118
  每个进程的线程 119
  配置 121
  启动和停止 97
  切断空闲连接 120
  性能参数 118
POP，请参见
  邮件访问
PORT 310
port 421，427
PORT_ACCESS 442，466
PORT_ACCESS 映射表 457，466，467
postheadbody 248
postheadbody 通道关键字 251
postheadonly 248
postheadonly 通道关键字 251
preferredLanguage 107
Q 记录 717
RAID 技术
  用于邮件存储 529
randommx 通道关键字 313
RBL 检查 476
readership 504，537
readsigncert 621
Received: 标题中的地址 334
Received: 标题中的信封 to 标题 334
receivedfor 334
receivedfrom 334
RECIPIENT_ADDRESS 245
recipientcutoff 349
recipientlimit 349
reconstruct 563，565
  性能 566
reconstruct 命令行实用程序 537
rejectsmtplonglines 349
relinker 540，541
  操作原理 540
  命令行模式 541
  实时模式 542
remotehost 331
resource.properties 140
restricted 333
restricted 通道关键字 333
return_option.dat 245
RETURN_PERSONAL 245
returnaddress 250

returnenvelope 248，251
returnpersonal 250
reverse 332
REVERSE 映射表 234
REVERSE 映射表标志 235
REVERSE_ADDRESS_CACHE_SIZE 203
REVERSE_ENVELOPE 235
REVERSE_URL 201，204
revocationunknown 621
RFC 2476 354
RFC 3507 393
rfc822MailMember 201
ROUTE_TO_ROUTING_HOST 182
routelocal 330
rules 337
S/MIME 605
  Apple 610
  LDAP 密码对 616
  LDAP 目录 615
  LDAP 目录中的公共密钥 609
  LDAP 证书 617
  smime.conf 文件 617
  SSL 624
  多语言支持 609
  概念前提 606
  基本配置 611
  开始使用 610
  密钥对 609
  所需软件 / 硬件 607
  通用访问卡 608
  下载 applet 611
  选项 623
  已定义的 606
  用户权限 609
  智能卡 608
  专用和公共密钥 608
SASL
  说明 573
  通道关键字 315
sasl.default.auto_transition 574，576
sasl.default.ldap 576
sasl.default.ldap.has_plain_passwords 574
sasl.default.ldap.searchfilter 575
sasl.default.ldap.searchfordomain 575
sasl.default.mech_list 575，577
sasl.default.transition_criteria 574
saslswitchchannel 313，315
SASVE
  部署 424
  配置示例 424
SAVSE
  部署 423，424
  概述 423
  选项 426
  要求和使用注意事项 423
sbin 文件 64
seen 522
SEND_ACCESS 映射表 457，460
sendencryptcert 621
sendencryptcertrevoked 621
sendetrn 303，304
sendmail
  客户端 60
sendpost 247
sendsigncert 622
sendsigncertrevoked 622
sensitivitycompanyconfidential 342
sensitivitynormal 342
sensitivitypersonal 342
sensitivityprivate 342
SEPARATE_CONNECTION_LOG 选项 653
service 326
service.{imap|pop|http}.plaintextmincipher 575
service.dcroot 162
service.defaultdomain 163，186
service.http 127
service.http.enable 100，676
service.http.enablesslport 127，676
service.http.idletimeout 128
service.http.maxmessagesize 128
service.http.maxsessions 128
service.http.maxthreads 128
service.http.numprocesses 128

service.http.plaintextmincipher 124，127
service.http.port 127
service.http.sessiontimeout 128
service.http.smtphost 128
service.http.smtpport 128
service.http.spooldir 128
service.http.sslport 127
service.imap 124
service.imap.allowanonymouslogin 574
service.imap.banner 116，124
service.imap.enable 100
service.imap.enablesslport 124
service.imap.idletimeout 124
service.imap.maxthreads 124
service.imap.numprocesses 124
service.imap.port 124
service.imap.sslport 124
service.loginseparator 116，163
service.pop 122
service.pop.banner 116，122
service.pop.enable 100，122
service.pop.enablesslport 122
service.pop.idletimeout 122
service.pop.maxsessions 122
service.pop.maxthreads 122
service.pop.numprocesses 122
service.pop.sslport 122
service.readtimeout 734
sevenbit 通道关键字 307
Sieve 486
Sieve 过滤语言 481
Sieve 另请参见
  过滤器，用户级别
silentetrn 303
silentetrn 通道关键字 304
sims40 190
sims401 187
single 314，350
single 通道关键字 315
single_sys 225，314，350
single_sys 通道关键字 315
slapd 719
slapd 问题 719
slave 320
SLAVE_COMMAND 选项 231
SLAVE_COMMAND 作业控制器选项 228
slave_debug 352，690
SMIME
  Communications Express S/MIME 最终用户信息 639
  CRL 访问 629
  CRL 访问问题 633
  CRL 检查 629
  CRL 检查和代理服务器 631
  LDAP 中的 CA 证书 635
  LDAP 中的公共密钥和证书 636
  查找用户的专用或公共密钥 628
  登录，首次 640
  管理证书 635
  过时 CRL 631
  启用 Java 控制台 642
  签名和加密设置 641
  权限 634
  网络安全服务 (NSS) 639
  验证 LDAP 中的密钥或证书 637
  验证专用密钥和公共密钥 628
  邮件发送时间 632
  证书撤销 633
SMPP V3.4 779
SMS 771
  SMS 选项 798
  本地化选项 806
  传送重试 812
  地址有效性检查 782
  电子邮件转换选项 794
  格式化模板 809
  将电子邮件转换成 SMS 775
  配置 788
  添加更多的通道 811
  调试 813
  通道定义和重写规则 789
  通道选项 791

通道选项文件 790
站点定义的文本转换 783
SMS 通道 771
attributes 774
操作 774
要求 773
SMS 通道，配置样例 812
SMS 通道，添加 788
SMS_Channel_TEXT 映射表 783
SMTP AUTH 470
SMTP MAIL TO 命令 305
SMTP 错误
os_smtp_* 错误 709
SMTP 代理 587，602
MMP 150
SMTP 服务
登录要求 578
端口号 578
访问控制 455
基于密码的登录 578
经过验证的 SMTP 578
启动和停止 97
添加中继 470
中继阻止 472
SMTP 服务器性能降低 696
SMTP 连接 695，717
SMTP 命令和协议支持 300
SMTP 通道 299
smtp 通道关键字 302
SMTP 通道线程 325
SMTP 通道选项文件 602
SMTP 验证 601
SMTP 中继 431
添加 470
SMTP 阻止
安装后的配置 58
smtp_client 进程 434
smtp_cr 通道关键字 302
smtp_crlf 通道关键字 302
smtp_crorlf 通道关键字 302
smtp_lf 通道关键字 302
SNMP 737
applTable 741
applTable 的用法 743
assocTable 743
assocTable 的用法 744
MTA 信息 744
mtaGroupAssociationTable 746
mtaGroupErrorTable 748
mtaGroupErrorTable 的用法 748
mtaGroupTable 745
mtaGroupTable 的用法 746
mtaTable 744
mtaTable 的用法 744
操作 739
服务器信息 741
实现 738
提供的信息 741
通道错误 748
通道网络连接 746
通道信息 745
网络连接信息 743
为 Messaging Server 配置 739
限制 738
与其他 iPlanet 产品共存 741
支持 MIB 738
SOCKS_HOST 427
SOCKS_PASSWORD 427
SOCKS_PORT 427
SOCKS_USERNAME 427
Solaris
修补程序 35
支持 35
sourceblocklimit 346
sourcecommentinc 334
sourcecommentmap 334
sourcecommentomit 334
sourcecommentstrip 334
sourcecommenttota 334
sourcefilter 354，483
sourcenosolicit 358
sourcepersonalinc 335
sourcepersonalmap 335

sourcepersonalomit 335
sourcepersonalstrip 335
sourceroute 328
sourcespamfilterXoptin 355，400
spamadjust 428
SpamAssassin 410
  mode 422
  verdict 410
  部署 412
  操作原理 410
  定位服务器 411
  分数 410
  归档垃圾邮件 413
  结果 410
  示例 412
  选项 (spamassassin.opt) 420
  要求和性能 411
spamd 410
spamfilterX_action_n 404
SpamfilterX_config_file 403
spamfilterX_final 404
SpamfilterX_library 403
SpamfilterX_null_action 404
SpamfilterX_null_optin 404
SpamfilterX_optional 403
SpamfilterX_string_action 404
spamfilterX_verdict_n 404，414
spamtest 428
SSL
  Messenger Express Multiplexor 160，164
  POP 基于 122
  安装 CA 证书 581
  安装服务器证书 581
  概述 578
  管理证书 582
  加密算法 585
  密码文件用于 582
  内部模块和外部模块 580
  启用 584
  请求服务器证书 581
  硬件加密加速器 580
  优化性能 587
  证书 580
sslpassword.conf 文件 582
sslrootcacertsurl 622
ssltap 588
SSO 129
  Cookie 133
  Messenger Express Multiplexor 166
  Messenger Express 配置参数 130
  错误诊断 132
  配置 130
  限制 130
  信任范围 132，134
SSR 702
  语法问题 703
start-msg 99，100
stop-msg 99
store.admins 497
store.cleanupage 527
store.defaultmailboxquota 511，513
store.defaultmessagequota 511
store.defaultpartition 532
store.expirerule 520
store.quotaenforcement 511，516
store.quotaexceededmsg 511，514
store.quotaexceededmsginterval 511，515
store.quotagraceperiod 511
store.quotanotification 511，514
store.quotawarn 511，515
store_root 495
stored 721
stored 操作 559
stored 进程
  邮件存储故障排除 559
streaming 通道关键字 307
subaddressexact 336
subaddressrelaxed 336
subaddresswild 336
subdirs 351
  如何使用 691
subdirs 通道关键字 351
submit 通道关键字 354

Sun Cluster 77
Sun ONE Console 96
sunManagedOrganization 184
SunPreferredDomain 186
sunPreferredDomain 184
suppressfinal 247，251
switchchannel 331，473
switchchannel 通道关键字 314
Symantec Anti-Virus Scanning Engine，请参见 *SASVE*
TCP 客户机访问控制
  EXCEPT 运算符 595
  identd 服务 596
  Netscape Console 界面 599
  地址欺骗检测 598
  访问过滤器工作原理 592
  概述 591
  过滤器语法 592
  示例 597
  通配符名称 594
  通配符模式 595
  虚拟域 598
  用户名查找 596
  主机规范 596
TCP/IP
  IDENT 查找 311
  MX 记录支持 312，313
  端口号 310
  反向 DNS 查找 311
  接口地址 310
  连接 308
  通道 222，300
TCP/IP 名称服务器查找 313
TCP/IP 通道 299
tcp_lmtp 通道 436
tcp_lmtpnative 通道 436
tcp_smtp_server 进程 433
TEXT_CHARSET 246
threaddepth 325
threaddepth 通道关键字 319
throttle 467
timestampdelta 622
TLS 122，317
  说明 578
  通道关键字 317
tls 通道关键字 586
TLS 问题 694
tlsswitchchannel 关键字 317
transactionlimit 324
truncatesmtplonglines 349
trustedurl 623
uniqueMember 200
UNIX 传送 758
UNIX 系统用户和组 38
unrestricted 333
unrestricted 通道关键字 333
UpgradeMsg5toMsg6.pl 68，70
urgentbackoff 321
urgentbackoff 通道关键字 319
urgentblocklimit 324
urgentblocklimit 通道关键字 319
urgentnotices 246
urgentnotices 通道关键字 320
USE_CHECK 421
USE_DOMAIN_DATABASE 204
USE_FORWARD_DATABASE 238，239，240
USE_REVERSE_DATABASE 201，204，235，236，239
USE_TEXT_DATABASES 437
use_text_databases 219
useconfig 实用程序 78
useintermediate 251
usercertfilter 623
uucp 328
UUCP 地址重写规则 259
VACATION_CLEANUP 452
VACATION_TEMPLATE 451，452
vacationEndDate 453
vacationStartDate 453
vdmap (Messaging Multiplexor) 149
verdict 421，427

VerifySSO 140
verifyurl 140
Veritas Cluster Server 77，79
  3.5 版 80
  配置 80
viaaliasoptional 337
viaaliasrequired 337
VRFY 命令 304
VRFY 命令支持 304
vrfyallow 通道关键字 305
vrfydefault 通道关键字 305
vrfyhide 通道关键字 305
warnpost 248
watcher 101，733
webmail
  HTTP 服务 125
  Messenger Express 113
wrapsmtplonglines 349
x_env_to 340
X-Envelope-to
  标题行
    生成 340
X-REWRITE-SMS-ADDRESS 映射表 783
<(小于号)
  包含文件 208
<nopage>MEM。请参见 Messenger Express Multiplexor 160
“成员”选项卡 761
“邮件”选项卡 754，762
（日志记录的）冗长度 669
（日志记录的）严重级别 669

A

安排任务时间 103
安全 / 通用 Internet 邮件扩展服务，**请参见** *S/MIME*
安全性
  HTTP 服务 120，573
  IMAP 服务 120
  POP 服务 120
  S/MIME，**请参见** *S/MIME*
  SASL 573
  SMTP 服务 578
  SSL 578
  TLS 578
  关于 572
  基于密码的登录 117
  基于证书的登录 117，586
  客户机对 TCP 服务的访问 591
  客户机访问控制 121
  验证机制 573
安装 Messaging Server 和 Directory Server 拷贝 54
安装程序
  无提示 53
安装后的端口号 65
安装后的目录布局 64
安装后的配置
  端口号 65
  配置
    SMTP 阻止 58
  通过重引导启动 60
安装文件 65

B

八位数据 307
百分比符号 (%) 275，277
百分比黑客 263
百分比黑客规则 259
版本不匹配 707
包含文件 65
备份组 545
备用电子邮件地址 755，763
备用转换通道 355
本地化，通知邮件

本地通道
选项 364
本地邮件传输协议，请参见 LMTP
本地主机太长
MTA 错误消息 706
编码 345
编码标题 340
编译，MTA 配置 206
编译的配置版本不匹配 707
标记的重写规则集 260
标题
IMAP 115
language 342
POP 115
Return-path 333
X-Envelope-to 340
处理关键字 338
分割长行 341
删除 339
删除非法的空收件人 332
最大长度 342
标题，定义 366
标题对齐 341
标题剪裁 339
标题选项文件 339
标准过程
MTA 故障排除 684
别名 231
别名数据库 232
别名文件 221，232
在别名文件中包含其他文件 233
别名的错误等值
MTA 错误消息 705
别名扩展 185
别名数据库 336
别名文件 239，336
病毒过滤 393
病毒扫描 365
不传送报告，请参见通知邮件
不可识别的
域说明 278
主机规范 278
部分邮件 343

C

擦除 496
擦除邮件 496
测试安装
Messenger Express Multiplexor 164
产品版本
Messenger Express Multiplexor 165
常规数据库 219，272，478，479
长时间服务故障 248
程序
从 226
主 226
程序，将邮件发送到 365
程序传送
pipe 通道 362
设置 362
指定 757
冲突
重复的百分比符号 264
重写
内部标题 333
重写错误消息 277
重写地址
提取第一个主机 / 域说明 263
重写规则 182，207
bang 式样 259
UUCP 地址 259
百分比黑客 259
标记的规则集 260
操作 262
测试 278
处理大量 278
检查 337
结构 256

空白行 177，207
控制序列 267
模板 260，265
模板替换 267
模板中的大小写区分 262
模式和标记 257
模式匹配 262
普通模板 A%B@C 261
扫描 264
失败 266
示例 279
说明 174
特定于方向 276
特定于位置 276
特定于主机位置 276
替换，LDAP 查询 URL 271
替换，常规数据库 272
替换，单个字段 274
替换，文字字符 271
替换，用户名和子地址 270
替换，用户提供的例程 273
替换，指定的映射 273
替换，主机 / 域和 IP 文字 270
完成重写进程 266
与任何地址匹配 260
域文字 266
指定的路由模板 A@B@C 261
重复的模板 A%B 261
重写后的语法检查 266
重写规则的失败 266
重写后的语法检查 266
重写进程失败 262
重新编译，MTA 206，220
重新装入 206
端口号 65
初始化 ch_facility 时出错
编译的字符集版本不匹配 705
没有空间进入 706
初始运行时配置 49
无提示 53
处理邮件 365
传输层安全性 (TLS) 578
传送报告，**请参见**通知邮件
传送失败 321，717
传送选项
POP/IMAP 传送 757
UNIX 传送 758
程序传送 757
邮件用户 756
传送重试频率 321
传送状态通知，**请参见**通知邮件 240
垂直条 (\|) 260
磁盘空间 713
监视 538
减少 539
配额用于 509
磁盘使用量 733
从
地址 329
从 5.2 升级 67
从程序 226，320
从域或 IP 地址停止外来处理 688
错误通知邮件，本地
错误消息
Messenger Express Multiplexor 164
MTA 704
本地主机太长 706
别名的错误等值 705
发现重复的别名 705
发现重复的映射名称 705
没有等值地址 706
通道表中的重复的主机 705
通道没有正式主机名 706
映射名称太长 705
正式主机名太长 707
初始化 ch_facility 时出错 705，706
无法打开别名包含文件 705

D

大型邮件的自动分段 344
单点登录
  Messenger Express 配置参数 140
单点登录，请参见 SSO 129
登录
  基于密码的 577
  基于证书的 117，586
登录分隔符
  Messenger Express Multiplexor 163
登录分隔符，用于 POP 116
登录服务
  基于密码的登录 117
地址
  ! 和 % 的用法 329
  envelope To: 275
  不完整 331
  重写 330
  处理 327
  从
    329
  多个目标 350
  后指 330
  解释 329
  空的信封返回 248
  路由信息 329
  目标 350
  无效 248
地址反向 201
地址反向，特定于通道 237
地址反向控制 235
地址反向数据库 234
地址更改 234
地址映射，FORWARD 237
地址邮件标题
  个人名称 335
  注释 334
地址邮件标题中的个人名称 335
地址中的路由信息 329
地址重写 330
定期邮件返回作业 249
端口号 65
端口通道关键字 310
短消息服务，已定义的 771
堆大小 668
队列 716
队列，邮件 177
多个 $M 子句 275
多个代理服务器
  Messenger Express Multiplexor 165
多个地址 350
多个地址扩展 326
多个目标地址 350
多个外发通道 314
多路复用器。请参见 Messaging Multiplexor。

F

发布和订阅 749
发现重复的别名
  MTA 错误消息 705
发现重复的映射名称
  MTA 错误消息 705
反病毒 393，405，422
  扫描程序 355
反垃圾邮件 347，393，422，455
  Brightmail，请参见 Brightmail
  Sieve 401
  SpamAssassin，请参见
    SpamAssassin
  部署第三方软件 394
  操作 401
  操作原理 394
  多个程序 395
  客户机库 395
  库路径 395
  垃圾邮件分数 393，422
  扫描程序 355
  通道级别的过滤 399，400
  限制收件人 349

要过滤的邮件 396
用户级别的过滤 396
域级别的过滤 398
反向高速缓存 192
反向数据库 234
特定于通道 332
反向通道关键字 236
反向映射 234，236
返回的邮件
内容 248
访问 Messenger Express 客户机
Messenger Express Multiplexor 164
访问控制
HTTP 服务 120，591
IMAP 服务 120，591
POP 服务 120，591
SMTP 服务 456
测试映射 469
创建访问过滤器 599
对 TCP 服务的访问，概述 591
过滤器语法 592
监视用户 556
客户机访问 120
应用后 468
映射表 456
邮件存储 497
访问控制，**另请参见**映射表
非 ASCII 字符 703
非标准邮件格式
转换 343
非法主机 / 域错误 709
MX 记录查找 709
分段
长邮件 344
分发程序
MAX_CONNS 选项 173
MIN_CONNS 选项 173
MIN_PROCS 选项 173
重新启动 174
故障排除 695
控制 173
配置文件 222
启动 173
说明 172
调试和日志文件 667
停止 174
分发程序配置文件 222，667
分隔符，设置 116
分区
RAID 技术 529
路径名 530
满 531
默认 530
添加 530
为邮件存储配置 529
移动邮箱于 531
邮件存储 517
主 529
昵称 530
分区，无效 568
服务
HTTP 113
IMAP 113
MTA 167，205
POP 113
SMTP 167，205
启动和停止 97
启用和禁用 114
服务标题 115
服务器端规则 482
不生效 702
故障排除 702
服务器响应时间。 733
服务器证书
安装 581
管理 582
请求 581
服务转换 326
复制的 54
附件 343
打开 375

G

感叹号 (\!) 264
高可用性
  Sun Cluster 84
  Sun Cluster 的必要条件 83
  useconfig 78
  绑定 IP 地址 88
  附加配置说明 88
  取消配置 90
  群集代理 78
  自动重新启动 102
更改您的配置 694
更新
  配置 68
工作单 843
  Administration Server 846
  comm_dssetup.pl 40，847
  Directory Server 844
  Messaging Server 49，848
共享文件夹 499
  ACL 504
  访问控制权限 504
  分布式 500，505
  公用文件夹 503
  监视和维护数据 507
  启用或禁用 505
共享文件夹，IMAP 537
孤立帐户 536
故障排除
  登录失败，POP 116
  通配符和命令 567
  邮件存储 567
关键字
  表 282，285
管理
  Messenger Express Multiplexor 164
管理拓扑 108
管理员访问控制
  对服务器的整体 590
  对服务器任务 590
  对邮件存储 497
  配置 589
规则通道关键字 275
过滤器 455，482
  IP 地址 467
  Messenger Express 63
  MTA 范围内 482，485
  Sieve 198
  Sieve 扩展 428
  基于用户 482
  调试用户级别 486
  通道级别 482
过滤器，**另请参见**
  邮件过滤
过期

H

后指地址 330
恢复，使用 Legato Networker 554
恢复任务
  reconstruct 实用程序 537
  邮箱 563
恢复邮件存储 543
恢复邮件存储，注意事项 549
恢复增量备份 550

J

基于 SSL 的 POP 122
基于 SSL 的目录查找 604
基于各个通道的大小限制 344
基于证书的登录 117，586
加密
  加速器用于 580
加密设置 111
加密算法
  关于 585
监视 711
  CPU 使用率 716

httpd 720
imapd 720
LDAP 服务器 724
LDAP 目录服务器 719
mboxlist 目录 723
msprobe 712，733
MTA 716
POP 和 IMAP 服务器 724
popd 720
SMTP 连接 717
stored 721，724
watcher 711，733
Webmail 服务 720
传送失败率 717
传送时间 713
磁盘空间 713
分发程序 718
工具和实用程序 723
日志文件 712
数据库日志文件 723
系统性能 713
用户访问 556
邮寄主管邮件 712
邮件存储 722
邮件存储数据库锁定 722
邮件队列 716
邮件访问 719
自动重新启动 101
作业控制器 718
剪裁邮件标题行 340
建立与 Messenger Express Multiplexor 的连接 161
降低行的长度 345
交互模式 41
交换空间
错误 708
命令 708
接收到的邮件
已编码 701
解释地址 329
仅电子邮件成员（组的） 761
进程
数量 118
警报属性
磁盘空间 538
拒绝服务攻击 717

K

可选标志 50
空白行
在一个配置文件中 207
空的信封地址 248，251
空的信封返回地址 248
空闲连接，切断 120
控制与重写相关联的错误消息 277

L

垃圾电子邮件
删除
垃圾邮件，**请参见**
反垃圾邮件，*Brightmail*，*SpamAssassin*
垃圾邮件，**请参见**反垃圾邮件
垃圾邮件过滤器 482
垃圾邮件过滤器选项 403
连接，同时的 790
连接缓存 310
链接计数 540
两位数年份 340
两位数日期 340
路由
显式 329，330
隐式 330
路由地址 193

M

麻烦的错误消息 277
没有等值地址
  MTA 错误消息 706
每个进程的线程 119
每个邮件副本一个目标系统 350
密码 94
密码登录 577
密码文件 （用于 SSL） 582
密码验证
  另请参见登录
  HTTP 服务 117
  IMAP 服务 117
  POP 服务 117
  SMTP 服务 578
  向 LDAP 用户目录 110
名称服务器查找 313
命令行实用程序
  mboxutil 532
  MTA 233
  reconstruct 537
  stored 538
默认 datasize 668
默认错误消息
  重写和通道匹配失败 277
默认通道 298
  在一个配置文件中 178，207
默认域
  Messenger Express Multiplexor 163
目标地址 350
目录 179
  对于日志文件 671
  邮件存储 493
目录布局 64

N

内部标题
  重写 333
内部标题重写 333
内部模块 (PKCS #11) 580

P

配额
  attributes 510
  configutil 参数 511
  Netscape Messaging Server 518
  磁盘 509
  磁盘空间 509
  禁用 516
  警告 513
  警告邮件 514
  宽限期 517
  默认 512
  默认值 510
  配置 509
  启用强制 516
  强制 509，516
  使用情况 537
  通知 509，513，516
  系列组 516
  用户 509，513
  邮件 509
  域 510，513，516
  阈值，设置 515
配额检查报告 732
配置
  Veritas Cluster Server 80
  初始运行时 49
  端口号 65
  高可用性 84
  可选标志 50
  密码 94
  组件 50
配置 SMTP 阻止 58
配置目录 108，109
配置文件 64，519，528
  dispatcher.cnf 667
  imta.cnf
    结构 206
  MTA 206
  nsswitch.conf 313
  sslpassword.conf 582
  别名 221

分发程序 222
空行 207
调整 224
选项 224
映射 223
转换 222
作业控制器 225
批量邮件 548
匹配过程，重写规则 265

Q

启动 / 停止
HA 服务器 97，100，101
非 HA 服务器 98
服务器自动重新启动 101
启动 / 停止服务器 97
启动各个通道 688
启用 Messenger Express Multiplexor 163
迁移
邮件存储大小 540
邮箱 74
迁移用户 364
清除 496
请参见通知邮件
取消配置高可用性 90
全限定域名 (FQDN) 263
群集代理 78

R

日期
两位数 340
日期规范
星期几 340
日期转换 340
日期字段 340
日志记录 643
LOG_CONNECTION 选项 653
LOG_FILENAME 选项 653
LOG_MESSAGE_ID 选项 652
LOG_MESSAGES_SYSLOG 选项 652
LOG_PROCESS 选项 653
LOG_USERNAME 选项 653
MTA 647，651
MTA 示例 653
MTA 条目代码 649
MTA 邮件和连接 647
SEPARATE_CONNECTION_LOG 选项 653
查看日志 674
分析日志 647
管理服务日志 669
管理工具 647
级别 669
类别 670
类型 644
启用 MTA 651
日志文件的目录 671
体系结构 673
通道 647
文件 644
文件格式 671
选项 672，674
严重级别 669
邮件存储 681
邮件存储和管理服务器 669
日志文件 64
MTA 故障排除 687
邮件存储故障排除 558
如何手动运行通道程序 688

S

删除 Received
  标题行 700
删除用户 95
删除邮件 496
删除域 96
生成字符集标记 306
生存期策略
  邮件存储 518
  邮件的数量 518
  邮箱的大小 518
  指定 518
生存期策略，**请参见** “自动删除邮件”
升级 67
  迁移邮箱 74
失败的传送尝试 248
失败的邮件 248
识别邮件路径中的通道
  如何 689
使用本地 sendmail 配置文件 60
示例文件 65
事件通知服务 749
事件通知服务，**请参见** ENS
手动运行通道程序 688
首选语言，域 107
授权服务 760
数据库
  常规 219
数据库，通用 479
数据库日志文件
  邮件存储故障排除 560
数据文件 64
四位数日期 340

T

特定于方向的重写 276
特定于位置的重写 276
特定于源通道
  重写 275
特定于主机位置的重写 276
特殊指令 377
替换，重写规则
  唯一字符串 274
调试 352，420，426
  分发程序 667
调试工具
  channel_master.log-* 文件 692
  imsimta cache -view 698
  imsimta process 686
  imsimta qm 685，717
  imsimta qm 启动和停止 688
  imsimta run 688
  imsimta test -rewrite 685，709
  log_message_id 690
  mail.log_current 690
  mail.log_current 记录 692
  master_debug 690
  slave_debug 690
  subdirs 691
  TCP/IP 网络
    PING、 TRACEROUTE 和 NSLOOKUP 697
  tcp_local_slave.log-* 文件 692
  映射表 688
  邮件文件 692
调整文件 224
停止 / 启动服务器 97
停止各个通道 688
通道
  IDENT 查找 311
  SASL 支持 315
  SMTP 选项文件 222
  SMTP 验证 315
  TCP/IP MX 记录支持 313
  TCP/IP 端口选定 310
  TLS 关键字 317
  八位数据 307

备用 314
从程序 175
定义 177
定义中的注释行 177
反向 DNS 查找 311
方向性 320
关键字 301
结构 177
解释名称 275
仅用来提交 354
连接缓存 310
名称服务器查找 313
默认，设置 298
目标主机选择 314
配置 281，361
说明 171，175
特定于通道的规则检查 275
协议流 307
协议选定和行终止符 302
邮件队列 177
预定义的 361
主程序 175
字符集标记 306
作业处理池 322
通道 l 207
通道 / 主机表 178
通道表中的重复的主机
MTA 错误消息 705
通道程序
故障排除 688
通道处理
同时进行的请求 225
通道块 178
通道没有正式主机名
MTA 错误消息 706
通道协议选定 302
通道主机表 207
通过重引导启动 60
通配符 567
通配符，映射中 212
通配符字段替换 215
通知
请参见通知邮件
通知邮件 –246，247，250
从标题中删除非美国 ASCII 字符 246
对邮寄主管发送 / 阻塞 247
附加功能 246
构造和修改 241
国际化 245
为无法传送的邮件设置传送间隔 246
自定义和本地化 242
阻塞内容返回 246
通知邮件的不正确处理
循环邮件 700
通知邮件中的已变更地址 247
同时连接，控制 790
托管域
Messenger Express Multiplexor 160

W

外部模块 (PKCS #11) 580
外来连接 314
外来邮件 694
外来邮件的备用通道 313
网络安全服务 587
网络服务 226
网络问题 717
为 Messaging Server 准备 LDAP Directory 39
为外部站点进行 SMTP 中继，允许在 NMS 中 471
委派的管理 95，589
未传送的邮件 321
未传送邮件 698
未经授权的批量电子邮件 476
位标志 248，251
文档
Communications Services 文档的位置 34
Messaging Server 文档的位置 33
概述 33
文件

包含在配置文件中 208
标题选项 339
文件布局 64
文件打开或创建错误 708
文件拥有权
故障排除 685
问候邮件 104
基于域 105
无法打开别名包含文件
MTA 错误消息 705
无提示安装 53
无提示模式 47
无效地址 248

X

显式路由 329，330
显式路由，禁用 330
限制
行长度 345
限制的邮箱编码 333
相应的通道特性 314
小于号 (<) 208
协议流 307
卸载
高可用性 90
信任的应用程序 132
信任范围 132
星号 703
星号，地址 172
星期几
日期规范 340
行长度限制 345
性能，中继 431
性能参数
进程数量 118
每个进程的连接 118
每个进程的线程 119
性能和调节 63
性能增强
LMTP 431
休假模式 759
休假邮件 449
修改密码 94
修正不完整的地址 331
虚名域 183，204
虚拟域
控制访问 598
选项
SLAVE_COMMAND 231
选项文件 224
循环邮件 699，700
通知邮件的不正确处理 700
邮寄主管地址损坏 700
寻址信息
备用地址 755，763
邮递列表 762
邮件用户 755
主地址 755，763
转发地址 758

Y

延迟传送日期 331
延迟邮件处理 320
验证
HTTP 116
IMAP 116
Messaging Multiplexor 147
password 577
POP 116
SASL 573
SMTP 578
基于证书的 573，578
机制 573
遥测 558
要求
comm_dssetup.pl 40

Sun Cluster 83
一般 MTA 错误消息 704
移动用户邮箱 543
移动邮箱 531
已编码的接收到的邮件 701
已编码邮件 701
已放弃的邮件 485
保存 485
已验证的地址 316
隐式路由 330
应用程序 ID 133
硬件空间
邮件存储故障排除 558
映射
/ 匹配 213
映射表 209，688
COMMENT_STRINGS 334
FROM_ACCESS 457
MAIL_ACCESS 457
NOTIFICATION_LANGUAGE 240
ORIG_MAIL_ACCESS 457
ORIG_SEND_ACCESS 457
PORT_ACCESS 457，467
SEND_ACCESS 457
SMS_Channel_TEXT 783
X-REWRITE-SMS-ADDRESS 783
处理大量的条目 478
列出全部 209
说明 456
映射表，**另请参见**访问控制
映射操作 211
映射名称太长
MTA 错误消息 705
映射模板替换和元字符 214
映射模板中的元字符 214
映射模式通配符 212
映射探测 216
映射条目模板 214
映射条目模式 211
映射文件 208–??，223
查找和装入 209
文件格式 210
用户
访问监视 556
删除 95
用户，创建 95
用户登录 . 请参见登录
用户管理实用程序，**请参见** *Delegated Administrator*
用户和组
UNIX 系统 38
用户目录 108
用户文件夹
邮件存储故障排除 560
用户邮箱
迁移 74
用户邮箱目录问题
邮件存储故障排除 568
用引号引起的本地部分 333
用于转换处理的通信 367
邮递列表
“成员”选项卡 （组的） 761
“邮件”选项卡 762
LDAP 搜索 URL 765
Netscape Console 访问 761
创建新组 761
地址 （主） 763
动态成员资格条件 765
访问现有组 762
仅电子邮件成员 761
列表成员 765
列表拥有者 764
添加列表 （仅电子邮件）成员 766
邮件拒绝操作 768
邮件邮寄的限制 767
中介人 768
主机名隐藏 764
邮递列表，创建 95
邮寄主管
地址 250
邮件
出队 330
大小限制 345

分段 346
清除
缺少收件人标题 331
删除 496
自动删除
邮件标题
日期字段 340
邮件标题行
剪裁 340
邮件处理通知 252，449
邮件处理通知，自定义 / 本地化 252
邮件处理通知**另请参见**
通知
邮件传输代理。另请参见 MTA
邮件存储 50
imsbackup 实用程序 547
imsrestore 实用程序 548
mboxlist 数据库日志文件 733
RAID 技术 529
reconstruct 实用程序 563
stored 实用程序 538
备份，排除垃圾箱 548
备份策略 544
备份组 545
擦除邮件 496
常见问题和解决方案 567
重建邮箱 565
磁盘空间减少 539
访问控制 497
分区 517，529
分区，更改默认 531
概述 492
故障排除 557
管理员访问权限 497
恢复数据 548
检查并修复邮箱 566
宽限期 517
命令行实用程序 492
默认分区 530
目录布局 493
配额（请参见“配额”） 512
配置磁盘配额 509
配置分区 529
清除邮件 496
日志记录 643，669
日志记录示例 681
删除孤立帐户 536
删除邮件 496
生存期策略 518
使用 Legato Networker 进行备份 551
使用第三方软件 554
维护和恢复过程 532
邮件跟踪 678
增量备份 547
主分区 529
自动删除邮件
邮件存储的备份过程
备份实用程序 547
并行备份 545
串行备份 545
创建备份组 545
创建策略 544
单个复制过程 544
高峰业务负载 545
使用 Legato Networker 551
使用第三方软件 554
说明 543
完全备份 545
增量备份 545
邮件存储故障排除 557，558
stored 操作 559
stored 进程 559
常见问题和解决方案
用户邮箱目录问题 568
监视 558
数据库日志文件 560
硬件空间 558
用户文件夹 560
主存文件 560
邮件的片段整理 343
邮件队列 177，716
邮件队列，监视 717
邮件队列目录
故障排除 685

邮件访问 113
HTTP
HTTP 服务 113
IMAP
POP
POP，IMAP 或 HTTP 114
不使用域名登录 116
登录要求 116
端口，加密 115
服务端口号 114
基于密码的 117
一般配置 114
邮件故障 692
邮件过滤
MTA 范围内的过滤器 482
服务器端规则 482
基于用户的过滤器 482
说明 455
通道级别的过滤器 482
映射表 456
邮件截止期 518
邮件拒绝 346
邮件片段整理 343
邮件未被排出队列 697
邮件用户
“邮件”选项卡 754
Netscape Console 访问 753
POP/IMAP 传送选项 757
UNIX 传送选项 758
备用地址 755
程序传送选项 757
传送选项配置 756
创建新用户 754
地址，指定 755
地址（主） 755
访问现有用户 754
休假模式 759
主机名隐藏 755
转发地址 758
自动回复设置 759
邮件转发 313
邮件转换标记 373
邮箱
INBOX 535
mboxutil 实用程序 532
reconstruct 实用程序 563
重建 563
管理 532
命名约定，用于 535
修复 563
用于传送的默认邮箱 535
自动删除邮件 518
邮箱编码
restricted 333
与任何地址匹配 260
语法问题
SSR 703
语言
服务器站点 107
用户首选 107
站点 107
域
地址中的说明 262
删除 96
数据库 278
文字 266
域首选语言 107
预验证 (Messaging Multiplexor) 148
原始收件人 460
源路由 337
源路由的地址 263
源文件
包含 208
远程系统 314
运行时配置 49

Z

在映射模板中替换 214
站点语言 107
正式主机名太长
  MTA 错误消息 707
正向数据库 237
证书 588
  安装，服务器 581
  安装，信任的 CA 581
  管理 582
  获得 580
  请求，服务器 581
支持
  Solaris 35
直接 LDAP，另请参见 MTA 181
直接 LDAP，设置 204
指定的邮箱 333
置备 55
置备选项
  LDAP 置备工具 57
智能卡 608
中继阻止 472
中继阻止，删除 470
中介人
  定义 768
  邮递列表 768
主程序 226，320
主存文件
  邮件存储故障排除 560
主电子邮件地址 755，763
主动提供的批量电子邮件，请参见反垃圾邮件
主机 / 域说明 263
主机名
  提取 263
  隐藏 755，764
注释
  地址邮件标题中 334
转发
  添加 470
转发地址 758
转发邮件 717
转换标记 373
转换地址 234
转换控制 222
转换通道 365
  保留邮件 377
  备用 355
  标题管理 375
  处理 368
  传递指令 374
  控制参数 380
  配置 365，368
  删除邮件 377
  示例 378
  输出选项 374
  退回邮件 377
  信息流程 370
  映射表 375
  用于转换处理的通信 367
  转换控制 222
转换文件 222
状态通知，请参见通知邮件
状态邮件
子地址 336
自动回复 449
  设置 759
自动删除邮件 518
  GUI 524
  部署 519
  策略定义 519，523
  规则设置 520
  排出用户 528
  排除用户 519
  时间安排 527
  时间安排 GUI 528
自动重新启动 101
自动重新启动，高可用性 102
字符集标记 306
组
  “成员”选项卡 761
  另请参见邮递列表

仅电子邮件成员 761
组，操作原理 199
组，创建 95
组件
配置 50
组扩展属性 199
最大长度的标题行 342
最后可用的主机 313
作业控制器
JOB_LIMIT 池选项 179
JOB_LIMIT 选项 228
MAX_MESSAGES 选项 180
maxjobs 通道选项 179
SLAVE_COMMAND 选项 228
重新启动 180
概念 179
命令 226
配置文件 225
启动 180
启动和停止 180
使用示例 225
停止 180
限制关键字 322