Sun Java System Messaging Server 6.3 管理指南

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

文件号码 820–0513
2007 年 6 月 8 日

070711@17466

目录

图

表

示例

前言

本指南说明如何管理 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服务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。

有关本文档的修订历史记录，请参见第 46 页中的 “Sun Java System Messaging Server 6.3 管理指南修订历史记录”。

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。此外，还应该阅读《Sun Java Communications Suite 5 Deployment Planning Guide》。

阅读本书之前

本指南假设您负责管理 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 Directory Server 和 LDAP
- 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 P–1 本书的结构

章节	说明
前言	关于使用本指南的一般信息。

表 P–1 本书的结构 （续）

章节	说明
第 1 章	介绍要使 Messaging Server 正常运行所需的任务。
第 2 章	说明如何从 Messaging Server 5.2 升级到该版本的 Messaging Server。
第 3 章	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	介绍 Messaging Server 的一般任务。
第 5 章	说明如何配置服务器以支持 POP、IMAP 和 HTTP 服务
第 6 章	说明如何启用单点登录。
第 7 章	介绍用于标准邮件协议（POP、IMAP 和 SMTP）的 Messaging Multiplexor (MMP)。
第 8 章	提供了 MTA 的概念性说明。
第 9 章	介绍地址转换和路由选择。
第 10 章	介绍 MTA 服务和配置。
第 11 章	说明如何在 imta.cnf 文件中配置重写规则。
第 12 章	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	说明如何在 MTA 中使用预定义的通道定义。
第 14 章	说明如何使用 Messaging Server 集成和配置垃圾邮件和病毒过滤软件。
第 15 章	介绍一种可在 SMTP 对话期间检测和拒绝伪造电子邮件的技术。
第 16 章	介绍 LMTP 操作和部署。
第 17 章	介绍休假自动回复机制。
第 18 章	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 19 章	介绍一种可取代 `conn_throttle.so` 的系统信息库进程，此进程提供了类似功能，但却将其扩展到 Messaging Server 安装。
第 20 章	介绍消息存储和消息存储管理界面。
第 21 章	介绍 Messaging Server 的归档概念。
第 22 章	说明如何配置 JMQ 通知插件，以生成供 Message Queue 服务中的客户端使用的消息。
第 23 章	说明如何配置 Messaging Server 的安全性和访问控制。
第 24 章	说明如何管理 S/MIME。

表 P–1 本书的结构 （续）

章节	说明
第 25 章	介绍 Messaging Server 日志记录工具。
第 26 章	介绍对 MTA 进行故障排除的常用工具、方法和过程。
第 27 章	介绍 Messaging Server 的监视功能。
附录 A	说明如何启用 Messaging Server 的 SNMP 支持功能。
附录 B	说明如何在 Messaging Server 中启用 Event Notification Service Publisher (ENS Publisher) 和管理 Event Notification Service (ENS)。
附录 C	说明如何实现短消息服务 (Short Message Service, SMS)。
附录 D	提供可以用来规划安装的工作单。

Messaging Server 文档集

下表汇总了 Messaging Server 文档集中包含的书籍。

表 P–2 Messaging Server 文档

文档标题	内容
《Sun Java System Messaging Server 6.3 Administration Reference》	提供关于 Messaging Server 命令、`configutil` 参数、配置文件和选项以及支持的标准的详细参考信息。
《Sun Java Communications Suite 5 Deployment Planning Guide》	包含部署 Sun Java System Communications Services（包括 Messaging Server）所需的信息。
《Sun Java System Delegated Administrator 6.4 管理指南》	说明如何配置和管理 Sun Java System Communications Services Delegated Administrator。还介绍了 Delegated Administrator 命令。
《Sun Java Communications Suite 5 Schema Migration Guide》	说明如何将 Sun Java System LDAP Directory 数据从 LDAP Schema 1 迁移到针对 System Messaging Server 和 Calendar Server 的 LDAP Schema 2。
《Sun Java Communications Suite 5 Event Notification Service Guide》	介绍针对 System Messaging Server 和 Calendar Server 的 Event Notification Service (ENS) 体系结构和 API。给出关于 ENS API 的详细说明，ENS API 可用于自定义服务器安装。
《Sun Java Communications Suite 5 发行说明》	包含 Sun Java System Messaging Serve 发行时可用的重要信息。此外，还介绍了新增功能和增强功能、已知问题和限制以及其他信息。

表 P–2 Messaging Server 文档 （续）

文档标题	内容
《Sun Java Communications Suite 5 Schema Reference》	作为针对 Messaging Server 和 Calendar Server 的模式信息的参考。
《Sun Java System Communications Express 6.3 管理指南》	说明如何管理 Communications Express 及其附带的软件组件。
《Sun Java System Communications Express 6.3 Customization Guide》	说明如何自定义 Communications Express 的外观。着重说明如何进行最常用的自定义。
《Sun Java Enterprise System 5 Installation Guide for UNIX》	包含安装 Sun Java Enterprise System (Java ES) 软件所需的信息。
《Sun Java System Messaging Server 6 2005Q4 MTA Developer's Reference》	介绍 Messaging Server 邮件传输代理 (Message Transfer Agent, MTA) 软件开发工具包 (Software Development Kit, SDK) 和 Callable Send 工具。
《Sun Java Enterprise System Glossary》	词汇表。
《Sun Java Communications Suite 5 Documentation Center》	指向 Communications Suite 文档的主题链接。

此外，请使用以下 URL 查看适用于所有 Communications Services 产品的文档：
(http://www.sun.com/bigadmin/hubs/comms/)

相关书籍

可以通过 http://docs.sun.com Web 站点联机访问 Sun 技术文档。您可以浏览归档文件或搜索某个特定的书名或主题。

有关与部署 Messaging Server 相关的其他服务器文档，请转至：

- Access Manager 文档：http://docs.sun.com/app/docs/coll/1292.2
- Calendar Server 文档：http://docs.sun.com/app/docs/coll/1313.2
- Communications Express 文档：http://docs.sun.com/app/docs/coll/1312.2
- Directory Server 文档：http://docs.sun.com/app/docs/coll/1316.2
- Instant Messaging 文档：http://docs.sun.com/app/docs/coll/1309.2
- Messaging Server 文档：http://docs.sun.com/app/docs/coll/1312.2

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 P–3 默认路径和文件名

占位符	说明	默认值
msg-svr-base	表示 Messaging Server 的基本安装目录。Messaging Server 的默认基本安装目录和产品目录，取决于具体的平台。	Solaris 系统：`/opt/SUNWmsgsr` Linux 系统：`/opt/sun/messaging`

印刷约定

下表描述了本书中使用的印刷约定。

表 P–4 印刷约定

字体或符号	含义	示例
`AaBbCc123`	命令、文件和目录的名称；计算机屏幕输出	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `machine_name% you have mail.`
`AaBbCc123`	用户键入的内容，与计算机屏幕输出的显示不同	`machine_name%` **`su`** `Password:`
AaBbCc123	要使用实名或值替换的占位符	用于删除文件的命令为 `rm` *filename*。
AaBbCc123	保留未译的新词或术语以及要强调的词（注意：某些强调的词在联机状态下以粗体显示）	这些称为 *Class* 选项。
新词术语强调	新词或术语以及要强调的词	**缓存**是存储在本地的副本。 **不要**保存文件。
《书名》	书名	阅读《用户指南》的第 6 章。

命令示例中的 Shell 提示符

下表显示了默认系统提示符和超级用户提示符。

表 P–5 Shell 提示符

Shell	提示符
UNIX 和 Linux 系统上的 C shell	`machine_name%`
UNIX 和 Linux 系统上的 C shell 超级用户	`machine_name#`
UNIX 和 Linux 系统上的 Bourne shell 和 Korn shell	`$`
UNIX 和 Linux 系统上的 Bourne shell 和 Korn shell 超级用户	`#`

符号约定

下表对本书中可能使用的符号进行了解释。

表 P–6 符号约定

符号	说明	示例	含义
`[ ]`	包含可选的参数和命令选项。	`ls [-l]`	`-l` 不是必需选项。
`{ | }`	包含必需命令选项的选项集。	`-d {y|n}`	`-d` 选项要求您使用参数 `y` 或参数 `n`。
`${ }`	表示变量引用。	`${com.sun.javaRoot}`	引用 `com.sun.javaRoot` 变量的值。
-	连接需要同时按下的多个键。	Control-A	在按 A 键的同时按 Ctrl 键。
+	连接需要连续按下的多个键。	Ctrl+A+N	按 Ctrl 键，再将其释放，然后按后续键。
→	表示图形用户界面中的菜单项选择。	“文件”→“新建”→“模板”	从“文件”菜单中选择“新建”。从“新建”子菜单中选择“模板”。

联机访问 Sun 资源

可以通过 docs.sun.com Web 站点联机访问 Sun 技术文档。您可以浏览 docs.sun.com 文档库或查找某个特定的书名或主题。这些书是以联机文件的形式提供的，有 PDF 和 HTML 两种格式。残障人士用户可以通过辅助技术读取这两种格式的文件。

要访问 Sun 资源，请转至 `http://www.sun.com`。

- Downloads of Sun products
- Services and solutions
- Support（包括修补程序和更新）
- Training
- Research
- Communities（例如，Sun Developer Network）

第三方 Web 站点引用

本文档引用了第三方 URL，并提供了其他相关信息。

注 – 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，请访问 `http://docs.sun.com`，然后单击“发送意见”(Send Comments)。在联机表单中，提供完整的文档标题和文件号码。文件号码包含 7 位或 9 位数字，可在书的标题页或在文档的 URL 中找到该号码。

Sun Java System Messaging Server 6.3 管理指南修订历史记录

版本	日期	更改说明
12	2007 年 6 月 8 日	■ 《Sun Java Communications Suite 5 发行说明》中的“新的 MTA 功能”。 ■ 添加了错误修复和其他小的文档修复。
11	2007 年 4 月 14 日	■ 添加了一个第 19 章示例。 ■ 将支持的 Veritas Server Cluster 版本更新为 3.5、4.0、4.1 和 5.0。 ■ 记录了新内容，第 369 页中的 “12.12.5 垃圾邮件过滤器关键字”。 ■ 添加了错误修复和其他小的文档修复。
10	2007 年 3 月	本技术说明的初始版本。

◆ ◆ ◆ 第 1 章

1 安装后任务和布局

本章假定您已阅读了《Sun Java Communications Suite 5 Deployment Planning Guide》并使用 Sun Java™ Enterprise System 安装程序安装了 Messaging Server。请参见《Sun Java Communications Suite 5 Installation Guide》。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 Delegated Administrator 6.4 管理指南》中对置备进行了介绍。

本章包含以下几个部分：

1.1 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。

▼ 创建 UNIX 系统用户和组

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 `mail` 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 `mailsrv` 并将其与 `mail` 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，则可以在执行第 49 页中的 “1.3 创建初始 Messaging Server 运行时配置”时再指定这些用户和组。

1.2 为 Messaging Server 配置准备 Directory Server

有关目录准备和目录准备脚本 comm_dssetup 的完整信息，请参见《Sun Java Communications Suite 5 Installation Guide》中的第 8 章 “Directory Preparation Tool (comm_dssetup.pl)”。本章说明了如何运行 Directory Server 设置脚本 (`comm_dssetup.pl`)，该脚本用于配置 LDAP Directory Server 以使其能够与 Messaging Server、Calendar Server 或 Delegated Admin CLI 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`。

1.3 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**可以设置具有通用功能的 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，请使用下面以及《Sun Java System Messaging Server 6.3 Administration Reference》中介绍的配置实用程序。

1.3.1 Messaging Server 的先决条件

在运行初始运行时配置程序前，您必须：

- 安装和配置 Directory Server。（请参见《Sun Java Enterprise System 5 Installation Guide for UNIX》。）
- 运行 `comm_dssetup.pl` 程序。（请参见《Sun Java Communications Suite 5 Installation Guide》中的“Messaging Server Postinstallation Configuration”。）
- 在附录 D提供的核对表中记录 Administration Server 和 Directory Server 的安装及配置参数。

1.3.2 Messaging Server 配置核对表

运行 Messaging Server 初始运行时配置程序时，请在表 D–3 中记录参数。要回答某些问题，请参见附录 D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 **确保在设置中正确配置 DNS，并明确指定路由到本地子网之外的主机的方式。**

- `/etc/defaultrouter` 应该包含网关系统的 IP 地址。此地址必须位于本地子网中。
- `/etc/resolv.conf` 存在，并包含可访问的 DNS 服务器和域后缀的适当条目。
- 在 `/etc/nsswitch.conf` 中，`hosts:` 和 `ipnodes:` 行添加了 `files`、`dns` 和 `nis` 关键字。关键字 `files` 必须位于 `dns` 和 `nis` 之前。因此，如果有如下行：

```
hosts:  nis dns files
ipnodes:  nis dns files
```

应将其更改为如下所示：

```
hosts:  files nis dns
ipnodes:  files nis dns
```

- 确保 FQDN 为 `/etc/hosts` 文件中的第一个主机名。

  如果 `/etc/hosts` 文件中的 Internet 主机表如下所示：

  ```
  123.456.78.910 budgie.west.sesta.com
  123.456.78.910 budgie loghost mailhost
  ```

  应对其进行更改，以使主机的 IP 地址只有一行。确保第一个主机名是全限定域名。例如：

  ```
  123.456.78.910 budgie.west.sesta.com budgie loghost mailhost
  ```

- 可通过运行以下命令来验证能否正确读取这些行：

  ```
  # getent hosts ip_address
  # getent ipnodes ip_address
  ```

  如果能正确读取这些行，则会看到后跟 FQDN 和其他值的 IP 地址。例如：

  ```
  # getent hosts 192.18.126.103
  192.18.126.103  budgie.west.sesta.com budgie loghost mailhost
  ```

2 使用以下命令调用 Messaging Server 初始运行时配置：

msg-svr-base`/sbin/configure` *[flag]*

如果是配置远程系统上的 Messaging Server，则可能需要使用 `xhost`(1) 命令。

下表介绍了可以使用 `configure` 程序设置的可选标志：

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。请参见第 53 页中的 “执行无提示安装”。

运行 `configure` 命令后，将启动此配置程序：

3 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。如果未配置管理服务器（仅 Messaging Server 2005Q4 或更低版本），系统会向您发出警告，请选择“确定”继续。

4 **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。

5 **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。有关这些符号连接的更多信息，请参见第 61 页中的 “1.11 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。

6 **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。

7 **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、传送用户邮件并处理 SMTP 验证。MTA 支持托管域、域别名和服务器端过滤器。
- Message Store：使用通用的 Message Store 为统一的邮件传送服务奠定基础。可通过多种协议（HTTP、POP、IMAP）访问消息存储。如果仅配置 Message Store，您还必须选择 MTA。
- Webmail Server：处理 HTTP 协议对来自 Message Store 的邮件的检索。Communication Express 还使用此组件来提供基于 Web 的访问。
- Messaging Multiplexor：作为组织内多个 Messaging Server 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。如果同时选中了 MMP 和 Message Store，则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 63 页中的 “1.12 安装后的端口号”。

  要配置 MMP，请参见第 7 章。

  请选中要配置的所有组件，并取消选择不希望配置的组件。

8 **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 47 页中的 “1.1 创建 UNIX 系统用户和组”。

9 **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。**请注意，它用于 Messaging Server 6 2005Q4 和更低版本，较高版本不在 Directory Server 中存储配置数据，因而不使用 Administration Server。**

从 Directory Server 安装收集配置服务器 LDAP URL。请参见表 D–1 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。默认和建议的标识名 (Distinguished Name, DN) 为 `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。

---

10 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 安装程序收集端口号信息。请参见表 D–1 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，并对 Directory Server 中的所有条目具有全部管理权限。默认和建议的标识名 (Distinguished Name, DN) 为 `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。

11 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` 域中的邮寄主管的地址。该地址不能以 "Postmaster" 开头”

不会自动创建电子邮件地址的用户。因此，您需要以后使用置备工具创建该用户。

12 管理员帐户的密码

输入初始密码，该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 99 页中的 “4.1 修改密码”。

13 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，则发送到不具有域的用户 ID 的邮件将被发送到该域。

如果您要使用 Delegated Administrator CLI（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 Delegated Administrator 6.4 管理指南》。

14 组织 DN

输入组织 DN（将在其下创建用户和组）。默认值为用户/组后缀前附加的电子邮件域。

例如，如果用户/组后缀为 `o=usergroup`，电子邮件域为 `siroe.com`，则默认值为 `o=siroe.com, o=usergroup`（其中 `o=usergroup` 是第 47 页中的 “1.1 创建 UNIX 系统用户和组”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 DN。

15 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。

16 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”。

将以 *msg-svr-base*`/install/configure_`*YYYYMMDDHHMMSS*`.log` 格式创建一个日志文件，其中 *YYYYMMDDHHMMSS* 表示配置的创建年（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（称为 `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指示 `configure` 程序读取无提示安装 state 文件。以后运行 Messaging Server 的初始运行时配置时，`configure` 程序将使用此文件中的答案，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 `saveState` *state* 文件存储在 *msg-svr-base*`/install/configure_`*YYYYMMDDHHMMSS* 目录中，其中 *YYYYMMDDHHMMSS* 表示 `saveState` 文件的创建年（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 **根据需要查看并编辑无提示安装 *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，针对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* 为 `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` 文件的目录的创建年（4 位数）、月、日、小时、分钟和秒。

1.4 针对 Directory Server 副本安装 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。

▼ 针对 Directory Server 副本安装 Messaging Server

1 **针对所有 Directory Server（包括 Directory Server 副本）运行 `comm_dssetup.pl` 程序（请参见《Sun Java Communications Suite 5 Installation Guide》中的"Messaging Server Postinstallation Configuration"）。**

2 **使用复制的 Directory Server 凭证运行 Messaging `configure` 程序，如第 49 页中的 " 1.3 创建初始 Messaging Server 运行时配置 "所述。**

默认情况下，该程序位于 *msg-svr-base*`/sbin/configure` 中。

由于权限无效，`configure` 程序尝试配置 Directory Server 管理员时会失败。但它将生成 *msg-svr-base*`/config/*.ldif` 文件，使用此文件可以对 Directory Server 副本拥有相应权限。

3 **将 `*.ldif` 文件移到主 Directory Server 中。**

4 **对 `*.ldif` 文件运行 `ldapmodify` 命令。**

有关 `ldapmodify` 的更多信息，请参见 Sun Java System Directory Server 文档，或查看 *msg-svr-base*`/install/configure_`*YYYYMMDDHHMMSS*`.log`。

5 **再次运行 `configure` 程序。**

Directory Server 副本（及主副本）配置完毕，可以与 Messaging Server 协同工作。

1.5 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 页中的 “1.5.1 Schema 1 Delegated Administrator for Messaging”
- 第 56 页中的 “1.5.2 LDAP 置备工具”
- 第 47 页中的 “1.1 创建 UNIX 系统用户和组”

1.5.1 Schema 1 Delegated Administrator for Messaging

Messaging Server 可以使用两种 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 Delegated Administrator 6.4 管理指南》。

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

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。

注 – 安装以下产品时，请使用 Java Enterprise System 安装程序。请注意，某些产品本身就有配置，其它产品的配置则嵌入在 Java Enterprise System 安装程序/配置程序中。有关详细信息，请参见特定的产品文档。

▼ 安装 iPlanet Delegated Administrator

1. **确保已安装和配置 Sun Java System Directory Server 5.2。**
   有关更多信息，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. **使用以前的 Messaging Server 5.2 捆绑软件安装 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，以获得最新版本。

   请参阅 iPlanet Delegated Administrator 文档。

1.5.2 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 Schema 1 LDAP 置备工具

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，请参见《Sun Java Enterprise System 5 Installation Guide for UNIX》。
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》。
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种 Sun Java System LDAP Schema，这取决于是否安装了 Access Manager。

4 **安装并配置 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更多信息，请参见第 61 页中的 “1.9 配置 Messenger Express 和 Communications Express 邮件过滤器” 。

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《iPlanet Messaging Server 5.2 Provisioning Guide》和《Sun Java Communications Suite 5 Schema Reference》。Schema Reference 包含用于 Sun LDAP Schema 1 和 v.2 的对象类和属性。

1.6 SMTP 中继阻止

默认情况下，将 Messaging Server 配置为阻止 SMTP 中继尝试；即，拒绝从未经验证的外部源（外部系统是指服务器本身所在的主机之外的任何其他系统）到外部地址的邮件提交尝试。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。特别是，Messaging Server 应该识别其自身的内部系统和子网，这些内部系统和子网的 SMTP 中继应始终被接受。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 客户端尝试通过 Messaging Server 系统的 SMTP 服务器将邮件提交到外部地址，而这些地址不使用 SMTP AUTH (SASL) 进行验证，则提交尝试将被拒绝。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` 中可以找到该表。

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

  $(192.45.67.89/32)  $Y
  127.0.0.1  $Y
  *  $N
```

初始条目用于指定与 `192.45.67.89` 全部 32 位匹配的任何 IP 地址是匹配项并将被视为内部地址（使用 `$(IP-pattern/significant-prefix-bits)` 语法）。第二个条目将把回送 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，则将希望此站点使用：

```
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，在检查 IP 地址是否与特定的 $(.../...) 测试条件相匹配时，*msg-svr-base*/sbin/ imsimta test-match 实用程序很有用。在检查 INTERNAL_IP 映射表是否返回了各种 IP 地址输入所需的结果时，imsimta test -mapping 实用程序通常会更有用。

修改 INTERNAL_IP 映射表之后，请确保运行 *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 6.3 Administration Reference》中的第 2 章 “Message Transfer Agent Command-line Utilities”中找到有关映射文件和普通映射表格式的详细信息以及 imsimta 命令行实用程序的信息。此外，可以在第 495 页中的 “18.6 添加 SMTP 中继”中找到有关 INTERNAL_IP 映射表的信息。

1.7 启用重新引导后启动

通过使用以下引导脚本可以在系统重新引导后启动 Messaging Server：*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）。

▼ 重新引导后启用 Messaging Server

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：**

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
```

1.8 处理 sendmail 客户端

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

要使 sendmail 客户端和 Messaging Server 兼容，您可以创建并修改 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（请参见以下第 60 页中的 “在 Solaris 9 平台上创建 sendmail 配置文件”中的说明）。对于 Solaris 8，请按照第 59 页中的 “在 Solaris 8 上获得正确版本的 /usr/lib/sendmail”中的说明操作。

当您安装以前版本的 Messaging Server 时，/usr/lib/sendmail 二进制文件将由 Messaging Server 产品的组件替换。从 Messaging Server 6.0 一直到当前版本，这种安装期间的替换不再是必需的。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 二进制文件。

对于 Solaris OS 9 平台，sendmail 不再是 setuid 程序。它是 setgid 程序。

▼ 在 Solaris 8 上获得正确版本的 /usr/lib/sendmail

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

在本节的此示例中，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
```

rhino.west.sesta.com 为本地主机名，west.sesta.com 为默认电子邮件域（如第 49 页中的 “1.3 创建初始 Messaging Server 运行时配置”所述）。在 HA 环境中，请使用逻辑主机名。有关高可用性环境中使用的逻辑主机名的更多信息，请参见第 3 章。

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。**

▼ 在 Solaris 9 平台上创建 sendmail 配置文件

1 **在目录 /usr/lib/mail/cf 中找到文件 submit.mc 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 为本地主机名。

rhino.west.sesta.com 为本地主机名，west.sesta.com 为默认电子邮件域（如第 49 页中的 “1.3 创建初始 Messaging Server 运行时配置”所述）。在 HA 环境中，请使用逻辑主机名。有关高可用性环境中使用的逻辑主机名的更多信息，请参见第 3 章。

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。**

1.9 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：

如果是使用 *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
```

如果是使用 *Application Server* 作为 *Web* 容器：

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

在两种情况中均设置以下 `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
```

有关最终用户邮件过滤器的信息，请参见 Messenger Express 和 Communications Express 联机帮助文件。

1.10 性能和调节

请参见《Sun Java Communications Suite 5 Deployment Planning Guide》中的“Performance Considerations for a Messaging Server Architecture”。

1.11 安装后的目录布局

安装 Sun Java System Messaging Server 后，其目录和文件将按照表 1–1 中所述组织进行安排。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 1–1 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。 每台计算机只允许一个 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：此目录通过符号链接（在 UNIX 平台上）被链接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：此目录通过符号链接（在 UNIX 平台上）被链接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/`）。
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 1–1 安装后的目录和文件 （续）

目录	默认位置和说明
SDK 包含文件 `include`	*msg_svr_base*`/include/` （必需位置） 包含软件开发工具包 (Software Development Kits, SDK) 的 Messaging 头文件。
示例 `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。

1.12 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 1–2 列出了安装后指定的端口号。

表 1–2 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.port`)
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`)
995	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`)

表 1–2 安装期间指定的端口号 （续）

端口号	服务（configutil 参数）
443	基于 SSL 的 HTTP 端口。用于加密通信。(service.http.sslport)
7997	Messaging and Collaboration Event Notification Service (ENS) 端口。
27442	作业控制器用以进行内部产品通信的端口。
49994	Watcher 用以进行内部产品通信的端口。有关 Watcher 的更多信息，请参见 Sun Java System Messaging Server 管理指南。(local.watcher.port)

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 1–3 显示了潜在的端口号冲突。

表 1–3 潜在的端口号冲突

冲突的端口号	端口	冲突的端口
995	基于 SSL 的 POP3	具有 SSL 的 MMP POP3 Proxy
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

如果可能，将端口号冲突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。

▼ 更改端口号

- **使用 `configutil` 实用程序更改端口号。**

  有关完整语法和用法，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“configutil”。

示例 1–1 更改 Messenger Express HTTP 端口号

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
# stop-msg http
$start-msg http
```

◆ ◆ ◆ 第 2 章

2 从 Messaging Server 5.2 升级到 Sun Java System Messaging Server

本章中的信息已经移至《Sun Java Communications Suite 5 Upgrade Guide》。请查看该文档以获得完整的信息。请注意，第 598 页中的 “20.15 将邮箱迁移或移动到新系统”仍保留在本书中。

2.1 移动的信息

请参见《Sun Java Communications Suite 5 Upgrade Guide》。

◆ ◆ ◆ 第 3 章

3 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《Sun Java Communications Suite 5 Deployment Planning Guide》中的第 6 章 “Designing for Service Availability”以及相应的 Veritas 或 Sun Cluster Server 文档，并已了解详细规划、安装说明、必需的修补程序和其他所需信息。

本章包含以下几个部分：

3.1 支持的版本

有关最新的支持版本和平台，请参见《Sun Java Communications Suite 5 发行说明》中的“此 Messaging Server 发行版的新增功能”。

3.2 高可用性模型

Messaging Server 可以使用不同的高可用性模型。下面是三个比较基本的模型：

以下几个小节更详细地介绍了其中的每个模型。

请注意，不同的 HA 产品可能会支持不同的模型，也可能不支持不同的模型。请参见 HA 文档以确定支持哪些模型。

3.2.1 不对称

基本不对称或**备用**高可用性模型由两个群集主机或**节点**组成。将为两个节点指定逻辑 IP 地址和关联主机名。

在这种模型中，只有一个节点在任何给定时间都处于活动状态，备份或备用节点大部分时间内处于空闲状态。这两个节点之间的单一共享磁盘阵列由活动或**主**节点进行配置和控制。消息存储分区和邮件传输代理 (Mail Transport Agent, MTA) 队列位于此共享卷上。

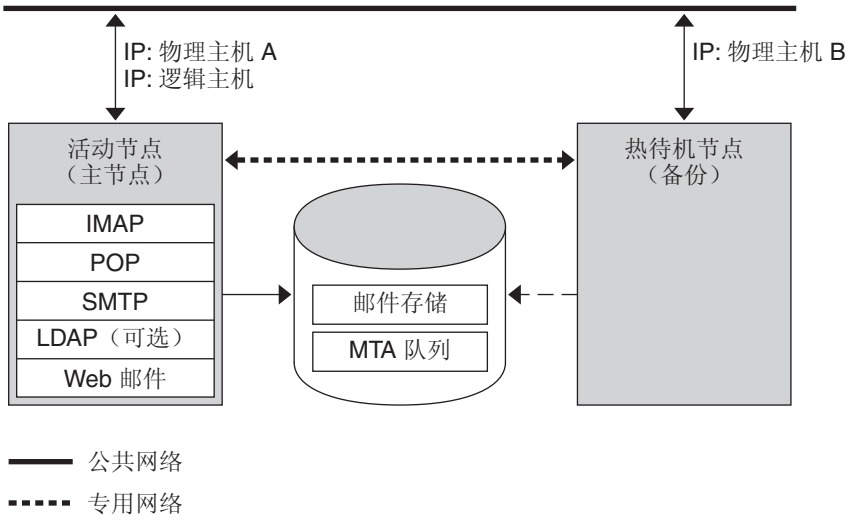


图 3–1 不对称高可用性模式

上图显示了两个物理节点 `Physical-A` 和 `Physical-B`。在故障转移之前，活动节点是 `Physical-A`。在故障转移之后，`Physical-B` 变为活动节点，并切换共享卷以便由 `Physical-B` 对其进行控制。将停止 `Physical-A` 上的所有服务，并在 `Physical-B`上启动这些服务。

此模型的优点在于，备份节点是专用的，并且是完全为主节点保留的。此外，发生故障转移时，备份节点上不会出现资源争用。但是，此模型也意味着备份节点大部分时间内处于空闲状态，因此资源的利用率很低。

3.2.2 对称

基本对称或“双重服务”高可用性模型由两个主机构成，每个主机都有自己的逻辑 IP 地址。每个逻辑节点都与一个物理节点相关联，并且每个物理节点都控制一个具有两个存储卷的磁盘阵列。一个卷用作其本地消息存储分区和 MTA 队列，另一个卷是其伙伴的消息存储分区和 MTA 队列的镜像。

下图显示了对称高可用性模式。两个节点同时处于活动状态，并且每个节点都用作另一个节点的备份节点。正常情况下，每个节点仅运行一个 Messaging Server 实例。

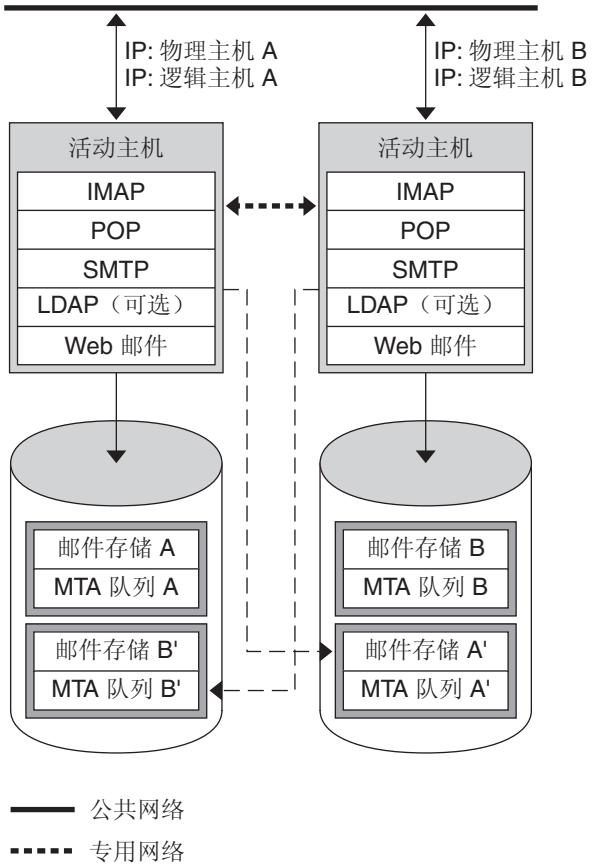


图 3–2 对称高可用性模式

在故障转移后，将关闭出现故障的节点上的服务，并在备份节点上重新启动这些服务。此时，备份节点为这两个节点运行 Messaging Server 并管理两个单独的卷。

此模型的优点在于，两个节点同时处于活动状态，因而充分利用计算机资源。但是，在出现故障期间，备份节点会发生较多的资源争用，因为它从两个节点运行 Messaging Server 服务。因此，应尽快修复出现故障的节点，并将服务器切换回其双重服务状态。

此模型还提供了一个备份存储阵列。如果磁盘阵列发生故障，备份节点上的服务可以选取其冗余映像。

要配置对称模型，您需要在共享磁盘上安装共享的二进制文件。请注意，这样做可能会阻止您执行滚动升级（一种可以让您在 Messaging Server 修补程序发行期间更新系统的功能）。（计划在将来的版本中提供此功能。）

3.2.3 N+1 (N Over 1)

N+1 或 "N over 1" 模型在多节点不对称配置下运行。需要 N 个逻辑主机名和 N 个共享磁盘阵列。将保留单一备份节点以作为所有其他节点的备用节点。备份节点能够从 N 个节点同时运行 Messaging Server。

下图说明了基本的 N+1 高可用性模型。

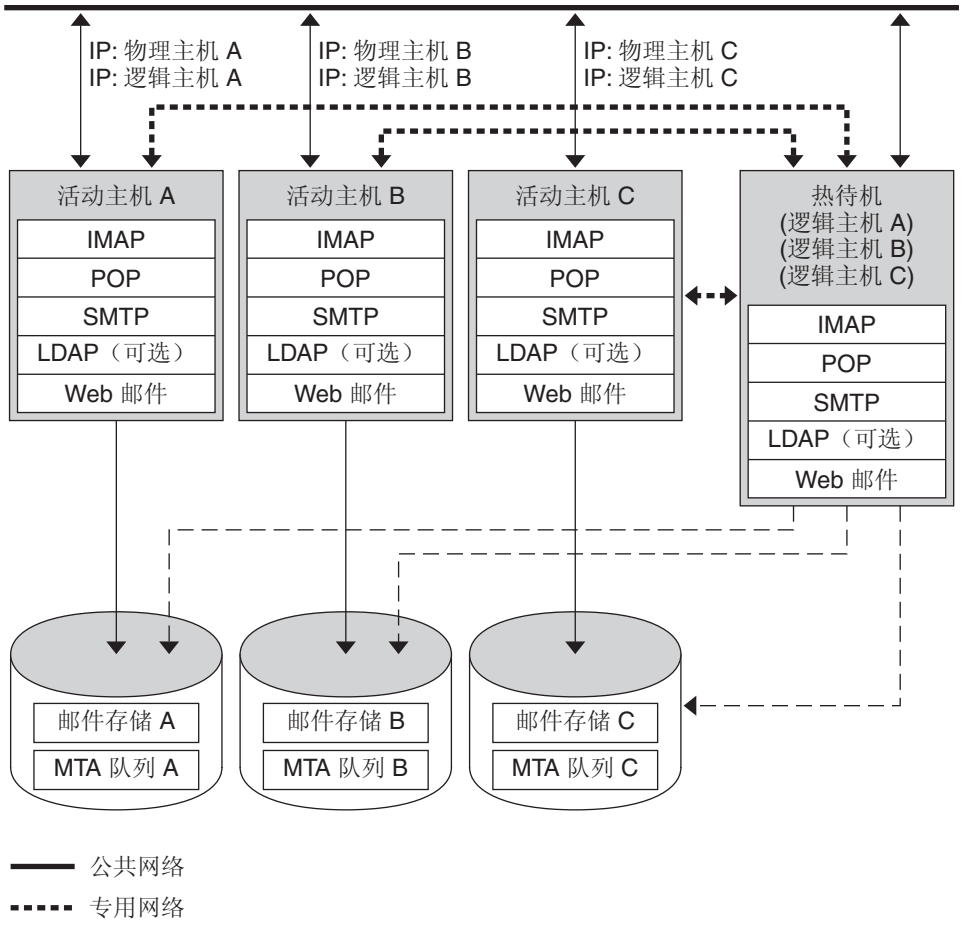


图 3–3 N+1 高可用性模式

在一个或多个活动节点进行故障转移后，备份节点将承担出现故障的节点的工作。

N+1 模型的优点在于，可以将服务器负载分配到多个节点上，在出现任何可能的节点故障时，只需由一个备份节点来承担这些节点的工作。因此，计算机空闲率为 1/N，而单一不对称模型为 1/1。

要配置 N+1 模型，您只需在本地磁盘上安装二进制文件（即，不是像对称模型一样在共享磁盘上安装二进制文件）。对于任何对称、1+1 或 N+1 不对称或对称 HA 解决方案，当前 Messaging Server 安装和设置过程强制您将二进制文件放在共享磁盘上。

3.2.4 选择高可用性模型

下表简要说明了每个高可用性模型的优点和缺点。使用这些信息将有助于确定适合您的部署的模型。

表 3–1 HA 模型比较

模型	优点	缺点	建议的用户
不对称	■ 简单配置 ■ 100% 保留备份节点	不能充分利用计算机资源。	计划将来扩大规模的小型服务提供商
对称	■ 系统资源使用率较高 ■ 可用性较高	备份节点上存在资源争用。 HA 需要完全冗余的磁盘。	在出现单一服务器故障时可以接受性能下降的小型公司部署
N+1	■ 负载分配 ■ 易于扩展	管理和配置比较复杂。	需要不受限制地分配资源的大型服务提供商

3.2.5 系统故障时间计算

下表说明了在任何给定的一天邮件传送服务由于系统故障而无法使用的概率。这些计算假设每个服务器平均每三个月会有一天出现故障（由于系统崩溃或服务器挂起），并且每个存储设备每 12 个月会有一天出现故障。这些计算还忽略了两个节点同时出现故障的小概率事件。

表 3–2 HA 故障概率

模型	服务器故障时间概率
单个服务器（没有高可用性）	概率（故障）=（4 天系统故障 + 1 天存储故障）/365 = 1.37%
不对称	概率（故障）=（0 天系统故障 + 1 天存储故障）= 0.27%
对称	概率（故障）=（0 天系统故障 + 0 天存储故障）/365 =（接近 0）
N+1 不对称	概率（故障）=（5 小时系统故障 + 1 天存储故障）/(365xN) = 0.27%/N

3.3 安装 Messaging Server 高可用性—概述

在为部署选择相应的 HA 模型后，您需要在 Sun Cluster HA 或 Veritas HA 之间进行选择。本节提供了初步 HA 部署信息。后续几节将提供有关 Sun Cluster 和 Veritas 高可用性解决方案的具体信息。

3.3.1 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 时安装的。可以在 Sun Java Communications Suite 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。）

3.3.2 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：

- 默认情况下没有为 Messaging Server 安装高可用性；请确保从 Java Enterprise System 安装程序的“自定义安装”菜单中选择“高可用性组件”。
- 在运行安装时，请确保 Messaging Server 的 HA 逻辑主机名和关联的 IP 地址能够正常使用（例如，处于活动状态）。这是因为部分安装将使用它们来建立 TCP 连接。在邮件服务器的 HA 逻辑主机名当前所指的群集节点上运行安装。
- 请确保 *msg_svr_base* 位于共享文件系统中；否则，高可用性将无法正常工作。例如，在故障转移到另一个节点后，服务器将无法再查看出现故障的节点上的服务器所积累的数据。
- 在初始运行时配置期间，当系统要求您输入 Messaging Server 主机的全限定域名时，请确保为 Messaging Server 指定全限定 HA 逻辑主机名。在安装期间，将尝试使用此逻辑主机名建立 TCP 连接。
- 在运行 `ha_ip_config` 时，当系统要求您输入 Messaging Server 的 IP 地址时，请确保指定与 Messaging Server 逻辑主机名关联的 IP 地址。不要使用物理主机的 IP 地址。
- 需要在安装和配置 Messaging Server 当前版本之前安装群集软件。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。
- 运行 Messaging Server 初始运行时配置（请参见第 49 页中的 “1.3 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，则需要使用群集主机名再一次重新配置。

3.3.3 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，如果您要升级第一个节点，则可以通过 Communications Suite 安装程序 安装 Messaging Server，然后对其进行配置。随后，您可以故障转移到第二个节点，在该节点上通过 Communications Suite 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` 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*。

以下两节第 93 页中的 “3.5 Veritas Cluster Server 代理安装”和第 74 页中的 “3.4 Sun Cluster 安装”介绍何时可以使用 `useconfig` 实用程序。

3.4 Sun Cluster 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。本节包含以下主题：

请参见 Sun Cluster 文档。

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

3.4.1 Sun Cluster 的要求

本节假定以下情况：

- 在 Solaris 操作系统（具有必需的修补程序）中安装并配置了 Sun Cluster。
- 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。

3.4.2 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。本地文件系统也称为故障转移文件系统 (Failover File Systems, FFS)，它提供了比群集文件系统 (Cluster File Systems, CFS) 更好的输入/输出性能，群集文件系统也称为全局文件系统。HAStoragePlus 支持 FFS 和 CFS。与之相反，HAStorage 仅支持 CFS。

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。

要确定是在数据服务资源组中创建 HAStorage 还是创建 HAStoragePlus 资源，请考虑以下条件：

- 如果使用的是 Sun Cluster 3.0 Release May 2002 或 Sun Cluster 3.1，请使用 HAStoragePlus
- 如果使用的是 Sun Cluster 3.0 December 2001 或更低版本，请使用 HAStorage

有关 HAStoragePlus 的详细信息，请参见相应的 Sun Cluster 文档，如《Sun Cluster 3.1 Data Service Planning and Administration Guide (`http://docs.sun.com/app/docs/coll/573.10`)》。

3.4.3 为 Messaging Server 配置 Sun Cluster HAStorage 或 HAStoragePlus

本节介绍了如何为 Sun Cluster 的 Messaging Server 配置 HAStorage 和 HAStoragePlus。第一节介绍了一般步骤。后面几节介绍了对称和不对称部署的具体示例。

配置 HA 后，请确保查阅第 91 页中的 “3.4.4 在服务器上绑定 IP 地址”，以了解与 HA 支持相关的其他步骤。

以下说明假设已使用 HA 逻辑主机名和 IP 地址配置了 Messaging Server。假设物理主机名为 `mars` 和 `venus`，HA 逻辑主机名为 `meadow`。图 3–4 说明了您在配置 Messaging Server HA 支持时要创建的各种 HA 资源的嵌套依赖性。

注 – 虽然我们介绍了如何配置 HAStorage 和 HAStoragePlus，但我们强烈建议您使用具有较好 I/O 性能的 HAStoragePlus。请参见第 75 页中的 “3.4.2 关于 HAStoragePlus” 。

本节包含以下小节：

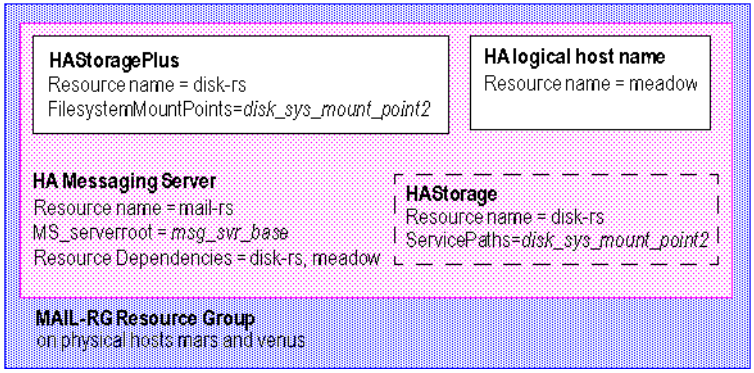


图 3–4 简单 Messaging Server HA 配置

▼ 为 Messaging Server 配置 Sun Cluster HAStorage 或 HAStoragePlus—一般示例

本节提供了为 Messaging Server 配置 HA 的一般步骤。在查看这些步骤后，请参见以下各节中的具体不对称或对称示例。在这些说明中，物理主机名为 `mars` 和 `venus`。逻辑主机名为 `meadow`。

图 3–4 说明了您在配置 Messaging Server HA 支持时要创建的各种 HA 资源的嵌套依赖性。

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` 中的消息。

2 在所有节点上安装所需的 Messaging Sun Cluster Data Service Agents 软件包 (SUNWscims)。

3 在每个群集节点上，创建用于运行 Messaging Server 的 Messaging Server 运行时用户和组。

用户 ID 和组 ID 号在所有群集节点上必须相同。**运行时用户** *ID* 是用于运行 Messaging Server 的用户名。此名称不应该为 `root`。默认值为 `mailsrv`。**运行时组** *ID* 是用于运行 Messaging Server 的组。默认值为 `mail`。

虽然 `configure` 实用程序可以为您创建这些名称，但也可以按照本章中所述，在运行 `configure` 之前创建这些名称以作为每个节点的准备过程的一部分。运行时用户和组 ID 名必须位于以下文件中：

- 在所有群集节点上，`mailsrv` 或您选择的名称必须位于 `/etc/passwd` 中
- 在所有群集节点上，`mail` 或您选择的名称必须位于 `/etc/group` 中

请参见第 47 页中的 “1.1 创建 UNIX 系统用户和组” 。

4 将所需的资源类型添加到 Sun Cluster 中。

配置 Sun Cluster 以了解要使用的资源类型。要将 Messaging Server 注册为资源，请使用以下命令：

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

要将 HAStoragePlus 注册为资源类型，请使用以下命令：

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

要对 HAStorage 执行相同的操作以将其注册为资源类型，请使用此命令：

```
# scrgadm -a -t SUNW.HAStorage
```

5 为 Messaging Server 创建故障转移资源组。

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 `mars` 和 `venus` 群集节点上：

```
# scrgadm -a -g MAIL-RG -h mars,venus
```

当然，您可以按照您的意愿对资源组使用任何名称。

6 创建一个 HA 逻辑主机名资源并将其联机。

如果尚未执行此操作，请为 HA 逻辑主机名创建并启用资源，将该资源置于资源组中。以下命令使用逻辑主机名 `meadow` 执行此操作。因为忽略了 `-j` 开关，所以创建的资源名称将仍旧为 `meadow`。`meadow` 是客户端用来与资源组中的服务进行通信的逻辑主机名。

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

7 创建 HAStorage 或 HAStoragePlus 资源。

接下来，您需要为 Messaging Server 所依据的文件系统创建 HAStorage 或 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* 置于其控制之下：

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

`SUNW.HAStoragePlus` 表示一个或多个数据服务资源要使用的设备组、群集和本地文件系统。用户可以将 `SUNW.HAStoragePlus` 资源类型添加到资源组中，并在其他资源和 `SUNW.HAStoragePlus` 资源之间建立依赖关系。这些依赖关系可确保数据服务资源在具备以下条件后保持联机：

- 所有指定的设备服务可用（并根据需要进行配置）
- 在执行检查后安装所有指定的文件系统

`FilesystemMountPoints` 扩展属性允许指定全局或本地文件系统。即，可以从所有群集节点或单个群集节点访问文件系统。`SUNW.HAStoragePlus` 资源所管理的本地文件系统安装在单个群集节点上，并要求基础设备为 Sun Cluster 全局设备。指定本地文件系统的 `SUNW.HAStoragePlus` 资源只能属于启用了关系切换的故障转移资源组。因此，可以将这些本地文件系统称为故障转移文件系统。可以同时指定本地和全局文件系统装入点。

如果 `/etc/vfstab` 条目满足以下两个条件，则假设装入点位于 `FilesystemMountPoints` 扩展属性中的文件系统为本地文件系统：

- 非全局安装选项
- 将 mount at boot 标志设置为 `no`

注 – `SUNW.HAStoragePlus` 资源类型的实例忽略全局文件系统的 mount at boot 标志。

对于 HAStoragePlus 资源，以逗号分隔的 `FilesystemMountPoints` 列表是 Messaging Server 所依据的群集文件系统 (Cluster File Systems, CFS) 或故障转移文件系统 (Failover File Systems, FFS) 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 15 中指示该附加依赖性。

对于 HAStorage，请使用以下命令：

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

对于 HAStorage 资源，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 15 中指示该附加依赖性。

8 **在主节点上安装所需的 Messaging Server 软件包。选择稍后配置选项。**

使用 Communications Suite 安装程序安装 Messaging Server 软件包。

对于对称部署：在 Sun Cluster 共享磁盘所安装的文件系统上安装 Messaging Server 二进制文件和配置数据。例如，对于 Messaging Server， 二进制文件可能位于 `/disk_sys_mount_point-1/SUNWmsgsr`，配置数据可能位于 `/disk_sys_mount_point-2/config`。

对于不对称部署：在每个 Sun Cluster 节点的本地文件系统上安装 Messaging Server 二进制文件。在共享磁盘上安装配置数据。例如，配置数据可能位于 `/disk_sys_mount_point-2/config`。

9 **配置 Messaging Server。**

请参见第 49 页中的 “1.3 创建初始 Messaging Server 运行时配置”。

在初始运行时配置中，系统会要求您输入全限定主机名。您必须使用 HA 逻辑主机名而不是物理主机名。

在初始运行时配置中，您需要在第 49 页中的 “1.3 创建初始 Messaging Server 运行时配置”中指定配置目录。请确保使用 HAStorage 或 HAStoragePlus 资源的共享磁盘目录路径。

10 **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.autorestart` 设置为 1）。

有关运行该脚本的说明，请参见第 91 页中的 “3.4.4 在服务器上绑定 IP 地址”。

只应在主节点上运行一次 `ha_ip_config` 脚本。

11 **修改 `imta.cnf` 文件，并用群集的逻辑主机名替换所有出现的物理主机名。**

12 **将资源组从主群集节点故障转移到辅助群集节点，以确保故障转移正常工作。**

手动将资源组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 mars 上联机，则使用以下命令将其故障转移到 venus：

```
# scswitch -z -g MAIL-RG -h venus
```

如果您要升级第一个节点，则可以通过 Communications Suite 安装程序 安装 Messaging Server，然后对其进行配置。随后，您可以故障转移到第二个节点，在该节点上通过 Communications Suite 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。

13 在辅助节点上安装所需的 Messaging Server 软件包。选择稍后配置选项。

在故障转移到第二个节点后，使用 Communications Suite 安装程序安装 Messaging Server 软件包。

对于对称部署：不会安装 Messaging Server。

对于不对称部署：在本地文件系统上安装 Messaging Server 二进制文件。

14 在第二个群集节点上运行 `useconfig`。

`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。无需运行初始运行时配置程序 (`configure`)，而是使用 `useconfig` 实用程序（请参见第 74 页中的“3.3.3 使用 useconfig 实用程序”）。

15 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,meadow
```

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 `meadow`。

如果 Messaging Server 具有附加文件系统依赖性，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。

16 启用 Messaging Server 资源。

现在应该激活 HA Messaging Server 资源，从而使邮件服务器联机。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。

17 验证上述操作是否生效。

使用 `scstat -pvv` 命令查看 MAIL-RG 资源组是否已联机。

您还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`。有关更多调试选项和信息，请参见第 90 页中的“3.4.3.1 如何在 Sun Cluster 上启用调试”。

▼ 为 Sun Cluster 3.x 取消配置 Messaging Server HA 支持—一般示例

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 74 页中的 “3.4 Sun Cluster 安装”中所述）（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
```

▼ 配置双节点对称 Messaging Server—示例

在此示例中，我们假设两个群集节点具有物理主机名 `mars.red.siroe.com` 和 `venus.red.siroe.com`。安装和配置目录位置必须是唯一的。如果每个节点上的安装和配置目录具有相同的目录名（如 `/opt/SUNWmsgsr` 和 `/var/opt/SUNWmsgsr`），则会出现争用问题。当 `venus` 故障转移到 `mars` 时，将出现争用问题，两个 Messaging Server 实例争用相同的安装和配置目录。

为安装和配置目录创建唯一名称的最佳做法是，安装目录使用格式 /opt/*NodeMember*/SUNWmsgsr；配置目录使用格式 /var/opt/*NodeMember*/SUNWmsgsr。您可以使用任何目录来安装二进制文件和配置数据，只要它们是唯一的。

在此示例中，我们假设两个群集节点具有物理主机名 mars.red.siroe.com 和 venus.red.siroe.com。

对于 mars.red.siroe.com，二进制文件安装在 /opt/mars/SUNWmsgsr 中，配置数据安装在 /var/opt/mars/SUNWmsgsr 中。

对于 venus.red.siroe.com，二进制文件安装在 /opt/venus/SUNWmsgsr 中，配置数据安装在 /var/opt/venus/SUNWmsgsr 中。

我们使用两个名为 meadow 和 pasture 的逻辑主机名及其相应的逻辑 IP 地址。例如，两个节点上的 /etc/hosts 文件类似于以下内容：

```
192.18.75.155 meadow.red.siroe.com meadow
192.18.75.157 pasture.red.siroe.com pasture
```

1 **在两个节点上安装 Messaging Server Sun Cluster 代理软件包 (SUNWscims)。**

2 **创建四个文件系统。**

这些文件系统可以是群集文件系统，也可以是本地文件系统（故障转移文件系统）。

```
/var/opt/mars/SUNWmsgsr
/var/opt/venus/SUNWmsgsr
/opt/mars/SUNWmsgsr
/opt/venus/SUNWmsgsr
```

这些文件系统应安装在共享磁盘上。例如，我们在下面显示了四个群集文件系统。下面显示的 /etc/vfstab 内容在所有群集节点上应该是类似的。

```
# cat /etc/vfstab
#device  device  mount  FS  fsck  mount  mount  to  mount  to  fsck  point  type
pass at_boot_options
/dev/md/penguin/dsk/d500 /dev/md/penguin/rdsk/d500 /opt/mars/SUNWmsgsr ufs 2 yes
logging,global
/dev/md/penguin/dsk/d400 /dev/md/penguin/rdsk/d400 /var/opt/mars/SUNWmsgsr ufs 2
yes logging,global
/dev/md/polarbear/dsk/d200 /dev/md/polarbear/rdsk/d200 /opt/venus/SUNWmsgsr ufs 2
yes  logging,global
/dev/md/polarbear/dsk/d300 /dev/md/polarbear/rdsk/d300 /var/opt/venus/SUNWmsgsr
ufs 2 yes logging,global
```

如果要将上面显示的四个文件系统作为本地文件系统（故障转移文件系统），请将 mount at boot 选项设置为 no 并删除安装选项 `global` 关键字：

3 配置主节点

a. 在主节点上添加所需的资源类型。

此操作配置 Sun Cluster 以了解要使用的资源类型。要注册 Messaging Server 和 HAStoragePlus 资源，请使用以下命令：

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

b. 为名为 `MS_RG_MARS` 的 Messaging Server 创建故障转移资源组。

```
# scrgadm -a -g MS_RG_MARS -h mars,venus
```

c. 创建一个名为 `meadow` 的逻辑主机名资源、将其添加到资源组中并使其联机。

```
# scrgadm -a -L -g MS_RG_MARS -l meadow
# scrgadm -c -j meadow -y R_description="LogicalHostname resource for meadow"
# scswitch -Z -g MS_RG_MARS
```

d. 使用以前创建的文件系统创建一个名为 `ms-hasp-mars` 的 HAStoragePlus 资源。

```
# scrgadm -a -j ms-hasp-mars -g MS_RG_MARS -t SUNW.HAStoragePlus -x
FileSystemMountPoints ="/opt/mars/SUNWmsgsr, /var/opt/mars/SUNWmsgsr" -x
AffinityOn=TRUE
```

e. 启用 HAStoragePlus 资源：

```
# scswitch -e -j ms-hasp-mars
```

4 在主节点上安装 Messaging Server。

使用 Communications Suite 安装程序安装 Messaging Server 软件包。确保在共享文件系统上安装 Messaging Server 二进制文件和配置数据（请参见步骤 2）。例如，对于此 Messaging Server 实例，邮件传送二进制文件位于 `/opt/mars/SUNWmsgsr` 中，配置数据位于 `/var/opt/mars/SUNWmsgsr` 中。

5 在主节点上安装并配置 Messaging Server（请参见第 49 页中的“ 1.3 创建初始 Messaging Server 运行时配置 ”）。

初始运行时配置程序要求输入全限定主机名。输入逻辑主机名 `meadow.red.siroe.com`。该程序还要求指定配置目录。输入 `/var/opt/mars/SUNWmsgsr`。

6 在主节点上运行 `ha_ip_config` 脚本，并提供逻辑 IP 地址。

此脚本仅在主节点上运行，而不在辅助节点上运行。`ha_ip_config` 脚本位于 `sbin` 目录下的安装目录中。例如：

```
# /opt/mars/SUNWmsgsr/sbin/ha_ip_config
```

```
Please specify the IP address assigned to the HA logical host name.
Use dotted decimal form, a.b.c.d

Logical IP address: 192.18.75.155
# This value is the logical IP address of the logical hostname. Refer
# to the /etc/hosts file.
Please specify the path to the top level directory in which iMS is
installed.

iMS server root: /opt/mars/SUNWmsgsr

. . .

Updating the file /opt/mars/SUNWmsgsr/config/dispatcher.cnf
Updating the file /opt/mars/SUNWmsgsr/config/job_controller.cnf
Setting the service.listenaddr configutil parameter
Setting the local.snmp.listenaddr configutil parameter
Setting the service.http.smtphost configutil parameter
Setting the local.watcher.enable configutil parameter
Setting the local.autorestart configutil parameter
Setting the metermaid.config.bindaddr configutil parameters
Setting the metermaid.config.serveraddr configutil parameters
Setting the local.ens.port parameter
Configuration successfully updated
```

7 **修改 imta.cnf 文件，并使用 HA 逻辑主机名 (meadow) 替换出现的所有物理主机名（mars）。**

8 **将资源组故障转移到辅助节点 (venus)。**

进行故障转移后，您将随后配置辅助节点 (venus)。

```
# scswitch -z -g MS_RG_VENUS -h mars
```

9 **在辅助节点 (venus) 上运行 useconfig 实用程序。请参见第 74 页中的“ 3.3.3 使用 useconfig 实用程序 ”**

您不必运行初始运行时配置程序 (configure) 或安装 Messaging Server 软件包。

在下面的示例中，/var/opt/mars/SUNWmsgsr 是共享配置目录。

```
# useconfig /var/opt/mars/SUNWmsgsr/setup/configure_20061201124116
cp /var/opt/mars/SUNWmsgsr/setup/configure_20061201124116/Devsetup.properties
/opt/mars/SUNWmsgsr/lib/config-templates/Devsetup.properties
/usr/sbin/groupadd mail
/usr/sbin/useradd -g mail -d / mailsrv
/usr/sbin/usermod -G mail mailsrv
sed -e "s/local.serveruid/mailsrv/" -e "s/local.serveruid/mail/" -e "s:<msg·RootPath>:/opt/mars/SUNWmsgsr:"
/opt/mars/SUNWmsgsr/lib/config-templates/devtypes.txt.template >
/opt/mars/SUNWmsgsr/lib/config-templates/devtypes.txt
sed -e "s/local.serveruid/mailsrv/" -e "s/local.serveruid/mail/" -e
```

```
"s:<msg·RootPath>:/opt/mars/SUNWmsgsr:"
/opt/mars/SUNWmsgsr/lib/config-templates/config.ins.template >
/opt/mars/SUNWmsgsr/lib/config-templates/config.ins
/opt/mars/SUNWmsgsr/lib/devinstall -l sepadmsvr:pkgcfg:config -v -m -i
/opt/mars/SUNWmsgsr/lib/config-templates/config.ins
/opt/mars/SUNWmsgsr/lib/config-templates
/opt/mars/SUNWmsgsr/lib/jars /opt/mars/SUNWmsgsr/lib
devinstall returned 0
crle -c /var/ld/ld.config -s
 /usr/lib/secure:/opt/SUNWmsgsr/lib:/opt/venus/SUNWmsgsr/lib:/opt/mars/SUNWmsgsr/lib
-s /opt/mars/SUNWmsgsr/lib
See /opt/mars/SUNWmsgsr/install/useconfiglog_20061211155037 for more details
```

10 创建 HA Messaging Server 资源并将其启用。

```
# scrgadm -a -j ms-rs-mars -t SUNW.ims -g MS_RG_MARS -x IMS_serverroot
=/opt/mars/SUNWmsgsr -y Resource_dependencies=meadow,ms-hasp-mars
# scswitch -e -j mail-rs-mars
```

以上命令为 Messaging Server 创建一个名为 `ms-rs-mars` 的 HA Messaging Server 资源，它将安装在 `/opt/mars/SUNWmsgsr` 上。此 HA Messaging Server 资源依赖于 HA 磁盘资源，即，以前创建的文件系统以及 HA 逻辑主机名 `meadow`。

11 确保所有功能均正常工作。

将 Messaging Server 资源故障转移回主节点。

```
# scswitch -z -g MAIL-RG -h mars
```

12 类似地，再为第二个 Messaging Server 实例创建一个故障转移资源组，并将 `venus` 作为主节点，而将 `mars` 作为辅助（或备用）节点。

重复第 3 步至第 10 步，并将 `venus` 作为此资源组的主节点，将 `MS_RG_VENUS` 作为资源组，将 `pasture` 作为逻辑主机名，而将 `ms-hasp-venus` 作为 HAStoragePlus 资源。因此，这些命令将如下所示：

要创建资源组 `MS_RG_VENUS`，请使用以下命令：

```
# scrgadm -a -g MS_RG_VENUS -h venus,mars
```

要创建名为 `pasture` 的逻辑主机名资源、将其添加到资源组中并使其联机，请使用以下命令：

```
# scrgadm -a -L -g MS_RG_VENUS -l pasture
# scrgadm -c -j pasture -y R_description="LogicalHostname resource for pasture"
# scswitch -Z -g MS_RG_VENUS
```

要使用以前创建的文件系统创建一个名为 ms-hasp-venus 的 HAStoragePlus 资源，请使用以下命令：

```
# scrgadm -a -j ms-hasp-venus -g MS_RG_VENUS -t SUNW.HAStoragePlus -x
FileSystemMountPoints ="/opt/venus/SUNWmsgsr, /var/opt/venus/SUNWmsgsr" -x
AffinityOn=TRUE
```

要启用 HAStoragePlus 资源，请使用以下命令：

```
# scswitch -e -j ms-hasp-venus
```

要在主节点上运行 ha_ip_config 脚本并提供逻辑 IP 地址，请使用以下命令：

```
# /opt/venus/SUNWmsgsr/sbin/ha_ip_config
```

要创建 HA Messaging Server 资源并将其启用，请使用以下命令：

```
# scrgadm -a -j ms-rs-venus -t SUNW.ims -g MS_RG_VENUS -x IMS_serverroot
=/opt/venus/SUNWmsgsr -y Resource_dependencies=pasture,ms-hasp-venus
# scswitch -e -j mail-rs-venus
```

要将资源组故障转移到辅助节点 (venus)，请使用以下命令：

```
# scswitch -z -g MS_RG_MARS -h venus
```

要在辅助节点 (mars) 上运行 useconfig，请运行 useconfig 实用程序：

```
# useconfig /var/opt/venus/SUNWmsgsr/setup/configure_20061201124116
```

要通过将 Messaging Server 资源故障转移回主节点以确保所有功能均正常工作，请使用以下命令：

```
 # scswitch -z -g MAIL-RG -h venus
```

▼ 取消配置 HA 对称部署

当需要升级 Messaging Server 或 Sun Cluster，或者需要卸载 Messaging Server 时，将执行取消配置操作。假设系统是使用上一示例配置的。

第一步是删除群集中的每个资源组。该示例中有两个资源组：MS_RG_MARS 和 MS_RG_VENUS。必须将这两个组都删除。

1 从群集中删除资源组 MS_RG_MARS。

仅在一个节点上使用以下命令。不必在每个节点上都执行此操作。

a. 使所有群集节点上的资源组脱机：

```
# scswitch -F -g MS_RG_MARS
```

b. 禁用所有特定的 Messaging Server 资源：

```
# scswitch -n -j ms-rs-mars
# scswitch -n -j meadow
# scswitch -n -j ms-hasp-mars
```

c. 删除所有特定的 MS 资源：

```
# scrgadm -r -j ms-rs-mars
# scrgadm -r -j meadow
# scrgadm -r -j ms-hasp-mars
```

d. 删除资源组：

```
scrgadm -r -g MS_RG_MARS
```

2 从群集中删除资源组 MS_RG_VENUS。

仅在一个节点上使用以下命令。不必在每个节点上都执行此操作。

a. 使所有群集节点上的资源组脱机：

```
# scswitch -F -g MS_RG_VENUS
```

b. 禁用所有特定的 Messaging Server 资源：

```
# scswitch -n -j ms-rs-venus
# scswitch -n -j pasture
# scswitch -n -j ms-hasp-venus
```

c. 删除所有特定的 MS 资源：

```
# scrgadm -r -j ms-rs-venus
# scrgadm -r -j pasture
# scrgadm -r -j ms-hasp-venus
```

d. 删除资源组：

```
scrgadm -r -g MS_RG_VENUS
```

3 取消注册未使用的资源类型。

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

▼ 配置双节点 HA 不对称 Messaging Server—示例

在本示例中，我们假设两个群集节点具有物理主机名 daisy.red.siroe.com 和 lavender.red.siroe.com，具有逻辑主机名 budgie。

对于 daisy.red.siroe.com，二进制文件安装在 /opt/SUNWmsgsr 中，配置数据安装在 /var/opt/SUNWmsgsr 中。

我们为逻辑主机名 budgie 指定了逻辑 IP 地址。例如，/etc/hosts 文件可能如下所示：

```
192.18.75.157 budgie.red.siroe.com budgie
```

1 **在两个节点上安装 Messaging Sun Cluster 代理 (SUNWscims)。**

2 **创建文件系统。**

在本示例中，文件系统 /var/opt/SUNWmsgsr 安装在共享磁盘上。此文件系统可以是群集文件系统，也可以是本地文件系统（故障转移文件系统）。

3 **配置主节点 (daisy)。**

a. **在主节点上添加所需的资源类型。**

此操作配置 Sun Cluster 以了解要使用的资源类型。要注册 Messaging Server 和 HAStoragePlus 资源，请使用以下命令：

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

b. **为名为 MS_RG_DAISY 的 Messaging Server 实例创建资源组。**

```
# scrgadm -a -g MS_RG_daisy -h daisy,lavender
```

c. **创建名为 meadow 的逻辑主机名资源、将其添加到资源组中并使其联机。**

```
# scrgadm -a -L -g MS_RG_DAISY -l meadow
# scrgadm -c -j meadow -y R_description="LogicalHostname resource for meadow"
# scswitch -Z -g MS_RG_DAISY
```

d. **使用以前创建的文件系统创建一个名为 ms-hasp-daisy 的 HAStoragePlus 资源。**

```
# scrgadm -a -j ms-hasp-daisy -g MS_RG_DAISY -t SUNW.HAStoragePlus -x
FileSystemMountPoints ="/var/opt/SUNWmsgsr" -x
AffinityOn=TRUE
```

e. **启用 HAStoragePlus 资源：**

```
# scswitch -e -j ms-hasp-daisy
```

4 **在主节点上安装并配置 Messaging Server（请参见第 49 页中的“ 1.3 创建初始 Messaging Server 运行时配置 ”）。**

初始运行时配置程序要求输入全限定主机名。输入逻辑主机名 meadow.red.siroe.com。该程序还要求指定配置目录。输入 /var/opt/SUNWmsgsr。

5 **在主节点上运行 ha_ip_config 脚本，并提供逻辑 IP 地址。**

此脚本仅在主节点上运行，而不在辅助节点上运行。ha_ip_config 脚本位于 sbin 目录下的安装目录中。例如：

```
# /opt/SUNWmsgsr/sbin/ha_ip_config

Please specify the IP address assigned to the HA logical host name.
```

```
Use dotted decimal form, a.b.c.d

Logical IP address: 192.18.75.155
# This value is the logical IP address of the logical hostname. Refer
# to the /etc/hosts file.
Please specify the path to the top level directory in which iMS is
installed.

iMS server root: /opt/SUNWmsgsr

. . .

Updating the file /opt/SUNWmsgsr/config/dispatcher.cnf
Updating the file /opt/SUNWmsgsr/config/job_controller.cnf
Setting the service.listenaddr configutil parameter
Setting the local.snmp.listenaddr configutil parameter
Setting the service.http.smtphost configutil parameter
Setting the local.watcher.enable configutil parameter
Setting the local.autorestart configutil parameter
Setting the metermaid.config.bindaddr configutil parameters
Setting the metermaid.config.serveraddr configutil parameters
Setting the local.ens.port parameter
Configuration successfully updated
```

6 **修改 `imta.cnf` 文件，并用 HA 逻辑主机名 (`meadow`) 替换出现的所有物理主机名 (`daisy`)。**

7 **将资源组故障转移到辅助节点 (`lavender`)。**

进行故障转移后，您将随后配置辅助节点 (`lavender`)。

```
# scswitch -z -g MS_RG_LAVENDER -h daisy
```

8 **在辅助节点 (`lavender`) 上安装 Messaging Server，然后运行 `useconfig` 实用程序。请参见 第 74 页中的“ 3.3.3 使用 useconfig 实用程序 ”**

您不必运行初始运行时配置程序 (`configure`)。

在以下示例中，`/var/opt/SUNWmsgsr` 是共享配置目录。

```
# useconfig /var/opt/SUNWmsgsr/setup/configure_20061201124116
cp /var/opt/SUNWmsgsr/setup/configure_20061201124116/Devsetup.properties
/opt/SUNWmsgsr/lib/config-templates/Devsetup.properties
/usr/sbin/groupadd mail
/usr/sbin/useradd -g mail -d / mailsrv
/usr/sbin/usermod -G mail mailsrv
sed -e "s/local.serveruid/mailsrv/" -e "s/local.serveruid/mail/" -e "s:<msg·RootPath>:/opt/SUNWmsgsr:"
/opt/SUNWmsgsr/lib/config-templates/devtypes.txt.template >
/opt/SUNWmsgsr/lib/config-templates/devtypes.txt
sed -e "s/local.serveruid/mailsrv/" -e "s/local.serveruid/mail/" -e
"s:<msg·RootPath>:/opt/SUNWmsgsr:"
/opt//SUNWmsgsr/lib/config-templates/config.ins.template >
```

```
/opt/SUNWmsgsr/lib/config-templates/config.ins
/opt/SUNWmsgsr/lib/devinstall -l sepadmsvr:pkgcfg:config -v -m -i
/opt/SUNWmsgsr/lib/config-templates/config.ins
/opt/SUNWmsgsr/lib/config-templates
/opt/SUNWmsgsr/lib/jars /opt/SUNWmsgsr/lib
devinstall returned 0
crle -c /var/ld/ld.config -s
 /usr/lib/secure:/opt/SUNWmsgsr/lib:/opt/SUNWmsgsr/lib:/opt/SUNWmsgsr/lib
-s /opt/SUNWmsgsr/lib
See /opt/SUNWmsgsr/install/useconfiglog_20061211155037 for more details
```

9 创建 HA Messaging Server 资源并将其启用。

```
# scrgadm -a -j ms-rs-daisy -t SUNW.ims -g MS_RG_DAISY -x IMS_serverroot
=/opt/SUNWmsgsr -y Resource_dependencies=meadow,ms-hasp-daisy
# scswitch -e -j mail-rs-daisy
```

以上命令为 Messaging Server 创建一个名为 `ms-rs-daisy` 的 HAMessaging Server 资源，它将安装在 `/opt/SUNWmsgsr` 上。此 HAMessaging Server 资源依赖于 HA 磁盘资源，即，以前创建的文件系统以及 HA 逻辑主机名 `meadow`。

10 确保所有功能均正常工作。

将 Messaging Server 资源故障转移回主节点。

```
 # scswitch -z -g MAIL-RG -h daisy
```

3.4.3.1 如何在 Sun Cluster 上启用调试

Messaging Server Data Service Sun Cluster 代理使用两个 API 来记录调试消息：

`scds_syslog_debug()` 将调试消息写入到级别为 1 的系统日志中。

`scds_syslog()` 将消息写入到级别为 `daemon.notice`、`daemon.info` 和 `daemon.error` 的系统日志中。

所有 `syslog` 消息都带有以下前缀：

`SC[`*resourceTypeName*，*resourceGroupName*，*resourceName*，*methodName*`]`

例如：

```
Dec 11 18:24:46 mars SC[SUNW.ims,MS-RG,mail-rs,ims_svc_start]: [ID 831728daemon.debug]
Groupname mail exists.
Dec 11 18:24:46 mars SC[SUNW.ims,MS-RG,mail-rs,ims_svc_start]: [ID 383726daemon.debug]
Username mailsrv exists.
Dec 11 18:24:46 mars SC[SUNW.ims,MS-RG,mail-rs,ims_svc_start]: [ID 244341daemon.debug]
IMS_serverroot = /opt/mars/SUNWmsgsr
Dec 11 15:55:52 mars SC[SUNW.ims,MS_RG,MessagingResource,ims_svc_validate]:
[ID 855581daemon.error] Failed to get the configuration info
```

```
Dec 11 18:24:46 mars SC[SUNW.ims,MS-RG,mail-rs,ims_svc_start]: [ID 833212daemon.info]
Attempting to start the data service under process monitor facility.
```

要记录来自 Messaging Server 资源类型 SUNW.ims 的消息，请在 /var/cluster 下面创建资源类型目录，如下所示：

```
mkdir -p /var/cluster/rgm/rt/SUNW.ims
```

要查看资源类型 SUNW.ims 的所有调试消息，请在所有群集节点上发出以下命令：

```
echo 9 > /var/cluster/rgm/rt/SUNW.ims/loglevel
```

要禁止资源类型 SUNW.iws 的调试消息，请在所有群集节点上发出以下命令：

```
echo 0 > /var/cluster/rgm/rt/SUNW.ims/loglevel
```

要记录来自 Sun Cluster 数据服务的调试消息以及来自 Messaging Server Agents 的最常见调试信息，请编辑 syslog.conf 文件。例如，要将所有 syslog 消息记录到文件 /var/adm/clusterlog 中，请将以下行添加到 syslog.conf 文件中：

```
daemon.debug /var/adm/clusterlog
```

这将在以下级别记录所有消息：emerg、alert、critical、error、warning、notice、information、debug。有关详细信息，请参见 syslog.conf 主页

立即重新启动 syslogd 守护进程：

```
pkill -HUP syslogd
```

3.4.4 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服务所必需的。

将 Messaging Server 配置为具有 HA 的部分工作包括配置 Messaging Server 绑定和侦听连接所在的接口地址。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：

▼ 在服务器上绑定 IP 地址

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。键入 control-d 可以中止正在处理问题的本脚本。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 Messaging Server 将使用的逻辑主机名的 IP 地址。必须将 IP 地址指定为点分十进制数字形式，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服务系统。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 基本目录 (*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 "no" 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 "yes"。**

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服务器的运行状况。进程故障和未响应的服务将产生反映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 105 页中的 “4.5 失败的服务或未响应服务的自动重新启动”。

3.4.5 有助于管理 Messaging HA 的 Sun Cluster 命令

要启用 Messaging Server 资源，请使用以下命令：

```
# scswitch -e -j messaging-resource
```

要禁用 Messaging Server 资源，请使用以下命令：

```
# scswitch -n -j cal-resource
```

要列出所有资源和资源组，请使用以下命令：

```
# scstat -pvv
```

要确定进程监视工具 (PMF) 标记（即，PMF 监视的进程），请使用以下命令：

```
# pmfadm -L
```

要列出所有资源和资源组及其状态，请使用以下命令：

```
# scstat -g
```

要管理 Sun Cluster，请使用以下命令：

```
scsetup
```

3.5 Veritas Cluster Server 代理安装

可以使用 Veritas Cluster Server 3.5、4.0、4.1 和 5.0 配置 Messaging Server。

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

使用 Communications Suite 安装程序安装 Messaging Server 并配置 HA 之后，请确保查阅第 91 页中的 “3.4.4 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。本节包含以下小节：

3.5.1 Veritas Cluster Server 的要求

- 已经在两个节点上安装和配置了 Veritas Cluster 软件和 Messaging Server 软件，如以下说明（第 94 页中的 “3.5.2 VCS 3.5 安装和配置说明”）中所述。

3.5.2 VCS 3.5 安装和配置说明

以下说明介绍了如何使用 Veritas Cluster Server 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。

▼ 使用 Veritas Cluster Server 将 Messaging Server 配置为 HA 服务

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 **使用 Cluster Explorer，添加一个名为 `MAIL-RG` 的服务组。**

3 **向服务组 `MAIL-RG` 添加 `DiskGroup` 类型的 `s1ms_dg` 磁盘组资源并启用该资源。**

4 **向服务组 `MAIL-RG` 添加 `Mount` 类型的 `s1ms_mt` 安装资源。**

a. **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。**

5 **在 `s1ms_mt` 和 `s1ms_dg` 之间创建一个链接。启用 `s1ms_mt` 资源。**

下图表示依赖性树：

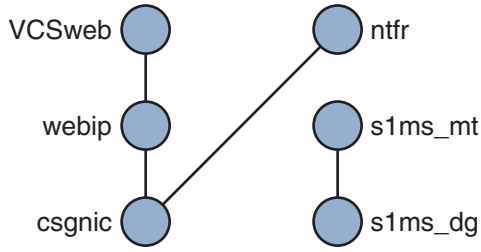


图 3–5 Veritas Cluster Server 依赖性树 1

6 运行 **Communications Suite** 安装程序 安装 **Messaging Server**。

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

b. 使用 `pkgadd`(**1M**) 命令安装 **Veritas Cluster Server** 代理软件包 `SUNWmsgvc`（位于 **Sun Java Communications Suite 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。

7 切换至备份节点（例如，**Node_B**）。

8 运行 **Communications Suite** 安装程序，以在备份节点 (**Node_B**) 上安装 **Messaging Server**。

9 安装 **Messaging Server** 之后，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 74 页中的“ 3.3.3 使用 useconfig 实用程序 ”。

至此，已将 Veritas 代理安装在 Node_B 上。

10 在 **Veritas Cluster Server Cluster Manager** 中，从“ 文件 ”菜单中选择“导入类型...”，系统将显示文件选择框。

11 从 `/etc/VRTSvcs/conf/config` 目录中导入 `MsgSrvTypes.cf` 文件。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。

12 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。

13 `Mail` 资源取决于 `s1ms_mt` 和 `webip`。如以下依赖性树所示，在资源之间创建链接：

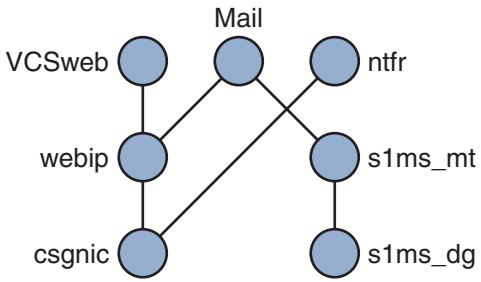


图 3–6 Veritas Cluster 依赖性树

a. **启用所有资源并使 `Mail` 联机。**

b. **应该启动所有的服务器。**

14 **切换至 Node_A 并检查高可用性配置是否正在工作。**

3.5.3 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 3–3。

表 3–3 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。
`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）。

3.6 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 97 页中的 “取消配置 Veritas Cluster Server”

▼ 取消配置 Veritas Cluster Server

本节介绍了如何取消配置 Veritas Cluster Server 的高可用性组件：

1. 使 MAIL-RG 服务组脱机并禁用其资源。
2. 删除 mail 资源、logical_IP 资源和 mountshared 资源之间的依赖性。
3. 使 MAIL-RG 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。

◆ ◆ ◆ 第 4 章

配置一般邮件服务功能

本章介绍了一般 Messaging Server 任务，如使用命令行实用程序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进行介绍。本章包含以下各节：

4.1 修改密码

由于在初始配置期间设置了多个具有相同密码的管理员（请参见第 49 页中的 “1.3 创建初始 Messaging Server 运行时配置”），因此您可能需要更改这些管理员的密码。

请参阅表 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。有关使用 `configutil` 实用程序的参数，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“configutil”以了解完整的语法和用法。

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`	用户/组管理员密码，通过 `configutil` 实用程序设置。
`local.service.pab.ldappasswd`	由绑定 DN 指定的用户进行 PAB 搜索时使用的密码，通过 `configutil` 实用程序设置。
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	这些证书在 LDAP 目录中直接设置（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。 可通过修改 LDAP 目录（使用 `ldapmodify` 命令）或使用 Delegated Administrator UI 来更改 Delegated Administrator 服务管理员的密码。
存储管理员	可通过修改 LDAP 目录（使用 `ldapmodify` 命令）来更改存储管理员的密码。

以下示例使用 `local.enduseradmincred configutil` 参数来更改最终用户管理员的密码。

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

4.2 管理邮件用户，邮件列表和域

所有用户、邮件列表和域信息均作为条目存储在 LDAP 目录中。LDAP 目录可以包含有关组织的员工、成员、客户或以各种方式“隶属于”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件列表包括创建和修改目录中的用户和邮件列表条目。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` 命令将用户标记为已删除。（请参见《Sun Java System Delegated Administrator 6.4 管理指南》中的第 5 章“命令行实用程序”。）**

2. **从用户中删除服务。**

   服务可以为邮箱或日历。对于 Messaging Server 的当前版本，此程序称为 `msuserpurge`。（请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“msuserpurge”。）对于日历服务，此程序称为 `csclean`。（请参见《Sun Java System Calendar Server 6.3 Administration Guide》。）

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` 命令将用户标记为已删除。（请参见《Sun Java System Delegated Administrator 6.4 管理指南》中的第 5 章“命令行实用程序”。）**

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，此程序称为 `msuserpurge`。（请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“msuserpurge”。）对于日历服务，此程序称为 `csclean`。（请参见 *Sun Java System Calendar Server* **管理指南**。）

3. **通过调用 `commadmin domain purge` 命令永久删除域。**

4.3 通过 Sun ONE Console 管理 Messaging Server

Messaging Server 中不再支持 Sun ONE Administration Console。请使用等效命令行界面。

4.4 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。

4.4.1 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，没有特定的 HA 命令单独用于启动、重新启动或停止其他 Messaging Server 服务（例如 SMTP）。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 的最佳粒度是单个资源。由于 Messaging Server 对于 Sun Cluster 来说是一种资源，因此 `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 3.5、4.0、4.1 和 5.0 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*

4.4.2 在非 HA 环境中启动和停止服务

使用命令 *msg-svr-base*`/sbin/start-msg` 和 *msg-svr-base*`/sbin/stop-msg` 从命令行启动和停止服务。虽然可以使用命令模板 *msg-svr-base*`/sbin/stop-msg` *service*（其中，service 可以为 `smtp`、`imap`、`pop`、`store`、`http`、`ens` 或 `sched`）分别启动和停止服务，但建议不要这样做（本手册中所述的特殊任务除外）。某些服务依赖于其他服务，并且必须按指定的顺序进行启动。尝试单独启动服务时，情况可能会比较复杂。为此，应使用 `start-msg` 和 `stop-msg` 命令同时启动和停止所有服务。

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 116 页中的 “5.1.1 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 105 页中的 “4.5 失败的服务或未响应服务的自动重新启动”），则当任何服务器进程崩溃时，均应停止所有进程，然后重新启动所有进程。这包括 POP、IMAP、HTTP 和 MTA 进程，以及 `stored`（消息存储）进程和用于修改消息存储的任何实用程序（例如 `mboxutil`、`deliver`、`reconstruct`、`readership` 或 `upgrade`）。

▼ 启动、关闭或查看任何邮件传送服务的状态

再次提醒您，建议不要关闭各个服务，本手册的各个部分中所述的特殊任务除外。某些服务依赖于其他服务，并且必须按指定的顺序进行启动。尝试单独启动服务时，情况可能会比较复杂。为此，应使用 `start-msg` 和 `stop-msg` 命令同时启动和停止所有服务。

- **请使用 `start-msg` 和 `stop-msg` 命令启动或停止任何邮件传送服务。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`

  必须启用了服务才能停止或启动服务。请参见第 103 页中的 “4.4.2.1 指定可以启动的服务”。

注 – `start-msg` 和 `stop-msg` 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《Sun Java System Messaging Server 6.3 Administration Reference》中的“start-msg”和《Sun Java System Messaging Server 6.3 Administration Reference》中的“stop-msg”。

4.4.2.1 指定可以启动的服务

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`、`loc` 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更多信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“configutil Parameters”。

4.4.3 启动和停止以 MTA-only 模式运行的 Messaging Server

要启动 MTA-only 系统，您还应该启动 `imsched`。执行该操作前，应该先删除不利于安装的计划任务。

`imsched` 是一个单独的 Messaging Server 组件，如果没有启动 Messaging Server 的所有项目，则必须单独启用该组件。如果您使用 `start-msg imta` 或 `start-msg smtp` 启用 MTA-only 系统，将不会运行 `imsched` 进程。

如果仅以 MTA 模式运行 Messaging Server（不运行 store/imap/pop/http 进程），则您可以选择仅在初始安装 (*msg_base*/sbin/configure) 后配置 Messaging Server 期间安装/配置的 MTA，或者使用以下 `configutil` 命令手动禁用消息存储和 `mshttp` 进程：

```
./configutil -o local.store.enable -v 0
./configutil -o service.http.enable -v 0
```

禁用 http 和其他存储进程后，可以通过运行以下命令启动 Messaging Server：

```
# ./start-msg
bash-3.00# ./start-msg
Connecting to watcher ...
Launching watcher ... 4034
Starting ens server ... 4035
Starting sched server ... 4036
Starting dispatcher server .... 4038
Starting job_controller server .... 4042
```

请注意，这将启动所有相应的进程，包括 `imsched` 和 `imta`。这样客户则无需启动 `sched` 进程。

4.5 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，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 监视服务器的崩溃情况。msprobe 通过检查响应时间监视服务器的挂起情况。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 显示了每个实用程序监视的服务。

表 4–4 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、消息存储 (stored)、imsched、MMP。（LMTP/SMTP 服务器由分发程序监视，LMTP/SMTP 客户端由 job_controller 监视。）	IMAP、POP、HTTP、证书、作业控制器、消息存储 (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 日志文件中以指明特定的故障。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，此参数设置为 no。

如果任何消息存储服务失败或冻结，则启动时启用的所有消息存储服务都将重新启动。例如，如果 imapd 失败，则至少 stored 和 imapd 将重新启动。如果其他消息存储服务（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。

如果某个消息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消息存储服务器。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（可使用 local.autorestart.timeout 进行配置）最多可重新启动服务和进程两次。

无论 local.autorestart 是否设置为 yes，系统仍将监视服务并向控制台发送失败或未响应的错误消息，并且默认情况下，*msg-svr-base*/data/log/watcher 将侦听端口 49994，但是可以使用 local.watcher.port 对此进行配置。

Watcher 日志文件是在 *msg-svr-base*/data/log/watcher 中生成的。此日志文件不是由日志系统管理的（不进行回滚或清理），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更多信息，请参见第 789 页中的 “27.8.9 使用 msprobe 和 watcher 功能进行监视”。

msprobe 由 imsched 控制。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，偶尔发生 imsched 挂起时，您需要使用 kill *imsched_pid* 中止 imsched，以使 watcher 重新启动 imsched。

4.5.1 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	在 start-msg 启动时启用 watcher。默认值为 yes。
local.autorestart	启用失败或冻结（未响应）的服务器的自动重新启动，其中包括 IMAP、POP、HTTP、作业控制器、分发程序和 MMP 服务器。默认值为 No。
local.autorestart.timeout	失败重试超时。如果服务器在此指定时间段内失败超过两次，则系统将停止尝试重新启动此服务器。如果这种情况发生在 HA 系统中，则将关闭 Messaging Server 并向另一个系统进行故障转移。应该将该值（以秒为单位设置）设置为比 msprobe 间隔长的时间段值。（请参见下面的 local.schedule.msprobe。）默认值为 600。
local.schedule.msprobe	msprobe 运行计划。crontab 样式的计划字符串（请参见表 20–10）。默认值为 5,15,25,35,45,55 * * * * lib/msprobe 要进行禁用：请将 local.schedule.msprobe.enable 设置为 NO。

4.6 安排自动任务时间

Messaging Server 提供了一般任务调度机制，该机制使用名为 imsched 的进程。它用于调度 Messaging Server 进程。可以通过设置 local.schedule.*taskname* configutil 参数来启用此功能。如果要修改计划，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/计划组合的唯一名称。

schedule 的格式如下：

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。路径可以是相对于 *msg-svr-base* 的路径，也可以是绝对路径。有关相对路径的示例，请参见第 108 页中的“4.6.2 预定义的自动任务”。

minute hour day-of-month month-of-year day-of-week 是运行命令的计划。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 代表星期天）。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 17 号和星期二，则仅在某月的 17 号是星期二时才会运行命令。请参见表 20–10。

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，或者刷新调度程序进程：

```
refresh sched
```

要禁用调度的任务，请运行以下命令：

```
# configutil -o local.schedule.taskname.enable -v no
#  refresh sched
```

4.6.1 调度程序示例

在 12:30am、8:30am 和 4:30pm 运行 imexpire：

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

每 20 分钟显示一次 MTA 通道队列邮件计数器：

```
# configutil -o local.schedule.counters -v "0,20,40 * * * * /opt/SUNWmsgsr/sbin/ims
# imta qm counters > /tmp/temp.txt"
```

从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"
```

4.6.2 预定义的自动任务

在安装时，Messaging Server 将创建、调度并启用一组预定义的自动任务。这些任务如下所示。

为消息存储设置并启用了以下自动任务：

```
local.schedule.expire = "0 23 * * * sbin/imexpire"
local.schedule.expire.enable = 1
local.schedule.snapshotverify = "0 0,4,8,12,16,20 * * * sbin/imdbverify -m"
local.schedule.snapshotverify.enable = 1
```

为 MTA 设置并启用了以下自动任务：

```
local.schedule.purge="0 0,4,8,12,16,20 * * * sbin/imsimta purge -num=5"
local.schedule.purge.enable = 1
local.schedule.return_job = "30 0 * * * lib/return_job"
local.schedule.return_job.enable = 1
```

为消息存储设置并启用了以下自动任务：

```
local.schedule.msprobe = "5,15,25,35,45,55 * * * * lib/msprobe"
local.schedule.msprobe.enable = 1
```

4.7 配置问候邮件

可以使用 Messaging Server 创建问候电子邮件以发送给每个新用户。

▼ 创建新用户问候

- **要创建新用户问候，请使用以下命令行：**

  `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），之后是 $$，然后是邮件正文。$ 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 $ 不再具有特殊含义（取决于所使用的 shell）。（$ 通常是 shell 的转义符。）

4.7.1 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。根据用户、域或站点的首选语言，问候邮件可有所不同。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
- 用户的首选语言为法语，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
- 站点语言为英语，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`)。

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，则将收到英语问候。

4.7.1.1 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，但没有针对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（如果已指定该参数）。如果用户设置了首选语言（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 siroe.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。以下值均可用（`mailDomainWelcomeMessage` 是域 siroe.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`。

4.8 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，除非它响应的外来邮件在邮件标题中指定了首选语言。标题字段（`Accept-Language`、`Preferred-Language` 或 `X-Accept-Language`）是根据在用户的邮件客户端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端中指定的首选语言），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）。

4.8.1 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。

▼ 指定站点语言

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。

- **命令行：按照以下方式指定站点语言：**

  `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《Sun Java System Directory Server 5 2005Q1 Administration Guide》的第 5 章。

4.9 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 需要访问目录以用于多种用途。例如：

- 创建或更新邮件用户或邮件组的帐户信息时，这些信息将存储在某个目录中，此目录称为**用户目录**。
- 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。
- 验证用户以进行邮件路由查找。

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。

▼ 修改 Messaging Server LDAP 用户查找设置

- **用于用户目录连接设置的命令如下所示，但是，请先按照以下方式设置 LDAP 和 PAB 密码：**

- 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。
- 如果将同一帐户用于在属性 `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 ]
```

主机名是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。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]
```

端口号是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)。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
```

基 DN是搜索基准—即表示用户查找起点的目录条目的标识名。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。要指定用于用户查找的 LDAP 基 DN，请运行以下命令：

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

绑定 DN是 Messaging Server 连接到目录服务器以进行查找时用于表示自身的标识符。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）的标识符。如果目录允许匿名搜索访问，则可以将此条目保留为空白。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
```

4.10 加密设置

第 650 页中的 “23.5.2 启用 SSL 并选择加密算法” 中对其进行了说明，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。

4.11 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：

▼ 设置故障转移 LDAP 服务器

1 **将 `local.ugldaphost` 设置为多台 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。

◆ ◆ ◆ 第 5 章

5 配置 POP、IMAP 和 HTTP 服务

Messaging Server 支持客户端使用邮局协议 3 (Post Office Protocol 3, POP3)、Internet 邮件访问协议 4 (Internet Mail Access Protocol 4, IMAP4) 和超文本传输协议 (HyperText Transfer Protocol, HTTP) 访问邮箱。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，其中的浏览器是运行在使用 HTTP 与 Internet 连接的计算机系统中。

本章介绍如何使用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 (Simple Mail Transfer Protocol, SMTP) 服务的信息，请参见第 10 章。

本章包含以下各节：

5.1 一般配置

Messaging Server POP、IMAP 和 HTTP 服务的配置包括启用或禁用服务、指定端口号和修改发送给连接客户端的服务标题（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 122 页中的 “5.5 配置 POP 服务”、第 123 页中的 “5.6 配置 IMAP 服务”和第 127 页中的 “5.7 配置 HTTP 服务”。本节包含以下几个部分：

- 第 117 页中的 “5.1.4 服务标题”

5.1.1 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 102 页中的 “4.4 启动和停止服务”）；要使 POP、IMAP 或 HTTP 发挥作用，必须将其启用并启动。

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 (Message Transfer Agent, 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 103 页中的 “4.4.2.1 指定可以启动的服务” 也对此过程进行了介绍。您还可以通过设置 LDAP 属性 `mailAllowedServiceAccess` 在用户级别启用或禁用服务。

5.1.2 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。）

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未为其他服务所保留。

5.1.3 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 客户端进行加密通信。有关 Messaging Server 支持 SSL 的一般信息，请参见第 640 页中的 “23.5 配置加密和基于证书的验证”。

5.1.3.1 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 客户端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。在同一端口上既使用 IMAP 又使用基于 SSL 的 IMAP 进行通信是刚刚出现的标准；只要 Messaging Server 已安装 SSL 证书（请参见第 641 页中的 “23.5.1 获得证书”），Messaging Server 便可以支持在同一端口上使用基于 SSL 的 IMAP。

5.1.3.2 基于 SSL 的 POP

默认的基于 SSL 的单独 POP 端口为 995。您也可以使用命令 "STLS" 启动基于 SSL 的普通 POP 端口（请参见第 122 页中的 “5.5 配置 POP 服务”）。

5.1.3.3 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。

5.1.4 服务标题

客户端首次连接到 Messaging Server POP 或 IMAP 端口时，服务器将向该客户端发送标识文本字符串。此服务标题（通常不向客户端用户显示）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端调试或问题隔离。

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

请使用 `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 6.3 Administration Reference》。

5.2 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）。本节提供了背景信息；有关完成这些设置所需的步骤，请参见第 122 页中的 “5.5 配置 POP 服务”、第 123 页中的 “5.6 配置 IMAP 服务”或第 127 页中的 “5.7 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。本节包含以下几个部分：

- 第 119 页中的 “5.2.3 基于证书的登录”

▼ 设置 POP 客户端的登录分隔符

某些邮件客户端不接受 @ 作为 登录分隔符（即，类似 uid@domain 地址中的 @）。这些客户端包括 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 客户端用户，登录时应将 + （而不是 @）作为登录分隔符。**

5.2.1 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，如果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，请参见《Sun Java System Messaging Server 6.3 Administration Reference》。

5.2.2 基于密码的登录

在典型的邮件服务安装中，用户通过在其 POP、IMAP 或 HTTP 邮箱客户端中输入密码来访问邮箱。。客户端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，或根据客户端策略对其加密。
- 如果选择非零值，则客户端将与服务器建立 SSL 会话（使用其密钥长度不小于指 定值的加密算法），从而加密客户端发送的所有 IMAP 或 HTTP 用户密码。

如果将客户端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端支持的长度，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 650 页中的 “23.5.2 启用 SSL 并选择加密算法”。

5.2.3 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。客户端与服务器建立 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 以使基于证书的用户可以登录到 IMAP 或 HTTP 服务的说明，请参见第 652 页中的 “23.5.3 设置基于证书的登录”。

如果您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，如果客户端建立 SSL 会话并提供证书，将使用基于证书的登录。如果客户端不使用 SSL 或不提供客户端证书，它将发送密码。

5.3 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。本节提供了背景信息；有关完成这些设置所需的步骤，请参见第 122 页中的 “5.5 配置 POP 服务”、第 123 页中的 “5.6 配置 IMAP 服务”或第 127 页中的 “5.7 配置 HTTP 服务”。本节包含以下几个部分：

5.3.1 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。

注释：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。

5.3.2 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端连接越多，对客户端就越有利。如果客户端由于无可用连接而被拒绝服务，则必需等到其他客户端断开连接。

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。每次进行 POP 重新连接时，都要求重新验证用户。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 会话的安全性的更多信息，请参见第 634 页中的 “23.2 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。

5.3.3 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。服务器使用线程极大地提高了执行效率，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端请求，以便为更多的客户端提供快速服务。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。

5.3.4 切断空闲连接

为了收回无响应客户端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 会话安全性的更多信息，请参见第 634 页中的 “23.2 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）致使客户端无法响应而造成的。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 客户端通常在小于 30 分钟的某个时间间隔内向 IMAP 服务器定期发送命令。

5.3.5 注销 HTTP 客户端

HTTP 会话可以持续多个连接。切断连接后并不注销 HTTP 客户端。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 会话并注销客户端（默认时间段是 2 小时）。切断会话后，客户端的会话 ID 将无效，客户端必须重新验证才能建立其他会话。有关 HTTP 安全性和会话 ID 的更多信息，请参见第 634 页中的 “23.2 关于 HTTP 安全性”。

5.4 客户端访问控制

Messaging Server 包含访问控制功能，使您可以决定哪些客户端可以访问 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端的访问。

客户端访问控制是 Messaging Server 重要的安全保护功能。有关创建客户端访问控制过滤器的信息及其使用示例，请参见第 655 页中的 “23.7 配置客户端对 POP、IMAP 和 HTTP 服务的访问”和第 666 页中的 “23.9 配置客户端对 SMTP 服务的访问”。

5.5 配置 POP 服务

您可以通过使用 `configutil` 命令对 Messaging Server POP 服务执行基本配置。本节介绍了一些比较常用的 POP 服务选项。在《Sun Java System Messaging Server 6.3 Administration Reference》中的“configutil Parameters”中可以查看完整的列表。

注 – 对于 POP 服务，将自动启用基于密码的登录。

有关详细信息，另请参见：

- 第 116 页中的 “5.1.1 启用和禁用服务”
- 第 118 页中的 “设置 POP 客户端的登录分隔符”
- 第 116 页中的 “5.1.2 指定端口号”
- 第 120 页中的 “5.3.2 每个进程的连接数量”
- 第 121 页中的 “5.3.4 切断空闲连接”
- 第 121 页中的 “5.3.3 每个进程的线程数量”
- 第 120 页中的 “5.3.1 进程数量”

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（有关详细信息，请参见第 120 页中的 “5.3.2 每个进程的连接数量”）：

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

设置连接的最大空闲时间（有关详细信息，请参见第 121 页中的 “5.3.4 切断空闲连接”）：

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

设置每个进程的最大线程数量（有关更多信息，请参见第 121 页中的 “5.3.3 每个进程的线程数量”）：

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

设置最大进程数量（有关其他信息，请参见第 120 页中的 “5.3.1 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
```

如果已正确配置 SSL，则还支持 TLS。

指定协议欢迎标题：

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

5.6 配置 IMAP 服务

您可以使用 `configutil` 命令对 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 6.3 Administration Reference》中的第 3 章 “Messaging Server Configuration”中可以查看完整的列表。有关详细信息，另请参见：

- 第 116 页中的 “5.1.1 启用和禁用服务”
- 第 116 页中的 “5.1.2 指定端口号”
- 第 118 页中的 “5.2.2 基于密码的登录”
- 第 120 页中的 “5.3.2 每个进程的连接数量”
- 第 121 页中的 “5.3.4 切断空闲连接”
- 第 121 页中的 “5.3.3 每个进程的线程数量”
- 第 120 页中的 “5.3.1 进程数量”
- 第 124 页中的 “5.6.1 配置 IMAP IDLE”

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
```

如果 *value* 大于 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端上启用 SSL 或 TLS，以防止在网络中泄露其密码。默认值为 0。

设置每个进程的最大网络连接数量（有关其他信息，请参见第 120 页中的 “5.3.2 每个进程的连接数量”）：

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

设置连接的最大空闲时间（有关其他信息，请参见第 121 页中的 “5.3.4 切断空闲连接”）：

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

设置每个进程的最大线程数量（请参见第 121 页中的 “5.3.3 每个进程的线程数量”）：

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

设置最大进程数量（请参见第 120 页中的 “5.3.1 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
```

5.6.1 配置 IMAP IDLE

IMAP 规范的 IMAP IDLE 扩展（在 RFC 2177 中定义） 允许 IMAP 服务器在新邮件到达时和在用户邮箱中进行其他更新时通知邮件客户端。IMAP IDLE 功能具有以下优点：

- 邮件客户端不必向 IMAP 服务器轮询外来邮件。

取消客户端轮询可减少 IMAP 服务器上的工作负荷并提高服务器性能。当用户没有收到任何邮件或只收到很少的邮件时，客户端轮询非常浪费资源；客户端将继续按配置的时间间隔进行轮询，通常为每 5 或 10 分钟轮询一次。

- 邮件客户端向用户显示新邮件的时间与实际到达用户邮箱的时间非常接近。它还会以近乎实时的方式显示邮件的状态变化。

  IMAP 服务器不必等待下一封 IMAP 轮询邮件，即可向客户端通知新邮件或更新邮件。只要有新的邮件到达或邮件状态发生更改，IMAP 服务器就会立即收到通知。服务器随后通过 IMAP 协议通知客户端。

5.6.1.1 先决条件

IMAP IDLE 功能依赖于事件通知服务 (Event Notification Service, ENS) 来传播通知。要使用 IMAP IDLE，您必须配置以下 ENS 组件：

- 至少一个主机上的 `enpd` 服务器
- 所有消息存储主机上的 `IBiff` 通知插件

有关为 Messaging Server 配置 ENS 的信息，请参见Sun Java System Communications Services Event Notification Service Guide。

有关配置 `IBiff` 通知插件的信息，请参见第 811 页中的 “B.1 在 Messaging Server 中装入 ENS Publisher”。

▼ 配置 IMAP IDLE

1 **将 enpd 服务器配置为仅接受来自运行消息存储的主机的连接。**

要限制到消息存储主机的连接，请设置 `ENS_ACCESS` 环境变量。该环境变量设置允许访问 `enpd` 的权限列表。语法如下：

```
setenv ENS_ACCESS 'allowdeny ipaddress|mask;
allowdeny ipaddress|mask; ...'
```

其中

allowdeny 可以为 + （指定允许）或 — （指定拒绝）

ipaddress 指定点分十进制 IP 地址

mask 指定点分十进制 IP 地址掩码

示例：

以下示例仅允许访问本地主机：

```
setenv ENS_ACCESS '+127.0.0.1|255.255.255.255'
```

以下示例允许访问本地主机和所有 IP 地址 192.168.0.*，但 192.168.0.17 除外：

```
setenv ENS_ACCESS '+192.168.0.1|255.255.255.0;+127.0.0.1|255.255.255.255; \
-192.168.0.17;255.255.255.255'
```

2 运行 configutil 实用程序，以指定运行 ENS 服务器的主机的名称。

```
cd msg-svr-base
./configutil -o local.store.notifyplugin.enshost -v "ipaddress"
```

其中，*ipaddress* 指定了 ENS 主机的点分十进制 IP 地址。

示例：

```
cd msg-svr-base
./configutil -o local.store.notifyplugin.enshost -v "127.0.0.1"
```

3 指定用于通知的事件密钥。

如果将 ENS 事件密钥 (ensEventKey) 设置为默认值，则 IMAP IDLE 无法运行。

您必须将 ensEventKey 值配置为以 %M 结尾。字符串 %M 是替换代码，它将被替换为发生事件的邮箱的名称。

运行以下 configutil 命令：

```
./configutil -o local.store.notifyplugin.enseventkey -v "eventkey"
```

其中，*eventkey* 是 ENS 使用的唯一标识符。其默认值为 enp://127.0.0.1/store。事件密钥的主机名部分不用于确定运行 ENS 的主机；它只是标识符的一部分。

示例：

```
./configutil -o local.store.notifyplugin.enseventkey -v "enp://127.0.0.1/store/%M"
```

4 加载 libibiff 通知插件文件，它将启用 Messaging Server 的 ENS Publisher。

运行以下 configutil 命令：

```
./configutil -o local.store.notifyplugin -v "msg-svr-base/lib/libibiff"
```

5 允许从所有用户邮箱发送通知，而不仅仅是收件箱。

默认情况下，仅收件箱中发生的事件生成通知。但是，IMAP IDLE RFC (2177) 规定当任何邮箱中发生事件时 IDLE 都必须通知客户端。

为了满足 RFC 的要求，IMAP IDLE 功能要求为所有邮箱启用通知。如果不启用通知，IMAP 服务器将无法公布 IDLE 功能。

要为所有邮箱配置通知，请将 configutil 命令 noneinbox 的值设置为 1：

```
./configutil -o local.store.notifyplugin.noneinbox.enable -v 1
```

其中，-v 1 启用来自所有邮箱的通知。

6 **停止 Messaging Server，然后重新启动。**

```
cd msg-svr-base/sbin

./stop-msg

./start-msg
```

7 **验证 IMAP 服务现在是否包含 IDLE 功能。使用 telnet 连接到 IMAP 主机和端口。**

```
telnet IMAP_hostname port
```

示例：

```
telnet myhost imap
trying 192.18.01.44 ...
connected to myhost.siroe.com

* OK [CAPABILITY IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS
CHILDREN BINARY UNSELECT SORT LANGUAGE STARTTLS IDLE XSENDER X-NETSCAPE
XSERVERINFO X-SUN-SORT X-SUN-IMAP X-ANNOTATEMORE AUTH=PLAIN]
myhost.siroe.com IMAP4 service (Sun Java(tm) System
Messaging Server 6.3-0.05 (built Feb 7 2006))
```

5.7 配置 HTTP 服务

Messaging Server 支持名为 Messenger Express 和 Communications Express 的 HTTP 邮件客户端。POP 和 IMAP 客户端将邮件直接发送到 Messaging Server MTA 以便进行路由或传送；而 HTTP 客户端将邮件发送到名为 Webmail Server（也称为 mshttpd 或 Messaging Server http 守护进程）的专用 Web 服务器。根据邮件的发送地址，Webmail Server 将邮件定向到出站 MTA 以进行路由，或者定向到使用 IMAP 的一个后端消息存储。如图 5–1 所示。请注意，Communications Express Server 只路由来自或发送到 Webmail Server 的请求。

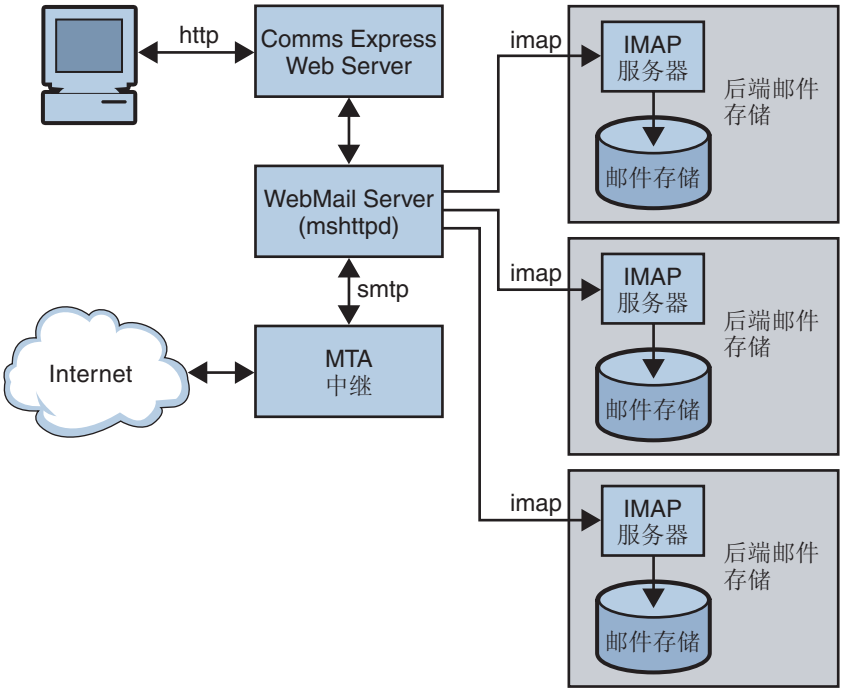


图 5–1 HTTP 服务组件

在以前的版本中，Webmail Server 直接访问消息存储。现在，它通过 IMAP 服务器访问消息存储。这具有很多优点：

- Messenger Express 和 Communications Express 客户端现在能够访问位于不同后端消息存储中的共享文件夹。
- Webmail Server 不必再安装在每个后端服务器上。
- Webmail Server 可以用作前端服务器，执行以前由 Messenger Express Multiplexor (MEM) 执行的多路复用功能。
- MEM 已过时而不再使用。
- 在客户端上，除了用户现在可以访问不在其消息存储中的共享文件夹外，没有进行任何更改。

在以前的版本中，MEM 接收 HTTP 客户端请求，并将其转发到后端消息存储上的相应 Webmail Server。因此，必须在每个后端服务器上安装 mshttpd 副本。现在，Webmail Server 用作接收 HTTP 客户端电子邮件请求的前端服务器。它将这些请求转换为 SMTP 或 IMAP 调用，并将调用转发到 MTA 或后端消息存储上的相应 IMAP 服务器。如果 Messaging Server 仅用于基于 Web 的电子邮件，请确保启用了 IMAP。

5.7.1 配置 HTTP 服务

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 6.3 Administration Reference》中的“configutil Parameters”中可以查看完整的列表。有关详细信息，另请参见：

- 第 116 页中的 “5.1.1 启用和禁用服务”
- 第 116 页中的 “5.1.2 指定端口号”
- 第 118 页中的 “5.2.2 基于密码的登录”
- 第 120 页中的 “5.3.2 每个进程的连接数量”
- 第 121 页中的 “5.3.4 切断空闲连接”
- 第 122 页中的 “5.3.5 注销 HTTP 客户端”
- 第 121 页中的 “5.3.3 每个进程的线程数量”
- 第 120 页中的 “5.3.1 进程数量”

对于用户访问的每个 IMAP 服务器，Webmail Server 需要了解 IMAP 端口、是否使用 SSL 以及用于用户登录的管理员凭证。用于执行此操作的 `configutil` 参数如下所示：

`local.service.proxy.imapport[.`*hostname*`]` — 连接时使用的 IMAP 端口（默认值为 143）。

`local.service.proxy.imapssl` — 启用 SSL（默认值为 no）。

`local.service.proxy.admin[.`*hostname*`]` — 管理员 ID。

`local.service.proxy.adminpass[.`*hostname*`]` — 管理员密码。

可以全局设置这些参数（应用于每个 IMAP 后端服务器），也可以为每个单独的 IMAP 后端服务器进行设置，即在选项名称后面附加后端的全限定域名。

为了使用基于 SSL 的 IMAP，还必须将 mshttpd 配置为 SSL HTTP 服务器，并且 mshttpd 证书数据库必须信任 IMAP 后端的 CA。您必须启用 `service.http.sslusessl`。如果运行 IMAP 的后端消息存储使用的是自签名证书（例如，由 `generate-certDB` 创建的证书），则需要将该证书添加到前端 `mshttpd` 守护进程服务器中。

请注意，如果未设置 `local.service.proxy.admin/pass`，登录将被拒绝，并出现以下错误消息**邮件服务器不可用。管理员，请查看服务器日志以了解详细信息。**并且 http 日志将列出缺少的配置选项。

您可以在命令行中按如下方式设置 IMAP 属性的其他值：

启用或禁用 HTTP 服务：

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

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。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
```

如果 *value* 大于 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端上启用 SSL 或 TLS，以防止在网络中泄露其密码。默认值为 0。

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 120 页中的 “5.3.2 每个进程的连接数量”）：

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

设置连接的最大空闲时间（有关更多信息，请参见第 121 页中的 “5.3.4 切断空闲连接”）：

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

设置客户端会话的最大空闲时间（有关更多信息，请参见第 122 页中的 “5.3.5 注销 HTTP 客户端”）：

```
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
```

HTTP 客户端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。要

指定客户端外发邮件的附件假脱机目录，请使用以下命令。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，参数中 5 兆字节的限制将导致邮件和附件的最大大小为 3.75 兆字节左右。

```
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* 为字节数。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，参数中 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

6 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，它以前称为 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，则用户在 Sun Java System Access Manager 登录屏幕登录后，就可以在其他窗口中访问 Messenger Express，而不必再次登录。同样，如果正确配置了 Sun Java System Calendar Server，则用户在 Sun Java System Access Manager 登录屏幕登录后，就可以在其他窗口中访问其日历，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环技术。使用信任环是实现 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：

6.1 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：

6.1.1 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。

6.1.2 将 Messaging Server 配置为支持 SSO

有四个 `configutil` 参数支持 Messaging Server SSO。在这四个参数中，仅有 `local.webmail.sso.amnamingurl` 参数是为 Messaging Server 启用 SSO 时所必需的。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 为 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`，该参数启用较旧的 SSO 机制。应该将 `local.webmail.sso.enable` 保留为 `off` 或不对其进行设置，否则系统将记录关于缺少配置参数的警告消息，而这些配置参数是旧的 SSO 机制所需的。

您可以使用 `configutil` 命令修改表 6–3 中所示的 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 为 `http://`*server*`/amserver/namingservice`。 默认值：未设置。
local.webmail.sso.amcookiename	Access Manager cookie 名称。默认情况下，Access Manager 将其会话句柄保存在名为 `iPlanetDirectoryPro` 的 cookie 中。如果将 Access Manager 配置为使用其他 cookie 名称，则需要在 Messaging Server 中将该名称配置为此参数，以便在进行单点登录时 Messaging Server 知道要查找的内容。如果 IS 有默认配置，则不能更改默认值。 默认值：`iPlanetDirectoryPro`

表 6–1 Access Manager 单点登录参数 （续）

参数	说明
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，该机制不同于 Messaging Server 的日志机制。其消息记录在 *msg-svr-base*/log 下名为 http_sso 的文件中。默认情况下，仅记录具有 *info* 或更高级别的消息，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，库的消息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。此外，http_sso 日志文件不由通用的 Messaging Server 日志代码管理，且无法清除或轮转此日志文件。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 是中心验证机构，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 客户端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：是

6.1.3 SSO 错误诊断

如果 SSO 有问题，首先应检查 webmail 日志文件 *msg-svr-base*/log/http，以查找错误。提高日志记录级别可能会很有帮助 (configutil -o logfile.http.loglevel -v debug)。如果这样做不起作用，请先检查 *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 仍然有问题，请确保您在登录过程中使用了 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，而浏览器不知道本地服务器名称所使用的域，因此必须在浏览器中使用全限定名称才能使 SSO 工作。

6.2 信任环 SSO（传统）

本节介绍了信任环 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，信任环 SSO 能够提供 Access Manager SSO 目前所没有的某些功能。本节包含以下几个部分：

- 第 136 页中的 “6.2.1 信任环 SSO 概述和定义”
- 第 136 页中的 “6.2.2 信任环 SSO 应用程序”
- 第 137 页中的 “6.2.3 信任环 SSO 限制”

- 第 137 页中的 “6.2.4 信任环 SSO 部署方案示例”
- 第 139 页中的 “6.2.5 设置信任环 SSO”
- 第 143 页中的 “6.2.6 Messenger Express 信任 SSO 配置参数”

6.2.1 信任环 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 和验证的应用程序。也称为**对等** *SSO* **应用程序**。
- **信任环**。信任的应用程序的环。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环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环中，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 环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_prefix-application 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。

6.2.2 信任环 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环中。可位于此信任环内的应用程序包括 Messenger Express、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 互相访问的应用程序。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： 来自：	Calendar Express	Messenger Express	Delegated Administrator
Calendar Express	SSO	SSO	SSO

表 6–2 SSO 互操作性 （续）

到： 来自：	Calendar Express	Messenger Express	Delegated Administrator
Messenger Express	SSO	N/A	SSO
Delegated Administrator	SSO	SSO	N/A

6.2.3 信任环 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 验证 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。

6.2.4 信任环 SSO 部署方案示例

最简单的 SSO 部署方案仅包含 Messenger Express 和 Delegated Administrator。通过在同一计算机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环中）的 Calendar Express，可以创建较复杂的方案。如图 6–1 所示。

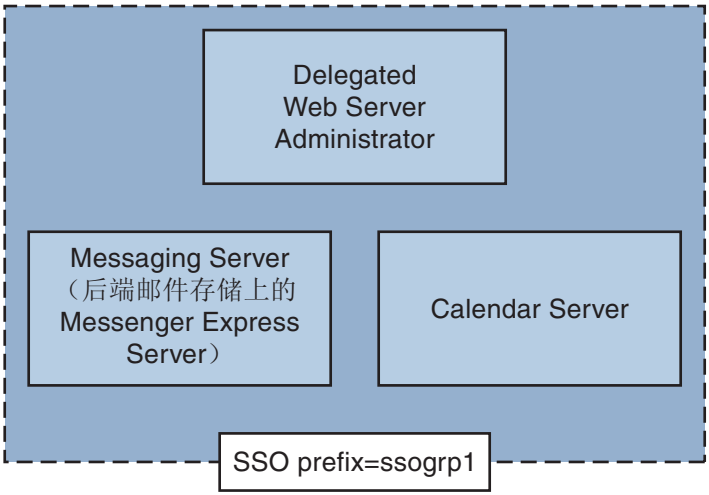


图 6–1 简单 SSO 部署

更复杂的部署将包括 Webmail Server 和负载平衡器。

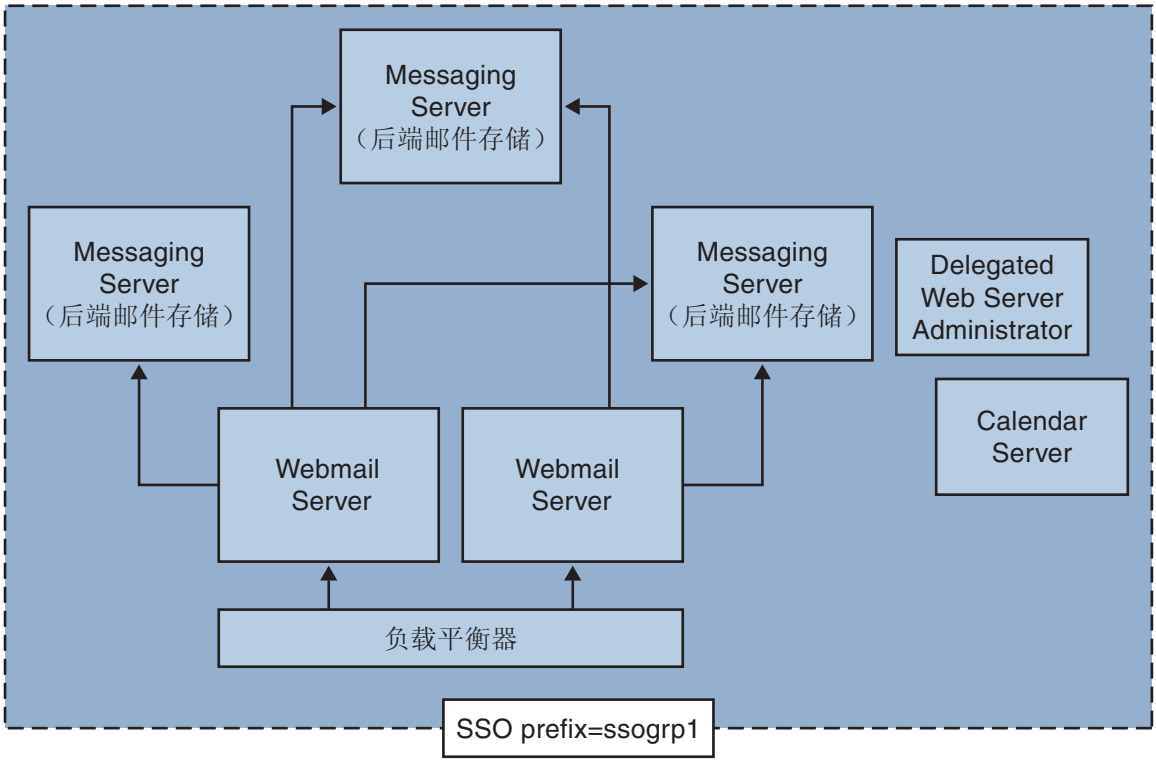


图 6–2 复杂 SSO 部署

6.2.5 设置信任环 SSO

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

▼ 为 Messenger Express、Delegated Administrator 和 Calendar Manager 设置 SSO

1 **配置 Messenger Express 以实现 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（假定默认域为 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 Delegated Administrator 使用的默认 SSO 前缀，尽管您可以选择其他前缀，但使用默认的前缀可以减少配置 Delegated Administrator 和 Calendar Server 时的键入操作。

```
configutil -o local.webmail.sso.id -v ims5
```

ims5 是您选择用于标识 Messenger Express (ME) 以使其区别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/浏览器客户端使用的域匹配，才能连接到服务器。因而，尽管此服务器上的托管域可能称为 `xyz.com`，但我们必须使用 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 是我们给予 SSO 应用程序的名称（例如：对于 Delegated Administrator 为 ida、对于 Calendar Server 为 ics50）。ApplicationHost:port 是应用程序的主机以及端口号。对于每个非 Messaging Server 应用程序，您将具有上述行中的其中一行。示例：

```
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 可以捆绑至 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（默认值为 `o=isp`）。`osiroot` 是组织树的根。

`dcroot`—您输入的用于存储域信息的后缀。（默认值为 `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` 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 的 `resource.properties` 文件。

在 Delegated Administrator `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=cesta.com,o=isp
LDAPDatabaseInterface-ldapauthpw=proxypassword
NDAAuth-singleSignOnId=ssogrp1-
NDAAuth-applicationId=ida
```

`resource.properties` 文件存储在以下位置：

iDA_svr_base`/nda/classes/netscape/nda/servlet/`

b. 添加参与的服务器的验证 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 为 `msg5`。编辑 Delegated Administrator 的 `resource.properties` 文件并添加如下条目：

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

`resource.properties` 文件位于以下目录中：

iDA_svr_base`/nda/classes/netscape/nda/servlet/`

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 `servlets.properties` 文件，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。

`servlets.properties` 文件位于以下目录中：

Web_Svr_Base`/https-`*instancename*`/config/`

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

编辑 Enterprise Server 的 `contexts.properties` 文件，并将以下行添加到文件底部、`#IDACONF-Start` 行之前：

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

`contexts.properties` 文件位于以下目录中：

Web_Svr_Base`/https-`*instancename*`/config/`

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 的 `contexts.properties` 文件中：

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

5 **重新启动 Messenger Express。**

按照步骤 1a 至 2c 中所述更改配置之后，您必须重新启动 Messenger Express 才能使更改生效：

Web_Svr_Base/**https-***instance_name*/**stop**
Web_Svr_Base/**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**

6.2.6 Messenger Express 信任 SSO 配置参数

您可以使用 `configutil` 命令修改 Messenger Express 的单点配置参数，如第 143 页中的“6.2.6 Messenger Express 信任 SSO 配置参数”所示。有关 `configutil` 的更多信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》。

表 6–3 信任环单点登录参数

参数	说明
`local.sso.` *appid*`.verifyurl`	为对等 SSO 应用程序设置验证 URL 值。*appid* 是其 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 的 `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 Webmail Server 和消息存储服务器（运行 Messenger Express）前端或 Calendar 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
`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端提供的 SSO cookie、在成功登录的情况下将 SSO cookie 返回给客户端以及响应来自其他 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。

表 6–3 信任环单点登录参数 （续）

参数	说明
`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 Delegated Administrator 在其 `resource.properties` 文件中所使用的字符串（不带结尾字符 -）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`	如果将此参数的整数值设置为任何非零值，当客户端注销时，将清除客户端（其前缀值与 local.webmail.sso.prefix 中配置的值相匹配）上的所有 SSO cookie。 如果设置为零，则客户端注销时 Messenger Express 将清除自己的 SSO cookie。 默认值为零。

◆ ◆ ◆ 第 7 章

7 配置和管理多路复用器服务

本章介绍了用于标准邮件协议（POP、IMAP 和 SMTP）的 Messaging Multiplexor (MMP)。以前的版本还介绍了用于 Messenger Express Web 接口的 Messenger Express Multiplexor，但已不再需要此项内容。请参见第 127 页中的 “5.7 配置 HTTP 服务”。

本章包含以下主题：

7.1 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 多路复用则内置于消息存储和邮件访问安装所附带的 HTTP 服务 (`mshttpd`) 中。

7.1.1 多路复用器的优点

频繁使用的 Messaging Server 上的消息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。用户与其消息存储之间的间接连接，以及在多个 Messaging Server 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端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、邮箱访问和其他客户端首选项都无需更改。

- **提高了性能**

  如果单个计算机上的消息存储增长到过分大，则可以通过将某些消息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，从而使慢速客户端连接（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端连接，您可以限制外部计算机对内部消息存储计算机的访问。多路复用器支持与客户端的未加密和加密的通信。

7.2 关于 Messaging Multiplexor

Sun Java System Messaging Multiplexor (MMP) 是专用的 Messaging Server，用作与多台后端 Messaging Server 之间的单点连接。使用 Messaging Multiplexor，大规模的邮件传送服务提供商可以将 POP 和 IMAP 用户邮箱分布在多台计算机上，以增大消息存储容量。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 Messaging Server。

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 Messaging Server 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，也可以在以后单独安装 MMP。MMP 支持：

- 与邮件客户端进行未加密和加密的 (SSL) 通信。
- 基于证书的客户端验证，如第 151 页中的 “7.2.3 基于证书的客户端验证”中所述。
- 用户预验证，如第 152 页中的 “7.2.4 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 152 页中的 “7.2.5 MMP 虚拟域”中所述。
- 在不同服务器上安装多个 MMP
- 增强的 LDAP 搜索功能。
- 用于传统 POP 客户端的“在 SMTP 之前先执行 POP”的服务。有关更多信息，请参见第 664 页中的 “23.8 启用 POP Before SMTP”。

本节包含以下几个部分：

7.2.1 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）的外来客户端连接。客户端将连接到 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端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消息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端呈现了一个单一的邮件主机（用户可以提高效率，外部客户端可以增强安全性）。第 149 页中的 “7.2.1 Messaging Multiplexor 的工作原理”显示了 MMP 安装中服务器和客户端彼此之间的相关方式。

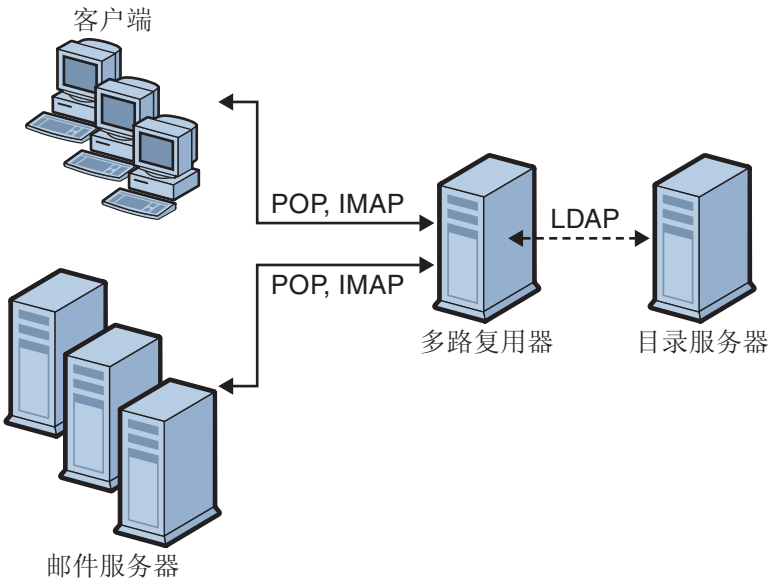


图 7–1 MMP 安装中的客户端和服务器

所有 POP、IMAP 和 SMTP 客户端都可以使用 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. 用户的客户端连接到 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。

7.2.2 加密 (SSL) 选项

Messaging Multiplexor 支持在 Messaging Server 及其邮件客户端之间进行未加密和加密的 (SSL) 通信。Messaging Server 的当前版本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 157 页中的 “7.4 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 6.3 Administration Reference》中的“Encryption (SSL) Option”。

7.2.3 基于证书的客户端验证

MMP 可以使用证书映射文件 (certmap.conf) 将客户端的证书与用户/组 Directory Server 中的正确用户相匹配。

要使用基于证书的客户端验证，还必须启用 SSL 加密，如第 150 页中的 “7.2.2 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=TOATTRmapname*: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

▼ 为您的IMAP 或POP 服务启用基于证书的验证

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单独的用户 ID（例如 mmpstore）。
2. **确保已启用（或将启用）SSL 加密，如第 150 页中的 “7.2.2 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，将 MMP 配置为使用基于证书的客户端验证。**
4. **至少安装一个信任的 CA 证书，如第 645 页中的 “23.5.1.6 安装可信 CA 证书”中所述**

7.2.4 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* 是会话标识符 (sid)，以十六进制数字表示；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。

7.2.5 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。

启用 Sun LDAP Schema 2 时（请参见《Sun Java Enterprise System 5 Installation Guide for UNIX》和《Sun Java Communications Suite 5 Schema Reference》），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完整路径。

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，并可以是您选择使用的任何名称；*IPaddr* 采用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《Sun Java System Messaging Server 6.3 Administration Reference》。

7.2.6 关于 SMTP 代理

MMP 包含一个 SMTP 代理（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 客户端所要求的“在 SMTP 之前先执行 POP”的验证功能。有关更多信息，请参见《Sun Java Communications Suite 5 Deployment Planning Guide》中的“Using the MMP SMTP Proxy”和第 664 页中的 “23.8 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 653 页中的 “23.5.4 如何使用 SMTP 代理服务器优化 SSL 性能”。

7.3 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 154 页中的 “7.3.1 配置 MMP 之前”
- 第 155 页中的 “7.3.2 多路复用器的配置”
- 第 155 页中的 “7.3.3 多路复用器文件”
- 第 156 页中的 “7.3.4 启动多路复用器”
- 第 156 页中的 “7.3.5 修改现有 MMP”

有关 MMP 的更多信息，请参见以下文档：

- 《Sun Java System Messaging Server 6.3 Administration Reference》中的第 5 章 “Messaging Multiplexor Configuration”

7.3.1 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 – 建议不要在同时运行 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 47 页中的 “1.1 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 48 页中的 “1.2 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，以匹配对尚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。

7.3.2 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 页中的 “1.3 创建初始 Messaging Server 运行时配置”

▼ 配置 MMP

1 **将 Sun Java System Messaging Server 置于您安装和配置 MMP 的计算机上。**

2 **通过创建 Messaging Server 初始运行时配置来配置 MMP。请参见第 49 页中的 “1.3 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。

7.3.3 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 6.3 Administration Reference》中的“Multiplexor Configuration Parameters”。

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。仅当使用 start-msg mmp 启动初始 MMP 后，文件才存在
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。仅当使用 start-msg mmp 启动初始 MMP 后，文件才存在
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。

表 7–1 Messaging Multiplexor 配置文件 （续）

文件	说明
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。仅当使用 start-msg mmp 启动初始 MMP 后，文件才存在
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”的更多信息，请参见第 664 页中的 “23.8 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。仅当使用 start-msg mmp 启动初始 MMP 后，文件才存在

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。

7.3.4 启动多路复用器

要启动、停止或刷新 Messaging Multiplexor 的实例，请使用表 7–2 中的以下命令之一，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。

7.3.5 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。

7.4 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 安装在没有消息存储或 MTA 的计算机上。

▼ 使用 SSL 配置 MMP

1. **安装 SSL 服务器证书（请参见第 640 页中的“ 23.5 配置加密和基于证书的验证 ”）。**
2. **编辑 `ImapProxyAService.cfg` 文件并取消相关 SSL 设置的注释。**
3. **如果需要 SSL 和 POP，请编辑 `PopProxyAService.cfg` 文件并取消相关 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`。
4. **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
   ```
5. **将 MMP 设置为使用 SSL 接受邮件，但使用非 SSL 将邮件发送到后端邮件服务器：**
   将 `ImapProxyAService.cfg` 或 `PopProxyAService.cfg` 中的 SSLBacksidePort 选项设置为 0。
6. **如果您不希望在 MMP 和后端服务器之间使用 SSL，则可以将 SSLBacksidePort 选项设置为 0。**

▼ 配置 MMP 以实现基于客户端证书的登录

如果希望基于客户端证书进行登录，请执行以下操作：

1. **获取一个客户端证书副本和签署它的 CA 证书。**
2. **将 CA 证书作为信任的证书授权机构导入（请参见第 641 页中的“ 23.5.1 获得证书 ”）**
3. **使用在安装 Messaging Server 过程中创建的存储管理员。**
   有关更多信息，请参见第 526 页中的 “20.4 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
```

这表示要通过查看 LDAP 服务器中的邮件属性搜索与证书 DN 中 e 字段相匹配的内容。

5 **编辑 `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 的客户端证书，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 **将客户端证书导入到您的客户端中。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端证书，则您的所有用户都必须执行此步骤。

7.4.1 样例拓扑

虚构的 Siroe Corporation 在两台计算机上各有一个 Messaging Multiplexor，均支持若干个 Messaging Server。POP 和 IMAP 用户邮箱分散在多台 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` 条目以限制客户端为仅访问 POP 服务；类似地，您也可以通过从 `ServiceList` 设置中删除 `PopProxyAService` 条目以限制客户端为仅访问 IMAP 服务）。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。

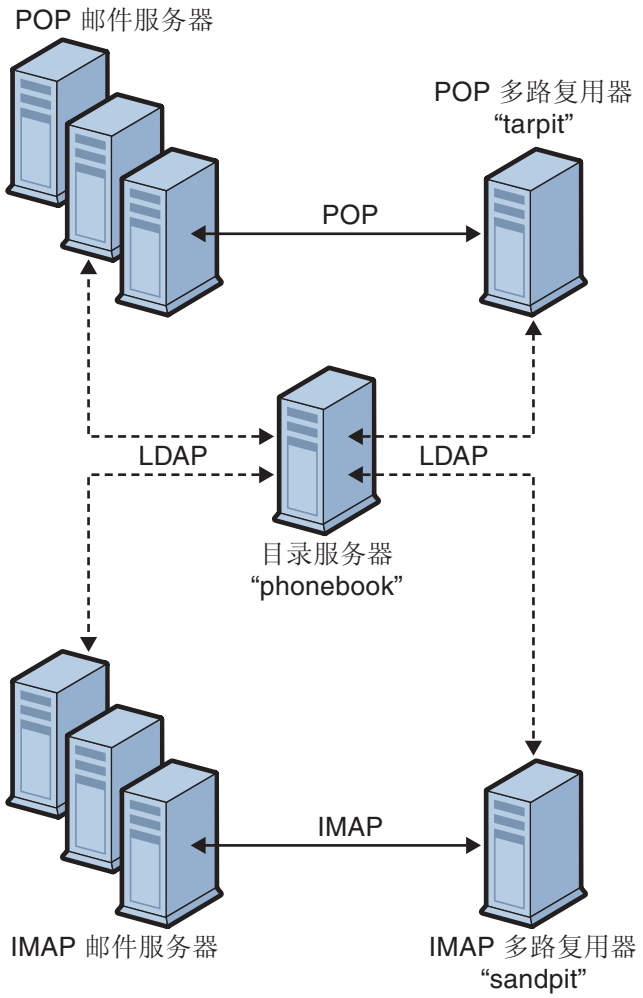


图 7–2 多个 MMP 支持多个 Messaging Server

7.4.1.1 IMAP 配置示例

图 7–2 中的 IMAP Messaging Multiplexor 安装在 `sandpit` 上，这是一台装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/cert8.db
default:SSLKeyFile /opt/SUNWmsgsr/config/key3.db
default:SSLKeyPasswdFile /opt/SUNWmsgsr/config/sslpassword.conf
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
```

7.4.1.2 POP 配置示例

第 158 页中的 “7.4.1 样例拓扑” 中的 POP Messaging Multiplexor 示例安装在 `tarpit` 上，这是一台装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。

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
```

7.5 MMP 任务

本节说明其他的 MMP 配置任务。这些元字符包含：

- 第 161 页中的 “7.5.1 用 MMP 配置邮件访问”
- 第 162 页中的 “7.5.2 设置故障转移 MMP LDAP 服务器”

7.5.1 用 MMP 配置邮件访问

MMP 不使用 PORT_ACCESS 映射表。如果希望拒绝来自某些 IP 地址的 SMTP 连接并且您正在使用 MMP，则必须使用 TCPAccess 选项。该选项的语法与

mailDomainAllowedServiceAccess 相同（请参见《Sun Java Communications Suite 5 Schema Reference》）。第 656 页中的 “23.7.2 过滤器语法”也对该语法作了介绍。

7.5.2 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"
```

注 – 请确保以上配置中的主机名之间留有空格。

◆ ◆ ◆ 第 8 章

8 MTA 概念

本章提供了 MTA 的概念性描述。其中包含以下各节：

8.1 MTA 功能

邮件传输代理 (*MTA*) 是 Messaging Server 的一个组件（图 8–1）。在最基础的级别上，MTA 是邮件路由器。它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端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。

图 8–2 中显示了支持这些功能的一系列子组件和进程。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 10 章
- 第 11 章
- 第 12 章
- 第 13 章
- 第 14 章
- 第 16 章
- 第 17 章
- 第 18 章
- 第 23 章
- 第 25 章
- 第 26 章
- 第 27 章

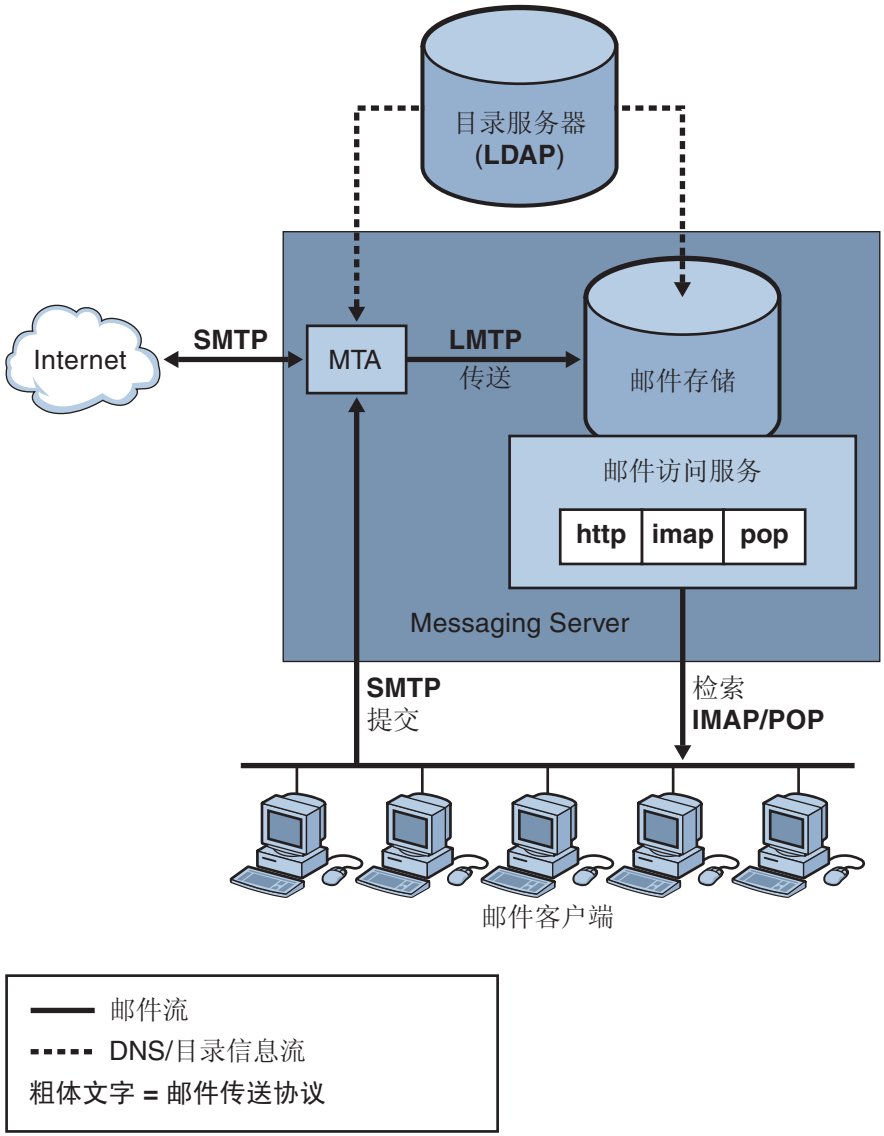


图 8–1 Messaging Server，简化后的组件视图（未显示 Communications Express）

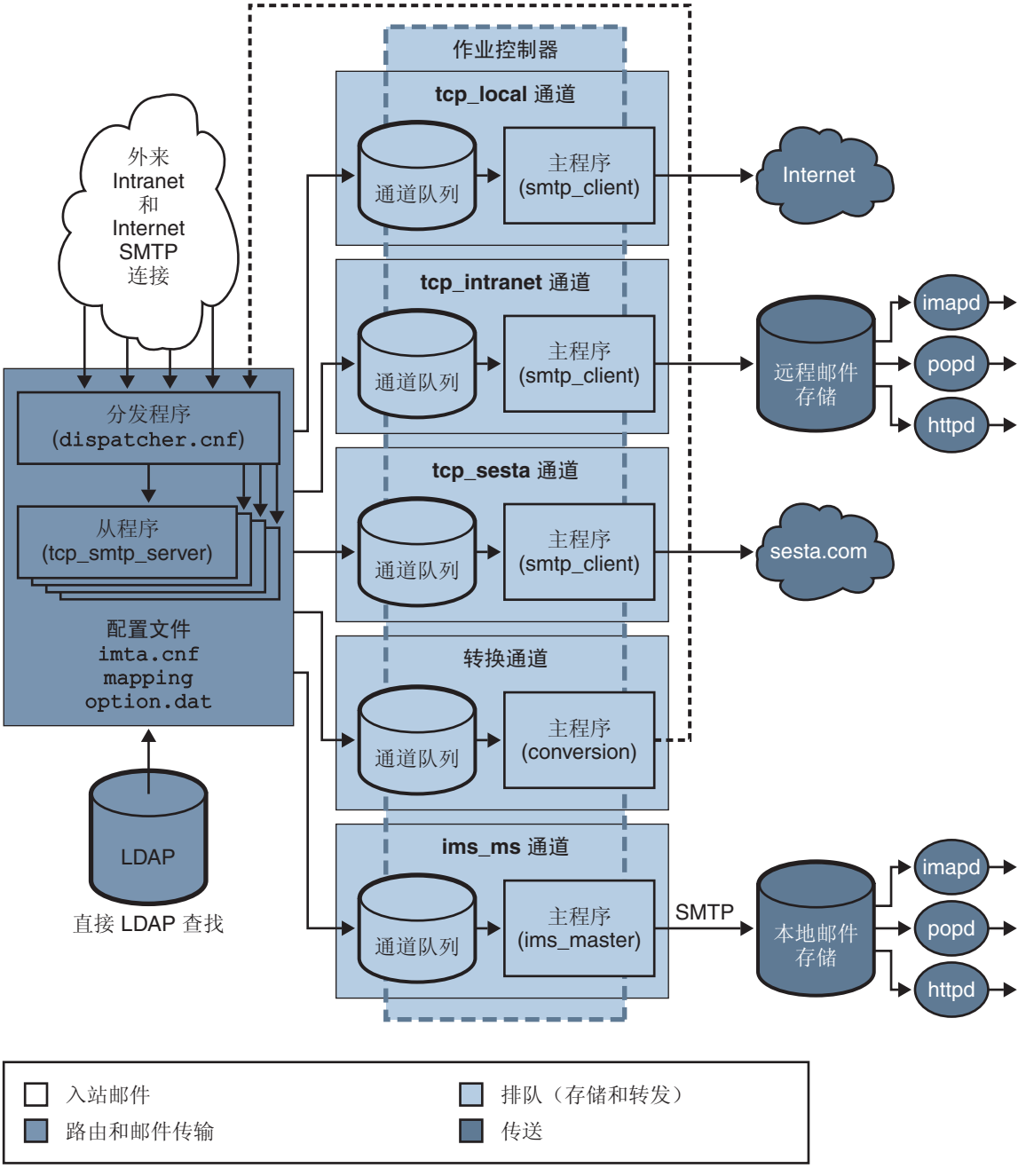

作业控制器
tcp_local 通道
通道队列
主程序
(smtp_client)
Internet
外来
Intranet
和
Internet
SMTP
连接
tcp_intranet 通道
通道队列
主程序
(smtp_client)
远程邮件
存储
imapd
popd
httpd
分发程序
(dispatcher.cnf)
从程序
(tcp_smtp_server)
tcp_sesta 通道
通道队列
主程序
(smtp_client)
sesta.com
配置文件
imta.cnf
mapping
option.dat
转换通道
通道队列
主程序
(conversion)
LDAP
直接 LDAP 查找
ims_ms 通道
通道队列
主程序
(ims_master)
SMTP
本地邮件
存储
imapd
popd
httpd
入站邮件
路由和邮件传输
排队（存储和转发）
传送

图 8–2 MTA 体系结构

8.2 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，而此图只是对邮件通过该系统的**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。

8.2.1 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 18 章）。
- 地址更改。外来的 `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 168 页中的 “8.3 分发程序” 。

8.2.1.1 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。此传送阶段完成了许多任务，其中的主要任务是：

- 别名扩展。
- 运行经过重写规则处理的地址，该处理包括以下两个部分：
  - 将地址的域部分重写为需要的格式。
  - 将邮件定向到正确的通道队列。

通道

通道是用于处理邮件的基本 MTA 组件。通道表示邮件与另一个系统的连接（例如，另一个 MTA、另一个通道或本地消息存储）。邮件传入时，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，要传送到本地消息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。用于读取域和确定正确通道的机制称为重写规则（请参见第 170 页中的 “8.4 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，都是在 `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。第 12 章中提供了通道关键字的完整描述。

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 位字符替换为星号。

8.3 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。

有关详细信息，请参见第 221 页中的 “10.4.4 分发程序配置文件”。

8.3.1 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为 MIN_PROCS 和 MAX_PROCS。MIN_PROCS 通过使若干服务器进程准备就绪并等待外来连接，提供了有保证的服务。另一方面，MAX_PROCS 设置了对于给定服务可以同时运行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 选项提供了一种有助于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”时连接的数量；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传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 221 页中的 “10.4.4 分发程序配置文件”。

8.3.2 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
```

此命令涵盖以前用于启动 MTA 组件（已经配置了分发程序以进行管理）的任何其他 start-msg 命令的功能，将不再使用这些旧有的命令。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。

8.4 重写规则

重写规则用于回答以下问题：

- 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。地址中包含 `siroe.com` 的所有邮件都将按照模板说明 (`$U%$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` 指定重写后的地址使用与模式匹配的相同域名。`@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。

有关配置重写规则的详细信息，请参见第 205 页中的 “10.2 MTA 配置文件”以及第 11 章。

8.5 通道

通道是用于处理邮件的基本 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。
- 将邮件传送到本地消息存储。
- 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。

本节包含以下几个部分：

8.5.1 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 客户端和服务器。

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。

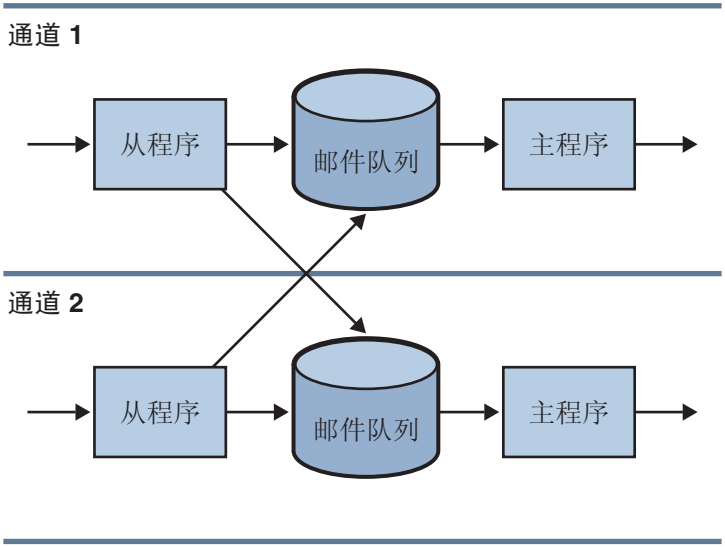


图 8–3 主程序和从程序

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从队列退回到本地消息存储系统，如图 8–4 所示。

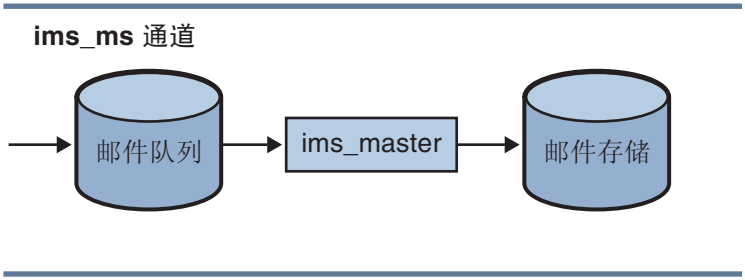


图 8–4 ims-ms 通道

8.5.2 通道邮件队列

所有通道均具有关联的邮件队列。邮件进入邮件服务系统时，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*`/*`。有关调整邮件队列大小的信息，请参见《Sun Java Communications Suite 5 Deployment Planning Guide》中的“Disk Sizing for MTA Message Queues”。

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，请在该安装点下创建子目录并将该子目录指定为 `IMTA_QUEUE` 的值。

8.5.3 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 205 页中的 “10.2 MTA 配置文件”中的规则部分和通道定义的开头部分）。

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）和唯一的通道标记（用于重写规则，以将邮件路由到该通道）。通道定义由单个空白行分隔。通道定义中可能会有注释，但不会有空白行。

```
[blank line]
! sample channel definition
Channel_Name  keyword1  keyword2
Channel_Tag
[blank line]
```

多个通道定义统称为通道主机表。单个通道定义被称为通道块。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**，用于指定如何处理邮件。许多不同的关键字允许用许多方式处理邮件。在第 12 章中列出了介绍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往往是本地通道 l。（例外情况是 defaults 通道，它可以出现在本地通道之前。）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 222 页中的 “10.4.6 选项文件”和第 220 页中的 “10.4.2 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。有关创建 MTA 通道的详细信息，请参见第 205 页中的 “10.2 MTA 配置文件”。

8.6 MTA 目录信息

对于 MTA 要处理的每封邮件，MTA 均需要访问其支持的用户、组和域的目录信息。此信息存储在 LDAP 目录服务中。MTA 直接访问 LDAP 目录。第 9 章中对此进行了完整说明。

8.7 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。可以将池看作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。有关池的详细信息，请参见第 223 页中的 “10.4.8 作业控制器文件”和第 339 页中的 “12.5.4 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。如果在第一次尝试传送邮件时未将其送出，则将延迟一段时间再次发送该邮件，该时间由相应的 backoff 关键字确定。一旦过了 backoff 关键字中指定的时间，就可以传送延迟的邮件，并且如果需要，将启动通道作业来处理该邮件。

内存中当前正在处理和等待处理的邮件的作业控制器数据结构，通常反映了存储在磁盘的 MTA 队列区域上的完整邮件文件集。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。

以前，作业控制器按文件在队列目录中找到的顺序读取所有文件。现在，它一次读取几个通道队列目录。这会使在启动、重新启动时以及超出 max_messages 后的行为变得更为合理。一次读取的目录数由作业控制器选项 Rebuild_Parallel_Channel 控制。可以将其设置为 1 到 100 之间的任何值，默认值为 12。

如果您的站点日常要处理大量邮件，则您需要使用 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信息，请参见第 223 页中的 “10.4.8 作业控制器文件” 和第 335 页中的 “12.5 配置邮件处理和传送” 。

8.7.1 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

9 MTA 地址转换和路由

在早于 Messaging Server 6 2003Q4 的版本中，Messaging Server 通常可以访问由 LDAP 服务器中存储的信息编译得到的数据库中的所有用户、域和组数据。更新 LDAP 服务器中的目录信息时，将通过称为 `dirsync` 的程序同步更新数据库信息。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：

9.1 直接 LDAP 算法和实现

以下各节介绍直接 LDAP 处理：

9.1.1 域位置确定

以 *user*@*domain* 格式的地址启动时，地址转换和路由进程将首先检查 *domain* 是否是本地域。本节包含以下几个部分：

- 第 180 页中的 “9.1.1.5 域检查重写规则的模式”
- 第 180 页中的 “9.1.1.6 汇总所有机制”

9.1.1.1 重写规则机制

MTA 重写规则机制添加了新的功能，可以检查给定字符串是否为需要在本地处理的域。通过 $V 或 $Z 元字符可以激活此新增功能。这些新增元字符在句法上与现有的 $N、$M、$Q 和 $C 元字符类似，即这些元字符之后都要跟模式字符串。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 $Z 而言，此模式是一个域，并将检查该域是否为本地域。$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 将检查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. 如果目录中有该域的条目，则将从域条目中检索由 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。该列表将与由 local.hostname configutil 参数指定的主机和由 local.imta.hostnamealiases configutil 参数指定的主机列表进行对比。这些选项可以分别由 LDAP_LOCAL_HOST 和 LDAP_HOST_ALIAS_LIST MTA 选项覆盖。 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，源路由（由 LDAP_DOMAIN_ATTR_ROUTING_HOSTS MTA 选项中列出的第一个值组成）将被附加到地址之前。
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。

   回溯域树的结果就是如果 siroe.com 被识别为本地域，则 siroe.com 的任何子域均将被识别为本地域。也可能会出现不需要这么做的情况，因此提供了 MTA 选项 DOMAIN_UPLEVEL 来控制该性能。特别是，如果清除 DOMAIN_UPLEVEL 的位 0（值为 1），则会禁用删除域组件的重试操作。DOMAIN_UPLEVEL 的默认值为 0。
4. 现在需要执行虚域检查。虚域没有域条目，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。通过使用由 DOMAIN_MATCH_URL MTA 选项指定的 LDAP URL 来执行 LDAP 搜索可以完成虚域检查。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 选项专用于为 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。

9.1.1.2 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 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 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，并继续进行步骤 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并返回到步骤 4。如果不存在 `aliasedObjectName` 属性，则处理过程会因故障而终止。可以通过 MTA 选项 `LDAP_DOMAIN_ATTR_ALIAS` 指定 `aliasedObjectName` 属性的替代使用方法。

   请注意，处理最多只能返回到步骤 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，可以使用 MTA 选项 `LDAP_ATTR_DOMAIN1_SCHEMA2` 和 `LDAP_ATTR_DOMAIN2_SCHEMA2` 分别覆盖用于此目的的 `sunPreferredDomain` 和 `associatedDomain` 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 中的域条目不需要具有 `inetDomainBaseDn` 属性；如果这些域条目不具有这些属性，则用户树的基目录将被假定为域条目本身。

有两个 MTA 选项支持通过用户基本域名称进行更有效的域查找。第一个选项是 `LDAP_BASEDN_FILTER_SCHEMA1`，它是一个字符串，在执行用户基本域名称搜索时指定用于标识 Schema 1 域的过滤器。如果指定了该 MTA 选项，则默认值为 `LDAP_DOMAIN_FILTER_SCHEMA1` 的值。如果两个选项都没有指定，则默认值为 `(objectclass=inetDomain)`。`LDAP_BASEDN_FILTER_SCHEMA2` 也是一个字符串，在执行用户基本域名搜索时指定用于标识 Schema 2 域的其他过滤元素。如果指定了该 MTA 选项，则默认值为 `LDAP_DOMAIN_FILTER_SCHEMA2` 的值。如果两个选项都没有指定，则默认值为空字符串。

9.1.1.3 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）可以设置高速缓存大小的最大值，通过 DOMAIN_MATCH_CACHE_TIMEOUT MTA 选项（默认值为 600 秒）可以设置高速缓存中条目的超时值。

9.1.1.4 错误处理

必须小心处理在此过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. 将临时错误 (4*xx*) 返回客户端，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，这样可以稍后在本地重试该地址。

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，也无法接受因重复进行此类查询而带来的系统开销。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是不足的。在域查找失败的情况下，将使用通过 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。

9.1.1.5 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 $* 可以确保此要求。在检查所有其他规则之前，先检查 $* 模式。

9.1.1.6 汇总所有机制

考虑到目前为止所述的所有机制，imta.cnf 中所需的新重写规则为：

```
$*      $E$F$U%$H$V$H@localhost
```

并且 option.dat 文件中的DOMAIN_FAILURE MTA 选项的值应为：

```
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 对 $V 的检查应在重新建立地址后以及在添加路由前进行。在临时查找失败的情况下，MTA 将更改路由。只要插入点发生了更改，就将应用暂挂通道匹配检查，以使第二个 $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。如果由于临时故障而无法执行检查，将使用通过 DOMAIN_FAILURE MTA 选项指定的值继续进行模板处理。首先，使用该模板的值将路由主机设置为 reprocess-daemon。然后，模板将检查 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。

9.1.2 本地地址的别名扩展

确定地址要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，包括：

1. 别名文件（已编译配置的一部分）。
2. 别名数据库。
3. 别名 URL。

要检查的确切别名源以及检查顺序取决于 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。这表示首先检查由 ALIAS_URL0 MTA 选项指定的 URL，再检查由 ALIAS_URL1 MTA 选项指定的 URL，接着检查由 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。

以下各节进一步介绍了别名扩展：

- 第 181 页中的 “9.1.2.1 使用 LDAP URL 检查别名”
- 第 181 页中的 “9.1.2.2 $V 元字符”
- 第 183 页中的 “9.1.2.3 从 URL 调用映射”
- 第 183 页中的 “9.1.2.4 $R 元字符”
- 第 184 页中的 “9.1.2.5 确定要获取的属性”
- 第 184 页中的 “9.1.2.6 处理 LDAP 错误”
- 第 184 页中的 “9.1.2.7 对 LDAP 结果的正常性检查”
- 第 184 页中的 “9.1.2.8 支持虚域”
- 第 185 页中的 “9.1.2.9 支持替换邮件地址”

9.1.2.1 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 LDAP 中的别名检查。上述第一个 URL 用于处理常规用户和组；后续别名 URL 用于处理虚域。第一个 URL 被指定为 ALIAS_URL0：

```
ALIAS_URL0=ldap:///$V?*?sub?$R
```

9.1.2.2 $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分别为 $V 和 $R。

$V 元字符将地址的域部分转换为基 DN。这与前面标题为第 178 页中的 “9.1.1.1 重写规则机制”一节中所述的 $V 重写规则元字符执行的初始步骤类似。$V 处理由以下步骤组成：

1. 获取当前域中用户条目的基 DN。
2. 获取与当前域相关联的规范域。在 Sun LDAP Schema 1 中，规范域名由域条目的 inetCanonicalDomainName 属性（如果该属性存在）指定。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，规范名称就是SunPreferredDomain 属性的值。

   提供了一个实用程序，用于验证具有交叉用户条目的域的规范域设置。请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimta test -domain”。
3. 如果存在基 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 [值为 4]）或当前域（如果设置了 DOMAIN_UPLEVEL 的位 2 [值为 4]）与 service.defaultdomain configutil 参数相比较来完成此操作。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 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 DN 成功，MTA 还将检索稍后会需要的若干有用的域属性。通过 option.dat 文件中的以下 MTA 选项设置检索到的属性的名称：

- 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_CATCHALL_MAPPING（无默认值）
- 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（无默认值）
- LDAP_DOMAIN_ATTR_MESSAGE_QUOTA（无默认值）
- LDAP_DOMAIN_ATTR_AUTOREPLY_TIMEOUT（无默认值）
- LDAP_DOMAIN_ATTR_NOSOLICIT（无默认值）
- LDAP_DOMAIN_ATTR_OPTIN（无默认值）

- LDAP_DOMAIN_ATTR_RECIPIENTLIMIT（无默认值）
- LDAP_DOMAIN_ATTR_RECIPIENTCUTOFF（无默认值）
- LDAP_DOMAIN_ATTR_SOURCEBLOCKLIMIT（无默认值）

9.1.2.3 从 URL 调用映射

以某些其他方式完成从域到基 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。可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；应该选择不会与映射名称和变量中通常使用的字符值发生冲突的字符。

9.1.2.4 $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，则将检查 local.imta.schematag configutil 参数，并根据它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 选项可以用于覆盖专为 MTA local.imta.schematag 进行的设置。

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（该域树是在标题为第 181 页中的 “9.1.2.2 $V 元字符”一节中的第二步保存的）中找到的域的地址。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（值为 2）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))
```

9.1.2.5 确定要获取的属性

如果 URL 将要返回的属性的列表指定为 *，则将用 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。

9.1.2.6 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，处理将终止并指示临时故障（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。

如果未设置此替换邮件地址属性，则检查通过 LDAP_DOMAIN_ATTR_SMARTHOST MTA 属性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。

9.1.2.7 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。

9.1.2.8 支持虚域

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)
```

9.1.2.9 支持替换邮件地址

最后，需要在 mailAlternateAddress 属性中检查 @*host* 格式的替换邮件地址。此格式的通配符允许在托管域和虚域中使用，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。

9.1.3 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：

9.1.3.1 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 显示了从各种 schematag 值得到的用户对象类和组对象类。

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对象类集和组对象类集。

例如，模式标记设置 ims50,nms41 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。

9.1.3.2 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 介绍了在生效的模式标记条目中要检查的常规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	General	邮件特定
sims40	用户	inetsubscriberstatus	mailuserstatus
sims40	组	无	inetmailgroupstatus
nms41	用户	无	mailuserstatus
nms41	组	无	无

表 9–2 要进行检查的属性 （续）

schematag	类型	General	邮件特定
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。特定于邮件的用户和组状态属性分别由 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

这些属性中的第一个属性，如果指定了除“活动”状态以外的其他状态，则优先于所有其他属性。其他允许的状态值包括“非活动”、“已删除”、“已移除”、“已禁用”、“保留”和“超过配额”。“保留”、“已禁用”和“已移除”状态仅可以用于邮件域、邮件用户或邮件组。“超过配额”状态仅能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”。未知状态值将被解释为“非活动”。

组合使用四种状态时，可能出现用户或组的下列状态：“活动”、“非活动”、“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，以便以后发送选项，此处所有选项都将被仅包含一个“保留”条目的选项列表覆盖。

9.1.3.3 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。MTA 只使用实际 UID，因此会使用通过 option.dat 文件中的 LDAP_DOMAIN_ATTR_UID_SEPARATOR MTA 选项获得的域分隔符来删除其余部分（如果存在）。

万一使用了非 uid 的某个属性来存储 UID，则可使用 LDAP_UID MTA 选项来强制使用该属性。

9.1.3.4 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。

9.1.3.5 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。主地址通常存储在 "mail" 属性中；另一属性可以通过相应地设置 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 477 页中的 “17.4 休假自动回复属性”）、LDAP_RECIPIENTLIMIT、LDAP_RECIPIENTCUTOFF（请参见第 364 页中的 “12.9.7 对邮件收件人进行限制”）和 LDAP_SOURCEBLOCKLIMIT（请参见第 361 页中的 “12.9.2 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，并且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。

进行反向的辅助地址通常存储在 mailAlternateAddress 属性中。另一属性可以通过设置 LDAP_ALIAS_ADDRESSES MTA 选项来指定。不进行反向的辅助地址通常存储在 mailEquivalentAddress 属性中。另一属性可以通过 LDAP_EQUIVALENCE_ADDRESSES MTA 选项来指定。

9.1.3.6 邮件主机和路由地址

现在来考虑 mailhost 和 mailRoutingAddress 属性。可以使用 LDAP_MAILHOST 和 LDAP_ROUTING_ADDRESS MTA 选项分别覆盖要使用的实际属性。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法，请参见第 190 页中的 “9.1.3.8 传送选项处理”（尤其是 # 标志）的说明。

就用户条目而言，mailhost 属性必须标识本地系统，才能使该属性对本地系统起作用。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 属性将被视为本地主机标识。

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 属性情况的处理有所不同。就用户而言，邮件主机是必需的，因此如果不存在 mailhost 属性，则格式为

@*smarthost*: *user*@*domain*

的新地址可以使用通过 LDAP_DOMAIN_ATTR_SMARTHOST MTA 选项确定的域的智能主机来构造。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。如果存在的问题导致处理终止，结果为 mailRoutingAddress。在版本 5.2 中，先执行 mailHost 检查，并且必须通过检查，路由地址才会生效。要在当前版本的 Messaging Server 中获得相同的行为，mailRoutingAddress 属性的格式可能如下所示：mailRoutingAddess: @mailhost:user@domain

9.1.3.7 其他属性支持

接下来，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。可以用 LDAP_BLOCKLIMIT MTA 选项覆盖 mailMsgMaxBlocks 的使用。

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内容。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 属性、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当前的一组转换标记中。可以使用 LDAP_CONVERSION_TAG MTA 选项更改该属性的名称。如果存在与该域的 mailDomainConversionTag 属性相关联的任何值，也将附加这些值。

9.1.3.8 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。通用的允许值包括 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或/和组。

该选项的值由 deliveryoption=template 对的以逗号分隔的列表组成，每对都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，相应的模板使用元字符替换方案（与 URL 处理使用的相同）来指定结果地址。

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。
`$`	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，表明在条目的指定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。这将使 MTA 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 * 和 & 都不存在，则将传送选项应用于用户和组中。

9.1.3.9 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 显示了其他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。
$*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（通过 `mailProgramDeliveryInfo` 属性）。
$*n*S	插入与当前地址关联的子地址。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 显示整数参数如何控制 $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。

表 9–7 控制 $nI 和 $nS 元字符的性能修改的整数 （续）

整数	性能说明
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。

除这些元字符之外，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。默认值设置为 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，如果有托管域）、加号（后面跟子地址，如果指定了子地址）和最后的 @ims-ms-daemon。

9.1.3.10 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）。

9.1.3.11 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，则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。有关详细信息，请参见第 477 页中的 “17.4 休假自动回复属性”。

9.1.3.12 Optin 和 Presence 属性

LDAP_OPTIN1 至 LDAP_OPTIN8 MTA 选项根据目标地址为每个用户的垃圾邮件过滤器 optin 值指定 LDAP 属性。如果指定了一个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。域级别属性（由 LDAP_DOMAIN_ATTR_OPTIN MTA 选项设置）设置的所有值也将被附加到列表中。LDAP_SOURCE_OPTIN1 至 LDAP_SOURCE_OPTIN8 提供类似的基于创始者地址的每个用户垃圾邮件过滤器 optin 值。

LDAP_PRESENCE MTA 选项可用于指定 URL，解析此 URL 后可以返回有关用户的当前信息。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 的源。

9.1.3.13 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。

特别是，通过使用 LDAP_FILTER MTA 选项可以覆盖 mailSieveRuleSource 属性。

9.1.3.14 延迟的处理控制

接下来将检查 mailDeferProcessing 属性。通过使用 LDAP_REPROCESS MTA 选项可以更改此属性。如果存在该属性并被设置为 no，则通常将继续进行处理。但如果该属性被设置为 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* 地址将只被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。（请参见第 190 页中的 “9.1.3.8 传送选项处理”一节，用户默认值为 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。

9.1.3.15 组扩展属性

许多附加属性与组扩展相关联，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、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) 单值属性，用于控制后续访问检查失败时进行的操作。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 到由 mgrpModerator 属性指定的中介人。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) 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服务标准。

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
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， 两者都表示 SMTP AUTH 命令必须用于标识发件人以便发送到组；SMTP_AUTH_USED 和 AUTH_USED，在效果上类似于 SMTP_AUTH_REQUIRED 和 AUTH_REQ，但不需要对邮寄人进行验证； PASSWORD_REQUIRED、PASSWD_REQUIRED 或 PASSWD_REQ，它们都表示由 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 为无操作。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) 允许将邮件提交到该组的域。OR_CLAUSES MTA 选项设置为 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 选项设置为 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，则避开此检查。可具有多个值，并允许使用全局样式通配符。
mgrpDisallowedDomain	(LDAP_CANT_DOMAIN) 不允许将邮件提交到该组的域。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) 允许将邮件发送到该组的标识邮件地址的 URL。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 选项设置为 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 选项设置为 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了所有访问控制检查的 SMTP EXPN。 mgrpallowedbroadcaster LDAP 属性上下文中的列表扩展现在包含用于存储电子邮件地址的属性（通常为 mail、mailAlternateAddress 和 mailEquivalentAddress）。以前仅返回 mail 属性，因而无法使用替代地址发送到仅限于其自己成员的列表。
mgrpDisallowedBroadcaster	(LDAP_CANT_URL) 不允许将邮件发送到该组的标识邮件地址的 URL。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了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）。该属性已作废，但仍支持向后兼容；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。如果存在 mgrpAuthPassword 属性，则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。

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
mgrpModerator	(LDAP_MODERATOR_URL) 该属性给出的将被扩展为一系列地址的 URL 列表。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，该属性将指定要接受邮件的中介人地址（如果任一访问检查失败）。如果缺少 LDAP_REJECT_ACTION 或具有任何其他值，则将把该地址列表与发件人地址相比较。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) 扩展时，将提供邮件列表成员地址的 URL 列表。
memberURL	(LDAP_GROUP_URL2) 扩展时，将提供邮件列表成员地址的另一个 URL 列表。
uniqueMember	(LDAP_GROUP_DN) 组成员的 DN 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??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。
rfc822MailMember	(LDAP_GROUP_RFC822) rfc822MailMember 支持向后兼容。rfc822MailMember 或 mgrpRFC822MailMember 都可以（但不能同时）用于任何给定组。
mgrpErrorsTo	(LDAP_ERRORS_TO) 将发件人 (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裁剪 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。
无默认值	(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 或可扩展属性。LDAP_EXPANDABLE MTA 选项可用于选择要检查的其他属性。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。

别名条目的负缓存由 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，在频繁使用虚域的情况下，站点应该考虑重新启用别名的负缓存。由 ALIAS_URL0 指定的 URL 所执行的搜索不大可能会成功。

9.1.4 修改组成员属性语法

添加了对使用映射进行 LDAP 扩展结果后处理的支持。可以使用新的 LDAP_URL_RESULT_MAPPING MTA 选项指定组属性的名称，从而指定映射的名称。该映射将被应用于通过扩展 mgrpDeliverTo 或 memberURL 属性所返回的任何结果。映射探测的格式如下：

LDAP-URL|*LDAP-result*

如果映射返回并设置了 $Y，则映射结果字符串将替代 LDAP 结果以进行别名处理。如果映射返回并设置了 $N，将跳过结果。

可以使用此机制定义组（基于不包含正确电子邮件地址的属性）。例如，假设一家公司在其所有的用户条目中放置了寻呼机号码。通过添加一个特定的域作为这些号码的后缀，可以向它们发送邮件。然后，可以按如下方式定义组：

1. 在目录中定义一个新的 mgrpURLResultMapping 属性，并将 LDAP_URL_RESULT_MAPPING MTA 选项设置为此属性的名称。
2. 使用以下属性定义所有页面的组：

```
mgrpDeliverto: ldap:///o=usergroup?pagerTelephoneNumber?sub
mgrpURLResultMapping: PAGER-NUMBER-TO-ADDRESS
```

3. 定义映射：

```
PAGER-NUMBER-TO-ADDRESS
  *|*    "$1"@pagerdomain.com$Y
```

将该机制与第 249 页中的 “10.12.1 优化对发送到邮件列表的邮件的 LDAP 目录所进行的授权检查”中介绍的 PROCESS_SUBSTITUTION 机制结合使用可获得更多有趣的效果。例如，可以很容易创建一个如下的元组：发送到格式为

pager+user@*domain.com*

的地址会将一个页面发送到名为 user 的用户。

9.2 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。由于 sleepycat 数据库已过时，您还应设置 USE_TEXT_DATABASES 以读取 IMTA_TABLE:reverse.txt 文件。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
```

$V 元字符已在别名 URL 的上下文中进行了介绍。但是，$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。

注 – 无论出于什么原因，建议您不要更改 REVERSE_URL。

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，不应再继续使用 $Q。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，该元字符将返回地址反向感兴趣的属性的列表。

无法完全控制 $N 的值：MTA 通过其自身的硬编码相关属性列表（并且可能会发生变化）对其进行构造以用于地址反向用途。如果使用不同的 LDAP_* 全局 MTA 选项来更改 MTA 认为感兴趣的属性的名称，事实上，您将从 LDAP 中获取不同的属性。但是，它始终是在语义上与 MTA 所认为的相关属性对应的任何属性。这些属性包括：LDAP_CAPTURE（无默认值）、LDAP_RECIPIENTLIMIT（无默认值）、LDAP_RECIPIENTCUTOFF（无默认值）、LDAP_SOURCEBLOCKLIMIT（无默认值）、LDAP_SOURCE_CHANNEL（无默认值）、LDAP_PERSONAL_NAME（无默认值）、LDAP_SOURCE_CONVERSION_TAG（无默认值）、LDAP_PRIMARY_ADDRESS (mail)、LDAP_ALIAS_ADDRESSES (mailAlternateAddress)、LDAP_EQUIVALENCE_ADDRESSES (mailEquivalentAddress) 以及 LDAP_SPARE_* 属性。

得到的选项值为：

```
REVERSE_URL=ldap:///$V?$N?sub?$R
```

通常，`local.imta.schematag` 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。

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（保存在第 178 页中的 “9.1.1.1 重写规则机制”的步骤 2 中）中找到的域的地址。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` 模式标记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))
```

反向查找返回几个属性，并且 MTA 知道使用邮件属性（更确切地说，是由 `LDAP_PRIMARY_ADDRESS` 命名的属性）作为用于地址反向的属性。请注意，还允许使用 `mailEquivalentAddress`（更确切地说，是由 `LDAP_EQUIVALENCE_ADDRESSES` 命名的属性）。

构建 URL 之后，将执行 LDAP 搜索。如果搜索成功，LDAP 实际上按任意顺序返回多个属性。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）可以设置高速缓存大小的最大值，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。

9.3 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功能。

异步 LDAP 查找的使用由 MTA 选项 `LDAP_USE_ASYNC` 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 属性的位和值设置。

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 和 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
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。

9.4 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，但不需要支持虚域，则应该使用以下选项：

```
ALIAS_URL1=ldap:///$V?*?sub?&(mailAlternateAddress=@$D)
```

需要删除 MTA 配置文件 (`imta.cnf`) 中 ims-ms 通道定义中的 `filter ssrd:$A` 子句。

9.5 处理多个具有相同语义的不同 LDAP 属性

MTA 现在能够处理多个具有相同语义的不同 LDAP 属性。请注意，这与处理相同属性的多个值（始终支持该功能）不同。属性接受的处理方式取决于属性的语义。可能的选项有：

1. 多个不同的属性没有意义并将用户条目视为无效。在 Mail Server 6.2 和更高版本中，除非另有指定，否则这种处理方式是所有属性的默认设置。
2. 如果指定了多个不同的属性，将随机选择并使用其中一个属性。
   `LDAP_AUTOREPLY_SUBJECT`、`LDAP_AUTOREPLY_TEXT` 和 `LDAP_AUTOREPLY_TEXT_INT` 仅在 6.2 版中接受这种处理方式；而在 6.3 和更高版本中接受第 477 页中的 “17.4 休假自动回复属性”中所述的处理方式。6.3 将 `LDAP_SPARE_3` 和 `LDAP_PERSONAL_NAME` 属性添加到此类别中。请注意，这是 6.2 以前版本处理所有属性的方式。
3. 多个不同的属性均有意义并起作用。这种处理方式当前对 `LDAP_CAPTURE`、`LDAP_ALIAS_ADDRESSES`、`LDAP_EQUIVALENCE_ADDRESSES` 和 `LDAP_DETOURHOST_OPTIN` 有效。请注意，`LDAP_DETOURHOST_OPTIN` 属性是首次添加到 6.3 版中。

◆ ◆ ◆ 第 10 章

10 关于 MTA 服务和配置

本章介绍常规 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：

10.1 编译 MTA 配置

只要修改了 MTA 配置文件（例如 `imta.cnf`、`mappings`、`aliases` 或 `option.dat`），就必须重新编译配置。该命令可以将配置文件编译成共享内存中的单个映像（在 UNIX 中）或动态链接库（在 NT 中）。

经过编译的配置中包含静态和动态可重新装入的部分。如果更改了动态部分，并且运行了 `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，因为使用编译后的配置时，配置文件本身不会处于“活动”状态。

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。

如果对 reverse、forward 或常规数据库进行了更改，可执行命令 imsimta reload 使更改生效。如果对 imta.cnf、mappings 文件、aliases、conversions 或 option.dat 文件进行了更改，而这些更改不会影响作业控制器，则应先执行 imsimta cnbuild，再执行 imsimta restart smtp。如果对 dispatcher.cnf 进行了更改，则需要执行 imsimta restart dispatcher。如果对编译后的配置中的配置文件进行了更改，并且这些更改会影响作业控制器但不会影响 SMTP 服务器，则通常应执行以下命令：imsimta cnbuild 和 imsimta restart job_controller。

如果对编译后的配置中的配置文件进行了更改，而这些更改会影响 SMTP 服务器和作业控制器，则应执行以下命令：

```
imsimta cnbuild
imsimta restart smtp
imsimta restart job_controller
```

（有关这些命令的详细信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“MTA Commands”。）

必须重新启动作业控制器的其他实例有：

- 更改控制器配置文件 job_controller.cnf、job_controller.site 或 job_controller.cnf 中的任何文件
- 添加或更改 imta.cnf 文件中通道关键字 pool、maxjobs、master、slave、single、single_sys 或 multiple 的用法。在 imta.cnf 中添加或更改 threaddepth 通道关键字可以使用 imsimta cache -change -thread_depth=... 来代替
- 使对主通道作业所作的更改立即生效（而无需控制器等待当前的通道作业超时）的情况下，对 MTA 配置或通道选项文件进行的所有相关（即几乎全部）更改。（对 mappings 文件或 MTA 数据库所作的更改：(1) 通常与出站通道作业无关，尽管它们可能对于“中间”通道（例如 conversion、process 和 reprocess）非常重要；(2) 如果需要考虑这些中间通道，通常可以通过 imsimta reload 来处理对 mappings 文件或数据库所作的更改，而无需重新启动作业控制器。）希望使更改立即生效时，需要综合重新启动作业控制器造成的损害和运行某特种作业将多用的时间慎重考虑。

MTA 配置包括 imta.cnf 及其所含的所有文件（例如 internet.rules）、alias 文件、mappings 文件、conversions 文件、option.dat 文件（以及上述所有文件中包含的所有文件）、imta.filter 以及 reverse、forward 和通用数据文件，还可能包括一些 configutil 参数。

请注意，以上对 imta.cnf 的所有更改（例如，添加/更改通道定义中的关键字）也需要 imsimta cnbuild—这是基本要求，无论是否需要重新启动作业控制器。

除非因上述条件之一必须重新启动作业控制器，否则应尽量避免重新启动，特别是在队列中有大量邮件的情况下。

建议不要在营运系统中使用 imsimta refresh 命令，因为通常没有必要重新启动作业控制器，而且重新启动作业控制器将会重置邮件重试次数、延迟的通知邮件、退回的邮件等。

10.2 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。使用默认的 imta.cnf 时，系统通常会运行良好。

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 章和第 12 章。

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至正确的通道。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。任何其他位置的感叹号均被解释为**文字**感叹号。
2. 重写规则在配置文件的上半部分显示。重写规则的各行之间不能出现空行。允许出现具有注释的行（以第一列中的感叹号开始）。
3. 文件中出现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**，该表定义了 MTA 可以使用的通道以及与每个通道相关联的名称。
4. 第一个显示的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，它可以显示在 `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。如果某一行中的第一列包含小于号 (`<`)，则该行中的剩余内容将被视为文件名；文件名应始终使用完整的绝对文件路径。该文件将被打开，其内容将在该点并入配置文件。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 显示了上述配置如何路由一些示例地址。

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，请参见第 170 页中的 “8.4 重写规则” 、第 173 页中的 “8.5.3 通道定义” 和第 11 章。

注 – 只要更改了 `imta.cnf` 文件，就必须重新编译 MTA 配置。请参见第 203 页中的 “10.1 编译 MTA 配置”。

10.3 映射文件

MTA 的许多组件都使用面向表查找的信息。此类表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（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）列给出了输入字符串映射到的结果输出字符串（模板）。有关 MTA 进程所使用的表以及何时使用的详细信息，请参见表 10–2。

大多数 MTA 数据库（包含不同类型的 MTA 数据，不应与映射表混淆）—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 `mappings` 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 203 页中的 “10.1 编译 MTA 配置”）。如果无法让所有人都能读取该文件，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 203 页中的 “10.1 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`	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。请参见第 325 页中的 “12.4.3 TCP/IP 连接和 DNS 查找支持”
`CHARSET-CONVERSION`	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。请参见第 396 页中的 “13.6 字符集转换和邮件重新格式化”
`COMMENT_STRINGS`	用于修改地址标题注释（括在括号中的字符串）。请参见第 349 页中的 “12.6.13 处理地址标题行中的注释”
`CONVERSIONS`	用于为转换通道选择邮件通信。请参见第 381 页中的 “13.5.2 选择用于转换处理的通信”
`FORWARD`	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。请参见第 234 页中的 “10.9.3 正向查找表和 FORWARD 地址映射”
`FROM_ACCESS`	用于基于信封源地址过滤邮件。`To` 地址为不相关的地址时使用该表。请参见第 482 页中的 “18.2.1 访问控制映射表—操作”

表 10–2 Messaging Server 映射表 （续）

映射表	页 说明
INTERNAL_IP	用于识别内部系统和子网。请参见第 495 页中的 “18.6 添加 SMTP 中继”
IP_ACCESS	用于根据源通道、远程服务器的 IP 地址和当前尝试的 IP 地址索引来阻止外来连接。请参见第 492 页中的 “18.3.5 IP_ACCESS 映射表”
MAIL_ACCESS	用于根据 SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息阻止外来的连接。请参见第 482 页中的 “18.2.1 访问控制映射表—操作”
NOTIFICATION_LANGUAGE	用于自定义或本地化通知邮件。请参见第 237 页中的 “10.10 控制传送状态通知邮件”
ORIG_MAIL_ACCESS	用于根据 ORIG_SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息阻止外来的连接。请参见第 482 页中的 “18.2.1 访问控制映射表—操作”
ORIG_SEND_ACCESS	用于根据信封源地址、信封目标地址、源通道和目标通道阻止外来的连接。请参见第 482 页中的 “18.2.1 访问控制映射表—操作”
PERSONAL_NAMES	用于修改个人名称（尖括号分隔的地址前的字符串）。请参见第 350 页中的 “12.6.14 处理地址标题行中的个人名称”
PORT_ACCESS	用于根据 IP 编号阻止外来的连接。请参见第 482 页中的 “18.2.1 访问控制映射表—操作”
REVERSE	用于将地址从内部格式转换为公用的公布格式。请参见第 230 页中的 “10.9 将地址由内部格式转换为公用格式”
SEND_ACCESS	用于根据信封源地址、信封目标地址、源通道和目标通道阻止外来的连接。请参见第 482 页中的 “18.2.1 访问控制映射表—操作”
*SMS_Channel*_TEXT	用于站点定义的文本转换。请参见第 828 页中的 “C.2.5 站点定义的文本转换”
X-ATT-NAMES	用于从映射表中检索参数值。请参见第 389 页中的 “13.5.3.5 通过转换条目调用映射表”
X-REWRITE-SMS-ADDRESS	用于本地 SMS 地址有效性检查。请参见第 826 页中的 “C.2.4 站点定义的地址有效性检查和转换”

10.3.1 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 template2-2 指定的任何内容。每种模式最多可以包含 256 个字符，每种模板最多可以包含 1024 个字符。在映射文件中，每行最多有 4096 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。

10.3.1.1 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
```

它可以有效地将文件 file-spec 的内容替换到 mappings 文件中包含出现的位置。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。此类包含的 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含的文件—不是需要时才将其装入，因此 使用包含的文件时不涉及性能或内存的节省。

10.3.2 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。有关 MTA 进程所使用的表以及何时使用的详细信息，请参见表 10–2。本节包含以下几个部分：

- 第 210 页中的 “10.3.2.1 映射条目模式”
- 第 212 页中的 “10.3.2.2 IP 匹配”
- 第 212 页中的 “10.3.2.3 映射条目模板”

10.3.2.1 映射条目模式

模式可以包含通配符。特别地，允许使用以下常用通配符：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。

表 10–3 映射模式通配符 （续）

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%	匹配一个十进制数字 (0-9)。
$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。
$[c_1 -c_n]%	匹配 c_1 至 c_n 范围中的任一字符。
$[c_1 -c_n]*	匹配 c_1 至 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。

请注意，`imsimta test -match` 实用程序可用于测试映射模式，特别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输入字符串，最大程度地匹配字符。例如，将输入字符串 `a/b/c` 与模式 `*/*` 进行比较时，左边的星号将匹配 `a/b`，右边的星号匹配剩余部分 `c`。

`$_` 修饰符使通配符匹配最小化，将最小匹配视为匹配，从左至右处理模式。例如，将字符串 `a/b/c` 与模式 `$_*/$_*` 进行比较时，左边的 `$_*` 将匹配 `a`，右边的 `$_*` 则匹配 `b/c`。

10.3.2.2 IP 匹配

使用 IPv4 前缀匹配时，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，以下示例匹配 `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，以下示例匹配 `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` 至 `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。

10.3.2.3 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。

请注意，元字符 $C、$E、$L 或 $R 中的任何一个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元字符 $C、$E、$L 或 $R 中的任何一个，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。
$]...[	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*{	添加该功能以访问每个域的属性。*domain* 是当前域，*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 的属性或以下定义的特殊属性： _base_dn_—域中用户条目的基 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。
元字符	**说明**
$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。
$E	立即结束映射进程；将此条目的输出字符串用作映射进程的最终结果。$+1E 立即退出，不解释模板的其余部分。

表 10–4 映射模板替换和元字符 （续）

替换序列	替换
$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。

本节包含以下几个部分：

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第 *n* 个通配符相匹配的内容。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有的大小写。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输入字符串，并且如果没有找到匹配的映射条目，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”或“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或失败的条目部分的左侧；否则，如果该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。这些标志是可设置的，设置后可使用 $:, $; 测试的通用映射表功能测试其是否存在。$: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 18–2 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 *x*%；在剩余时间内，该条目“失败”，并且将映射条目的输入按原样输出。（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* 应是一个指定成功百分比的实际数字。

例如，假设 IP 地址为 123.45.6.78 的系统向您的站点发送了过多的 SMTP 电子邮件，您想要使其速度减慢；可以按以下方式使用 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，该条目上的初始 $C 将使 MTA 从下一个条目继续执行映射，导致连接尝试被拒绝，同时显示 SMTP 错误和消息：**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，并将该值替换至模板。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* 参数分别指定用于输出序列值的基数（基）和输出的位数。默认基数为 10。从 -36 至 36 范围内的值均可作为基数；例如，基数 36 给出以数字 0 至 9、字母 A 至 Z 表示的值。默认情况下，序列值按其原有宽度打印，但是如果指定的宽度需要更多的位数，则输出结果的左侧将用 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。要使用此类序列号文件，还必须具有 MTA 用户帐户（在 imta_tailor 文件中配置为 nobody）。

URL 替换，$]...[

$]*url* [格式的替换是特殊处理的。*url* 可以是任何支持的 URL 类型，其中包括 file: 和 data:。也可以使用标准的 LDAP URL 并省略主机和端口；主机和端口改为由 LDAP_HOST 和 LDAP_PORT 选项指定。即，应将 LDAP URL 指定为：

ldap:///*dn*[?*attributes*[?*scope*?*filter*]]

其中，显示的方括号字符 [和] 表示 URL 的可选部分。*dn* 是必需的标识名，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（默认值）、one 或 sub 中的任何一个。*filter* 描述匹配条目的特性。

某些 LDAP URL 替换序列可以在 LDAP 查询 URL 中使用。URL 长度可以为 1024 个字符。这还适用于通过映射以及对其他映射的映射调用所创建的表达式。

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* 作为具有此名称的辅助映射表的输入。具有此名称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）；如果具有此名称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，原始的映射条目也将被视为失败：原始的输入字符串将被用作输出字符串。

请注意，如果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），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，映射表替换“失败”将导致不能显示进程控制元字符。

常规查找表或数据库替换 (${...})

${*text*} 格式的替换要特殊处理。*text* 部分用作访问通用查找表或 数据库的密钥（有关更多信息，请参见第 232 页中的 “10.9.1 MTA 文本数据库”）。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，则输入字符串将按原样用作输出字符串。

如果您使用的是通用查找表，则需要设置 MTA 选项 use_text_databases 的低顺序位。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。

如果要在执行通用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），则应将进程控制元字符置于映射表模板中通用表替换的左侧；否则通用表替换“失败”将导致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。然后使用以下参数列表将 *routine* 例程作为函数调用：

```
status = routine (argument, arglength, result, reslength)
```

`argument` 和 `result` 是长度为 252 字节的字符串缓冲区。`argument` 和 `result` 将作为指针传递至字符串（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` 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* 例程应返回 0；如果映射表替换成功，则该例程应返回 -1。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`），应该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，映射表替换的“失败”将导致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，可以调用某些类型的装入监视服务，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` 应可由所有用户读取。

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。

10.4 其他 MTA 配置文件

除了 imta.cnf 文件，Messaging Server 还提供了其他几个配置文件，以帮助您配置 MTA 服务。表 10–5 中汇总了这些文件。本节包含以下几个部分：

如果对 reverse、forward 或常规数据库进行了更改，可执行命令 imsimta reload 使更改生效（请参见第 232 页中的 “10.9.1 MTA 文本数据库”）。如果对 imta.cnf、mappings 文件、aliases、conversions 或 option.dat 文件进行了更改，而这些更改不会影响 job_controller，则应先执行 imsimta cnbuild，再执行 imsimta restart smtp。如果对 dispatcher.cnf 进行了更改，则需要执行 imsimta restart dispatcher。如果对编译后的配置中的配置文件进行了更改，并且这些更改会影响作业控制器但不会影响 SMTP 服务器，则通常应执行以下命令：imsimta cnbuild 和 imsimta restart job_controller。

有关这些命令的详细信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“MTA Commands”。

表 10–5 MTA 配置文件

文件	说明
第 220 页中的 “10.4.1 别名文件”（强制）	实现目录中不存在的别名。*msg-svr-base* /config/aliases
第 220 页中的 “10.4.2 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
第 220 页中的 “10.4.3 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
第 221 页中的 “10.4.4 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
第 223 页中的 “10.4.8 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

表 10–5 MTA 配置文件 （续）

文件	说明
第 207 页中的 “10.3 映射文件”（强制）	映射表的系统信息库。*/msg-svr-base/*`config/mappings`
第 222 页中的 “10.4.6 选项文件”	全局 MTA 选项文件。*/msg-svr-base/*`config/option.dat`
第 222 页中的 “10.4.7 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`

10.4.1 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` 文件的更多信息，请参见第 228 页中的 “10.5 别名”。

对 `aliases` 文件进行更改后，必须重新启动 MTA 以使更改生效。

10.4.2 TCP/IP (SMTP) 通道选项文件

TCP/IP 通道选项文件可以控制 TCP/IP 通道的各种特性。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`。有关更多信息，请参阅第 318 页中的 “12.4.1 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《Sun Java System Messaging Server 6.3 Administration Reference》。

10.4.3 转换文件

转换文件 `conversions` 指定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更多信息，请参见第 379 页中的 “13.5 转换通道”

10.4.4 分发程序配置文件

分发程序配置文件 dispatcher.cnf 用于指定分发程序配置信息。安装时将创建一个默认的配置文件，可不必对其进行更改而直接使用。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。（有关概念性信息，请参见第 168 页中的 “8.3 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 为基数表示的基数，*v* 是以 *b* 为基数表示的实际值。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
```

有关此文件的参数的更多信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》。

10.4.5 映射文件

mappings 文件定义 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。

可以使用 imsimta test -mapping 命令来测试映射表。有关 mappings 文件和 test -mapping 命令的语法的更多信息，请参见第 207 页中的 “10.3 映射文件”和《Sun Java System Messaging Server 6.3 Administration Reference》

对 mappings 文件进行更改后，必须重新启动 MTA 或执行命令 imsimta reload。

10.4.6 选项文件

选项文件 option.dat 指定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 ; 开头的行被视为注释行，即使前一行带有表示待续的后缀 \ 也不例外。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）。

对于因自然布局而具有以 # 或 ! 开头的连续行的传送选项，有一种安全而巧妙的解决方法。

有关选项文件语法的更多信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》。

10.4.7 调整文件

调整文件 imta_tailor 用于设置各种 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。

有关此文件的完整信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》。

10.4.8 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。可以将池看作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，请参阅第 174 页中的 “8.7 作业控制器”、第 339 页中的 “12.5.4 用于通道执行作业的处理池”和第 339 页中的 “12.5.5 服务作业限制”。）

作业控制器文件 `job_controller.cnf` 用于指定以下通道处理信息：

- 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，可以使用 `pool` **关键字**指定进程池（已在 `job_controller.cnf` 中定义）的名称。例如，以下 `job_controller.cnf` 样例文件的片段定义池 `MY_POOL`：

```
[POOL=MY_POOL]
job_limit = 12
```

以下 `imta.cnf` 样例文件的片断指定通道块中的池 `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其他池，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。

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`。

10.4.8.1 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。您可以通过创建具有作业限制的新池来完成此操作，然后使用 `pool` 通道关键字将这些通道定向到更适合的新池。

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轮询某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，经过 TCP/IP 处理 SMTP 的通道就不使用从程序，因为网络服务和 SMTP 服务器将根据 SMTP 服务器发出的请求接收外来 SMTP 邮件。SMTP 通道的主程序是 MTA 的 SMTP 客户端。

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。

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。

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
```

示例 10–1 UNIX 中的样例作业控制器配置文件 （续）

```
!
[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)
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 SLAVE_COMMAND。
3. 为后续的 [CHANNEL] 部分设置默认 MAX_LIFE_AGE。
4. 该 [POOL] 部分定义了名为 DEFAULT 的池。
5. 将此池的 JOB_LIMIT 设置为 10。
6. 该 [CHANNEL] 部分应用于名为 l 的通道，即 UNIX 本地通道。该部分中所需的唯一定义是 master_command，作业控制器执行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. 该 [CHANNEL] 部分应用于名称以 tcp_* 开头的所有通道。由于此通道名称中包含通配符，所以它将与名称以 tcp_ 开头的任何通道相匹配。

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。可以将池看作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。请注意，在 job_controller 中设置的作业限制是针对每个池的。例如，如果将 SMTP_POOL 的 job_limit 定义为 10，则在任一给定时刻，只能有 10 个 tcp_smtp 客户端进程可以在该池中运行。

某些情况下，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，并且它们全在 SMTP_POOL 中运行，则在任一给定时刻，每个 tcp_* 通道上可能只有一个 tcp_smtp 客户端在运行（具体情况取决于是否有目标为所有 tcp_* 通道的邮件，以及是否将 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_* 通道发送出去，这样效率就会很低。用户很可能会为附加的 tcp_* 通道定义附加的池，以防止出现争用槽的情况。

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
```

有关池的更多信息，请参见第 339 页中的 “12.5.4 用于通道执行作业的处理池” 。

表 10–6 作业控制器配置文件选项

选项	说明
常规选项	**说明**

表 10–6 作业控制器配置文件选项 （续）

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，且具有一个“内部网络”适配器和一个“外部网络”适配器，而您不能确信防火墙可以阻止到高端口号的连接，则应考虑指定“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。最小值为 10。 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* 是事件之间的时间间隔（以小时 [*h*] 和分钟 [*m*] 表示）。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 *msg-svr-base* /config/imta_tailor 中相应的 IMTA_JBC_SERVICE 选项，以使其匹配。TCP_PORT 选项应用于全局，如果显示在 [CHANNEL] 或 [POOL] 部分中，将被忽略。
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 单独应用于每个池；作业的最大总数为所有池的 JOB_LIMIT 参数之和。如果在某部分之外设置此选项，则所有未指定 JOB_LIMIT 的 [POOL] 部分都会将其用作默认选项。在 [CHANNEL] 部分中，该选项将被忽略。
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，则所有未指定 MASTER_COMMAND 的 [CHANNEL] 部分都会将其用作默认选项。在 [POOL] 部分中，该选项将被忽略。
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 14400（240 分钟）。

表 10–6 作业控制器配置文件选项 （续）

选项	说明
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，则所有未指定 SLAVE_COMMAND 的 [CHANNEL] 部分都会将其用作默认选项。在 [POOL] 部分中，该选项将被忽略。

10.5 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**。别名对于构建邮件列表、转发邮件以及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 181 页中的 “9.1.2.2 $V 元字符”

在 aliases 文件或别名数据库中定义的旧样式邮件列表现在接受非位置 [capture] 参数。如果使用，[capture] 参数将指定一个捕获地址，指定时使用的语义与由 LDAP 中的用户或组的 LDAP_CAPTURE 属性指定的捕获地址相同。

作为 [envelope_from] 非位置别名参数、位置别名参数错误或 LDAP 属性 mgrpErrorsTo 值指定的值 "/" 现在被解释为请求恢复使用外来邮件的原始信封 From: 地址，同时保留邮件列表语义。这对于设置邮件列表以向原始发件人报告所有形式的列表错误可能非常有用。

10.5.1 别名数据库

建议不要使用别名数据库。请改用 aliases 文件，因为可以使用 imsimta reload 命令动态地重新装入别名文件。

MTA 将使用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。

10.5.2 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。可以通过执行 imsimta reload 命令（或重新启动 MTA）来激活更改。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 提供了用于地址处理的其他工具，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。

此文件中的一个物理行最多可包含 1024 个字符。可以使用反斜杠 (\) 继续符将一个逻辑行分隔成多个物理行。

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。例如**：*default-domain*）

例如：

```
! A /var/mail/ user
inetmail@siroe.com: inetmail@native-daemon

! A message store user
ms_testuser@siroe.com: mstestuser@ims-ms-daemon
```

10.5.3 在别名文件中包含其他文件

可以在主 aliases 文件中包含其他文件。以下格式的行对 MTA 进行定向，以读取 file-spec 文件：

```
<file-spec
```

文件规范必须是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，必须可由所有用户读取。

被包含文件的内容将插入到其在 aliases 文件中的引用位置。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。

10.6 命令行实用程序

Messaging Server 提供了多个命令行实用程序，让您可以为 MTA 执行各种维护、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《Sun Java System Messaging Server 6.3 Administration Reference》。

10.7 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 18 章。

10.8 日志文件

所有特定于 MTA 的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 25 章。

10.9 将地址由内部格式转换为公用格式

使用地址反向文本数据库（又称为**反向文本数据库**）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，`uid@mailhost.siroe.com` 是 `siroe.com` 域中的有效地址，但它可能不适于向外公开。您可能更希望使用类似于 `firstname.lastname@siroe.com` 的公用地址。

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。

本节包含以下几个部分：

在反向文本数据库中，每个用户的公用地址都是由目录中用户条目的 `mail` 属性指定的。

反向文本数据库包含一个有效的地址与公用地址之间的映射。有关更多信息，请参见第 232 页中的 “10.9.1 MTA 文本数据库”。

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。如果未找到该地址，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，则结果字符串将在反向数据库中再运行一次；如果找到匹配内容，数据库中的模板将替换映射结果（从而替换地址）。通用 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。请注意，必须将 option.dat 中的 use_reverse_database 设置为 13，特定于通道的条目才能正常工作。

```
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。

10.9.1 MTA 文本数据库

MTA 使用 sleepycat 数据库的做法已过时，因为它会在 Messaging Server 部署中产生不稳定性。（请注意，近期内不会删除 sleepycat。）因此，应改用 MTA 文本数据库作为反向、正向以及常规数据库。

设置文本数据库：

1. 准备一个包含数据的文本文件。

   此文件的格式与 `imsimta crdb` 使用的格式相同：每行一个条目，其中包含两个以一个或多个空格分隔的字段。文件名称是由 `imta_tailor` 中的 `IMTA_GENERAL_DATA`、`IMTA_REVERSE_DATA` 和 `IMTA_FORWARD_DATA` 选项指定的，这些选项通常分别指向 *msg-svr-base*`/config/` 中的 `IMTA_TABLE:general.txt`、`IMTA_TABLE:reverse.txt` 和 `IMTA_TABLE:forward.txt`。

   `general.txt` - 常规数据库 `reverse.txt` - 反向数据库`forward.txt` - 正向数据库

2. 在 `USE_TEXT_DATABASES` 选项中设置相应的一个或多个位：

   位 0（值为 1）- 使用文本文件作为常规数据库；位 1（值为 2）- 使用文本文件作为反向数据库；位 2（值为 4）- 使用文本文件作为正向数据库

3. 设置启用所需数据库时需要使用的任何附加选项。

   例如，`USE_REVERSE_DATABASE`、`USE_FORWARD_DATABASE` 或任何其他选项

4. 运行 `imsimta cnbuild`

5. 运行 `imsimta reload`

`USE_TEXT_DATABASES` 不适用的唯一情况是用于高动态数据。在这些情况下，编写您自己的 MTA 插件而不是依赖于内置数据库支持可以获得更好的效果。

如果文本数据库不适用，并且您希望使用 `crdb` (Sleepycat) 数据库支持，可通过构造数据库使用方式并相应地更新进程以使用 `imsimta crdb` 或 `imsimta db` 更新数据库，而无需重新编辑、重新加载或重新启动。但要，这种方法仅在以下场合奏效：您只能添加或更新现有条目，在这种情况下，您可以使用 `imsimta crdb`。否则，您必须将数据构造为一系列添加/删除/更改操作。如果没有使用这种方法构造数据（通常不会这样构造数据），在更新时将恢复为替换整个数据库，而此时最好使用文本数据库。

10.9.2 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` 都可以用来控制何时以及如何应用地址反向的具体设置。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。而 reverse 指定应用地址反向。有关详细信息，请参见第 348 页中的 “12.6.9 启用特定于通道的反向数据库使用”。

USE_REVERSE_DATABASE 控制 MTA 是否将地址反向文本数据库和 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。值为 5（默认值）指定在 MTA 地址重写进程执行重写后，对所有地址都应用地址反向（而不仅是应用于反向指向地址）。值为 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（而不仅是应用于反向指向地址）。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 6.3 Administration Reference》中的“Option File Format and Available Options”。

REVERSE_ENVELOPE 选项用来控制是否将地址反向应用于信封 From 地址以及邮件标题地址。

有这些选项和关键字的作用的其他信息，请参见 Sun Java System Messaging Server Administration Reference 中的详细说明。

10.9.2.1 常规反向映射示例

以下是通用 REVERSE 映射的示例：假设 siroe.com 中内部地址的格式为 user@mailhost.siroe.com。而且，用户名称空间规则为：user@host1.siroe.com 和 user@host2.siroe.com 为 siroe.com 中的所有主机指定同一个人。以下 REVERSE 映射可以与地址反向文本数据库一起使用：

```
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 元字符使地址反向数据库可以被查询。地址反向文本数据库应包含以下格式的条目：

```
user@mailhost.siroe.com     first.last@siroe.com
```

10.9.2.2 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，则将使用地址反向文本数据库。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
```

此条目通知 MTA，对于源通道为 tcp_*、外发目标通道为 tcp_local 的所有邮件，都会将地址格式从 binky@macho.siroe.com 更改为 Rebecca.Woods@siroe.com。

注 – 要启用特定于通道的反向映射，必须将 option.dat 中的 USE_REVERSE_DATABASE 选项设置为 13（默认值为 5）

10.9.3 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 映射主要用于一些特殊种类的地址转发，大多数种类的地址转发可以使用 MTA 的某一其他转发机制更好地执行。

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。

10.9.3.1 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；如果指定 $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 输出映射表标志说明

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

表 10–8 FORWARD 输出映射表标志说明 （续）

标志	说明
$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）。如果已通过 USE_FORWARD_DATABASE 的相应设置启用了正向查找表，则当 FORWARD 映射匹配且具有标志 $G 时，会将 FORWARD 映射的结果与正向查找表进行核对。（请注意，如果已指定特定于通道的正向查找表，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（和可选的转发表查找）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（使用 $D 的结果）期间将不会执行进一步的 FORWARD 映射或数据库查找。

以下输入标志现在可用于 FORWARD 映射。过去只能在各种 *_ACCESS 映射中使用这些标志。

表 10–9 FORWARD 输入映射表标志说明

标志	说明
$A	用来验证连接的 SASL
$D	对于此收件人，NOTIFY=DELAYS 为活动状态
$E	传入连接使用的 ESMTP/EHLO
$F	对于此收件人，NOTIFY=FAILURES 为活动状态
$L	传入连接使用的 LMTP/LHLO
$S	对于此收件人，NOTIFY=SUCCESSES 为活动状态。
$T	用于安全连接的 SSL/TLS

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 的伪域生成通用格式的 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.example.com $Y"$1,$ $2"@am.sigurd.example.com
 *|mr_local|"*,*"@am.sigurd.example.com   $Y"$1,$ $2"@am.sigurd.example.com
 *|*|"*,$ *"@am.sigurd.example.com        $Y$3.$2@am.sigurd.example.com
 *|*|"*,*"@am.sigurd.example.com          $Y$3.$2@am.sigurd.example.com
 *|mr_local|*.*@am.sigurd.example.com     $Y"$2,$ $1"@am.sigurd.example.com
 *|*|*.*@am.sigurd.example.com            $Y$2.$3@am.sigurd.example.com

FORWARD

 "*,$ *"@am.sigurd.example.com            $Y"$0,$ $1"@am.sigurd.example.com
 "*,*"@am.sigurd.example.com              $Y"$0,$ $1"@am.sigurd.example.com
 *.*@am.sigurd.example.com                $Y"$1,$ $0"@am.sigurd.example.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 REVERSE 映射中，假设已设置了 MTA 选项 USE_REVERSE_DATABASE 中的第 3 位。）

10.9.3.2 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。请注意，通常不应使用正向查找表进行邮件的简单转发；执行此类转发时，使用 aliases 文件或别名查找表效率更高。默认情况下不会使用正向查找表，必须通过 USE_FORWARD_DATABASE 选项明确启用后才能使用该表。转发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文本数据库。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_databases 选项中的第 2 位（值为 4）和 use_forward_database 启用散列表。散列表从 *msg-svr-base*/configure/forward.txt 中读取，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的 MTA 进程。

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 2 位启用特定于源的转发数据库，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。

有关正向文本数据库的更多信息，请参见第 232 页中的 “10.9.1 MTA 文本数据库” 。

10.10 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。您还可以分别为每类传送状态（例如 `FAILED`、`BOUNCED`、`TIMEDOUT` 等）创建不同的邮件。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` 目录中（由 *msg-svr-base*`/config/imta_tailor` 文件中的 `IMTA_LANG` 设置指定）。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` 和 `return_suffix.txt`。

在 `*.txt` 文件的邮件文本中，每行都不能超过 78 个字符。请注意，您不应直接更改这些文件，因为升级 Messaging Server 的当前版本时会覆盖这些文件。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。

本节包含以下几个部分：

10.10.1 构造和修改状态通知

单个通知邮件由三个文件构建而成：`return_prefix.txt` + `return_`*ActionStatus*`.txt` + `return_suffix.txt`

要自定义或本地化通知，应为每种语言环境和/或自定义创建一组完整的 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 10–10 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* 指邮件的 MTA 状态类型。例如，return_failed.txt 的默认文本如下：

   无法将您的邮件传递给下列收件人：%R

   return_bounced.txt 的默认文本为：

   您的邮件被退回。是邮件管理员将其强行退回的。

   此邮件的收件人列表是：%R

3. return_suffix.txt 包含结束文本。默认情况下，此文件为空。

表 10–10 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	扩展为邮件在返回之前留在队列中的单位[1] 的数量。

表 10–10 通知邮件替换序列 （续）

替换	定义
%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" 可扩展为“1 天”或“2 天”。
%U [%u]	扩展为正在使用的时间单位小时或天。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，则需要编辑除英语外所有语言的 return_delayed.txt 和 return_timedout.txt 并将“天”替换为“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	扩展为邮件的收件人列表。
%%	%（请注意，无论为何种字符集，都将针对替换序列逐字节地扫描文本。如果您正在使用双字节字符集，请检查意外出现的 % 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）。

10.10.2 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 237 页中的 “10.10.1 构造和修改状态通知”中说明了此操作
2. 设置 NOTIFICATION_LANGUAGE 映射表。

NOTIFICATION_LANGUAGE 映射表（位于 *msg-svr-base*/config/mappings 中）根据**原始邮件**（导致系统发出通知的邮件）的属性（例如，语言、国家/地区、域或地址），指定要使用的一组本地化或自定义的通知邮件文件。

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 映射表的格式如下所示。由于印刷原因，该样例条目行经过了换行。实际条目应显示在一行中。

```
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`—通用的永久性错误消息（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 一直无法传送邮件，但将继续尝试传送。使用 `return_delayed.txt` 文件。
  - `deferred`—与 "delayed" 类似的未传送通知，但没有指示 MTA 将继续尝试传送的时间。使用 `return_deferred.txt` 文件。
  - `forwarded`—为此邮件请求了传送回执，但是该邮件现已被转发给不支持此类回执的系统。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` 对应于消息存储的传送队列，`tcp_local` 对应于出站 SMTP 队列，等等。
- `preferred-language` 是正在处理的邮件（为其生成通知的邮件）中所使用的语言。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，则它将成为对 `Preferred-language:` 或 `X-Accept-language:` 标题行指定的邮件创始者。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:` *address*。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` 是原始邮件发往的信封的 `To:` 地址（如果邮件无法到达多个收件人处则为第一个地址）。例如，在通知“无法将您的邮件传送至 dan@siroe.com 中”的情况下，dan@siroe.com 即为报告的信封 `To:` 地址。
- `directory-spec` 是是包含要使用的 `return_*.txt` 文件的目录（如果映射表探测匹配）。请注意，`$I` 必须位于目录规范之前。

  例如，在 `/lc_messages/table/notify_french/` 目录中存储法语通知文件 (`return_*.txt`) 以及在 `/lc_messages/table/notify_spanish/` 目录下的 `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。

```
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。）

10.10.3 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 10–11 介绍了可用于这些文件的选项。

表 10–11 传送状态和邮件处理通知选项

选项	说明
DAY (DSN)	设置 RETURN_UNITS=0（默认值）时，用于替换 %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)	覆盖 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)	设置 RETURN_UNITS=1 时，用于替换 %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)	构建 DSN 的各收件人部分时，将检查是否存在名称与各收件人的数值状态相匹配的选项。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 选项生成零长度的结果，则不会插入 REASON 字段。
ORIGINAL_ADDRESS (DSN)	覆盖 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)	覆盖 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)	覆盖 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。
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也未提供主题，则构建一个适当的主题。
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。

10.10.4 附加的状态通知邮件功能

前几个小节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：

- 第 242 页中的 “10.10.4.1 阻止较大邮件的内容返回”
- 第 243 页中的 “10.10.4.2 从状态通知邮件包含的标题中删除非美国 ASCII 字符”
- 第 243 页中的 “10.10.4.3 设置通知邮件传送间隔”
- 第 244 页中的 “10.10.4.4 在状态通知邮件中包含已变更的地址”
- 第 244 页中的 “10.10.4.5 对邮寄主管发送、阻止和指定状态通知邮件”

10.10.4.1 阻止较大邮件的内容返回

通常情况下，当邮件被退回或阻止时，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。要阻止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。

MTA 获取与信封返回地址关联的阻止限制，并且在没有指定返回策略且邮件大小超过阻止限制时设置 RET=HDRS。这保证了较大邮件的未传送报告自身是可传送的。没有与此更改关联的新选项或设置。

10.10.4.2 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?=
```

电子邮件客户端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"）与 return_prefix.txt 中 Content-Type 标题字符集参数中的字符集匹配，则 Messaging Server 将删除编码。如果不匹配，Messaging Server 将保留编码，不作更改。

10.10.4.3 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。

请注意，MTA 选项文件中的 RETURN_UNITS 选项使您可以用小时 (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，它还将每小时翻滚 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 configutil 参数 local.schedule.return_job 控制。但请注意，默认情况下，此命令定期运行（请参见第 108 页中的 “4.6.2 预定义的自动任务”）。

如果没有指定 notices 关键字，则默认使用本地通道 l 的 notices 设置。如果未对本地通道进行设置，则默认使用 notices 3, 6, 9, 12。

10.10.4.4 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、传送回执邮件等）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。对于要对外界“隐藏”内部邮箱名称的站点，抑制包含最终格式的地址可能会符合其利益。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。如果状态通知邮件中存在原始地址格式，则 suppressfinal 会使 MTA 抑制最终的地址格式。

useintermediate 关键字使用中间地址格式，亦即在列表扩展之后、用户邮箱名称生成之前生成的地址格式。如果此格式不存在，则使用最终格式。

10.10.4.5 对邮寄主管发送、阻止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。可以通过以下小节和表 10–12 中介绍的众多通道关键字来控制进一步精确地向邮寄主管传送通知邮件。本节包含以下几个部分：

- 第 244 页中的 “返回的失败邮件”
- 第 244 页中的 “警告消息”
- 第 245 页中的 “空的信封返回地址”
- 第 245 页中的 “邮寄主管返回的邮件内容”
- 第 245 页中的 “设置每个通道邮寄主管的地址”

返回的失败邮件

关键字：sendpost、nosendpost、copysendpost、errsendpost

通道程序可能会因长时间服务故障或地址无效而无法传送邮件。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。可以选择将所有失败邮件的副本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 10–12。）

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 通道关键字设置引起的超时所致，尽管在某些情况下，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 10–12。）

空的信封返回地址

关键字：returnenvelope

returnenvelope 关键字使用单个整数值，这些整数值可解释为一组位标志。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，此操作本身并不能保证邮件的安全性；如果愿意，邮寄主管和系统管理员通常可以使用 root 系统权限阅读邮件内容。（请参见表 10–12。）

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 构建退回邮件或状态通知邮件时所使用的邮寄主管返回地址为 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的错误消息。

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 分别使用必需参数，以

指定邮寄主管地址和个人名称。默认设置为 noreturnaddress 和 noreturnpersonal，表示应使用默认值。默认值通过 RETURN_ADDRESS 和 RETURN_PERSONAL 选项或正常的默认值（如果未设置该选项）建立。

如果通道中含有 aliaspostmaster 关键字，则按正式通道名寄往用户名 postmaster（小写、大写或大小写混合）的所有邮件都将重定向到 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，虽然 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，但是 aliaspostmaster 将影响 MTA 对寄往邮寄主管的邮件的处理。

表 10–12 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失败通知。**
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）。
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	**指定是向邮寄主管发送整个邮件还是只发送标题。**

表 10–12 用于将通知邮件发送给邮寄主管和发件人的关键字 （续）

关键字	说明
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，此操作并不能保证邮件的安全性，如果愿意，邮寄主管和系统管理员可以使用 root 系统权限阅读邮件内容。
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 关键字使用单个整数值，这些整数值可解释为一组位标志。 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。如果此格式不存在，则使用最终格式。
返回的邮件内容	**指定通知地址**
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。
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。

10.11 控制邮件处理通知

邮件处理通知 (Message Disposition Notifications, 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服务过滤和休假邮件。

10.11.1 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 239 页中的 “10.10.2 自定义和本地化传送状态通知邮件”和第 241 页中的 “10.10.3 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（请参见第 239 页中的 “10.10.2 自定义和本地化传送状态通知邮件”）相当。

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 的源通道。

`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，从而不能从这些文件继承字符集。）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。在 `*.txt` 文件的邮件文本中，每行都不能超过 78 个字符。

10.12 优化 MTA 性能

本节介绍了 MTA 的其他优化。其中包含以下各节：

10.12.1 优化对发送到邮件列表的邮件的 LDAP 目录所进行的授权检查

您可以使用元字符替换减少对发送到邮件列表的邮件的 LDAP 目录所进行的授权检查。

现在可以在 `mgrpModerator`、`mgrpAllowedBroadcaster` 和 `mgrpDisallowedBroadcaster` 属性中指定元字符替换。特别是各种与地址有关的元字符序列（用于整个地址的 `$A`、用于邮箱部分的 `$U`、用于域部分的 `$D`）都引用当前的信封 `From:` 地址，在某些情况下可以用于将 URL 返回的结果限制在可能（或保证）匹配的条目中。这可以使授权检查变得更有效。

新的 MTA 选项 `PROCESS_SUBSTITUTIONS` 控制是否在指定 URL 的各种 LDAP 属性中执行替换。该选项是位编码的值，每个位定义如下：

位	值	说明
0	1	如果设置，则在 mgrpDisallowedBroadcaster 中启用替换
1	2	如果设置，则在 mgrpAllowedBroadcaster 中启用替换
2	4	如果设置，则在 mgrpModerator 中启用替换
3	8	如果设置，则在 mgrpDeliverTo 中启用替换
4	16	在 memberURL 中启用替换

`PROCESS_SUBSTITUTIONS` MTA 选项默认值为 0，表示默认情况下所有这些替换都被禁用。

例如通过 LDAP 查找定义的动态列表，该列表中的每个人都允许邮寄。在这种情况下，您通常要给列表定义如下属性：

```
mgrpAllowedBroadcaster:
ldap:///o=Sesta,c=US??sub?(&(objectClass=inetMailUser)(objectClass=inetOrgPerson))
mgrpDeliverTo:
ldap:///o=Sesta,c=US??sub?(&(objectClass=inetMailUser)(objectClass=inetOrgPerson))
```

但是，这样定义的效果是将列表扩展两次，一次是用于授权检查，另一次是建立实际的收件人列表。这是一项非常消耗服务器资源的操作。另一方面，如果您添加限制，以便在授权检查中只返回包含当前信封 From: 地址的条目，则可能会获得更好的效果。首先，将 PROCESS_SUBSTITUTION 的设置更改为 2，然后，您可以设置以下条目：

```
mgrpAllowedBroadcaster:
ldap:///o=Sesta,c=US??sub?(&(objectClass=inetMailUser)(objectClass=inetOrgPerson)
(mail=$A)
mgrpDeliverTo:
ldap:///o=Sesta,c=US??sub?(&(objectClass=inetMailUser)(objectClass=inetOrgPerson))
```

在本例中，只对发件人的条目进行广播授权检查，而不是检查 Sesta US 中的所有用户条目。这减少了目录服务器对单个匹配（最好是通过索引）和单个返回值必须执行的操作。另一种方法是返回条目列表，并让 MTA 执行匹配。

请注意，可用于替换的信息会有所不同，具体取决于属性是用于授权检查，还是用于实际的列表扩展。对于授权属性，整个地址 ($A)、域 ($D)、主机 ($H) 和本地部分 ($L) 都源自已验证的发件人地址。对于列表扩展属性，所有这些替换值都源自指定列表的信封收件人地址。但是对这两种情况来说，子地址替换 ($S) 都源自当前的信封收件人地址。

由于可以访问列表扩展 URL 中的子地址信息，因此可以定义 *metagroups*，即用于创建不同组的整个集合的单个组条目。例如，一个组的 mgrpDeliverTo 值为

```
mgrpDeliverTo: ldap:///o=usergroup?mail?sub?(department=$S)
```

并且相应的 PROCESS_SUBSTITUTIONS 值为 8，则可以使用格式为 group+department@domain.com 的地址向给定部门中的每个成员发送邮件。请注意，如果子地址看起来过于复杂，可以使用转发映射之类的机制修改语法。

◆ ◆ ◆ 第 11 章

11 配置重写规则

本章介绍如何在 imta.cnf 文件中配置重写规则。如果您还未阅读第 10 章，则应该在阅读本章之前先阅读这一章。

本章包含以下各节：

Messaging Server 的地址重写工具是处理和更改地址的主机或域部分的主要工具。Messaging Server 提供了用于地址处理的其他工具，例如别名、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。

11.1 开始之前

在对 imta.cnf 文件中的重写规则做出更改后，您必须重新启动仅在启动时装入一次配置数据的所有程序或通道，例如使用 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更多信息，请参见 《Sun Java System Messaging Server 6.3 Administration Reference》 。

11.2 重写规则结构

重写规则显示在 MAT 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，后跟等值字符串或**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相匹配，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。

有关模式语法的更多信息，请参见第 253 页中的 “11.3 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 指定如何重写地址的用户部分。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 262 页中的 “11.6 模板替换和重写规则控制序列”。

DomainTemplate 指定如何重写地址的域部分。与 *UserTemplate* 相同，*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。有关控件的更多信息，请参见第 262 页中的 “11.6 模板替换和重写规则控制序列 ”。

有关模板语法的更多信息，请参见第 256 页中的 “11.4 重写规则模板”。

11.3 重写规则模式和标记

本节包含以下几个部分：

大多数重写规则模式包含仅与某一主机匹配的特定主机名，或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一主机或域匹配的子域模式：

```
.siroe.com
```

但该模式将不会匹配确切的主机名 `siroe.com`；要匹配确切的主机名 `siroe.com`，需要单独的 `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，对于 Internet 上的站点，会经常使用包含子域重写规则模式的重写规则。此类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。

为确保正确重写传送至 Internet 目的地（不是通过较具体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 IP 文字 `[1.2.3.4]` 完全匹配：

```
[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.]
```

除了已经介绍的较为常用的几种主机或子域重写规则模式以外，重写规则还可以使用几种特殊的模式，表 11–1 中概述了这些模式，并在以下小节中将对此进行介绍。

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 格式的任何主机/域说明匹配。
$!	Bang 样式规则。与 B!A 格式的任何主机/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 还包含**标记**的概念，标记可以在重写规则模式中出现。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 255 页中的 “11.3.4 标记的重写规则集” 。

11.3.1 与百分比黑客匹配的规则

如果 MTA 尝试重写 `A%B` 格式的地址时失败，则其将在失败并将该地址格式处理为 `A%B@localhost` 之前尝试一个附加规则。（有关这些地址格式的更多信息，请参见第 256 页中的 “11.4 重写规则模板” 。）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。

11.3.2 与 Bang 样式 (UUCP) 地址匹配的规则

如果 MTA 尝试重写 `B!A` 格式的地址时失败，则其将在失败并将该地址格式处理为 `B!A@localhost` 之前尝试一个附加规则。此附加规则是 *bang* **样式规则**。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 样式规则可用于将 UUCP 样式地址强制路由至具有 UUCP 系统和路由的全面知识的系统。

11.3.3 与任何地址匹配的规则

如果其他规则均不匹配，并且在通道表中找不到主机/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，当无法使用其他方法进行地址重写时，”.” 规则将作为最后的解决方案。

注 – 在替换序列方面，当全匹配规则匹配并且其模板已扩展时，`$H` 将扩展为完整主机名，`$D` 将扩展为单个句点 "."。因此，`$D` 在全匹配规则模板中的使用将受到限制！

11.3.4 标记的重写规则集

随着重写过程的继续，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。重写地址完成后，标记将被重置为默认标记—空字符串。

依照约定，所有标记值均以垂直条 | 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。

11.4 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 汇总了这些模板格式。

表 11–2 重写规则的模板格式摘要

模板	用法
A%B	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。第 256 页中的 “11.4.2 重复的重写模板 A%B”
A@B	将被视为 A%B@B。第 256 页中的 “11.4.1 一般重写模板：A%B@C 或 A@B”
A%B@C	A 将是新的用户/邮箱名称，B 将是新的主机/域说明，路由到与主机 C 关联的通道。第 256 页中的 “11.4.1 一般重写模板：A%B@C 或 A@B”
A@B@C	将被视为 A@B@C@C。第 257 页中的 “11.4.3 指定的路由重写模板 A@B@C@D 或 A@B@C”
A@B@C@D	A 将是新的用户/邮箱名称，B 将是新的主机/域说明，插入 C 作为源路由，路由到与主机 D 关联的通道。第 257 页中的 “11.4.3 指定的路由重写模板 A@B@C@D 或 A@B@C”

11.4.1 一般重写模板：A%B@C 或 A@B

以下模板为最常用的模板格式。此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*]

下一个模板格式在应用方面与最常用的模板格式相同。但是，仅当 *DomainTemplate* 和 *ChannelTag* 相同时，才可使用此模板格式。

UserTemplate@*ChannelTag*[*controls*]

11.4.2 重复的重写模板 A%B

以下模板格式用于在应用规则后还需要附加重写的元规则。规则应用后，将在产生的新地址上重复整个重写过程。（所有其他重写规则格式会导致重写过程在规则应用后终止。）

UserTemplate%*DomainTemplate*[*controls*]

例如，以下规则可以从地址的结尾处删除出现的所有 `.removable` 域：

```
.removable $U%$H
```

使用这些重复规则时必须非常谨慎；如果不小心，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。请务必使用 `imsimta test -rewrite` 命令测试元规则。有关 `test -rewrite` 命令的更多信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》。

11.4.3 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见的模板 *UserTemplate* `%`*DomainTemplate*`@` *ChannelTag*（注意第一个分隔符的区别）的工作方式相同，除了 *ChannelTag* 作为源路由被插入地址中。然后邮件将被路由到 *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
```

11.4.4 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。特别是，$\ 将强制后续被替换的材料为小写，$^ 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
```

11.5 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. 识别第一个主机或域名之后，MTA 将执行搜索，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 会将邮件加入关联的通道队列中；否则该重写过程失败。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。

本节包含以下几个部分：

11.5.1 步骤 1：提取第一个主机或域说明

重写地址的过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。）地址中主机/域说明的扫描顺序如下：

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）

如果 bangoverpercent 关键字在正进行地址重写的通道上有效（即，如果尝试将邮件加入队列的通道自身被标上 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	“简短格式”域名。
user@a.b.c	a.b.c	“全限定”域名 (fully qualified domain name, FQDN)。
user@[0.1.2.3]	[0.1.2.3]	“域文字”
@a:user@b.c.d	a	源路由的地址，“路由”部分是简短格式域名。
@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	此非标准的路由格式称为“百分比黑客”。
user%A	A	
user%A%B	B	
user%%A%B	B	
A!user	A	“Bang 样式”寻址；通常用于 UUCP。
A!user@B	B	
A!user%B@C	C	
A!user%B	B	nobangoverpercent 关键字处于活动状态；默认值。
A!user%B	A	bangoverpercent 关键字处于活动状态。

RFC 822 不对地址中的感叹号 (!) 和百分比符号 (%) 进行解释。如果没有 at 符号 (@)，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。

重复的百分比符号有一种特殊的解释，用于允许将百分比符号作为本地用户名的一部分；这在处理某些外部邮件系统地址时可能会十分有用。感叹号的解释符合 RFC 976 的“bang 样式”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很有用，但默认值更“标准”一些。

注 – 不建议在地址中使用感叹号 (!) 或百分比符号 (%)。

11.5.2 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，通常为主机名）将被删除并用星号 (*) 替换，然后将再次尝试查找生成的主机或域说明，但只在配置文件重写规则中查找（不查询域数据库）。

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：

- 使用主机/域说明作为比较字符串 spec_1 和 spec_2 的初始值。（例如，spec_1 = spec_2 = a.b.c）。
- 将比较字符串 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为星号。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（例如 .c 或 c），则该字符串将被单个句点 "." 替换，如果结果字符串 spec_1 的长度为非零值，则您将返回步骤 1。如果结果字符串长度为零（例如，为先前的 "."），则查找过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
*.*.*.*
.
```

11.5.3 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（到达该地址的邮件应该发送到此通道）的通道标记。

11.5.4 步骤 4：完成重写过程

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有 `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）的地址，并且重写过程将终止。
- 如果通道标记与本地通道或标有 `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，原始（初始）主机/域说明将从地址中被删除，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过程从地址中删除了。

11.5.5 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；例如原始说明将成为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。

11.5.6 重写后的语法检查

重写规则应用到地址后不进行任何附加的语法检查。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。

11.5.7 处理域文字

在重写过程中将对域文字进行特殊处理。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。

与常规的域或主机说明类似，域文字也是按最特定到最不特定的顺序进行尝试。其模式匹配的第一个规则将是用于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。重写程序将依次查找 `[128.6.3.40]`、`[128.6.3.]`、`[128.6.]`、`[128.]`、`[]` 以及 `[*.*.*.*]`，最后是全匹配规则 `"."`。

11.6 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：

例如，在以下模板中，`$U` 是一个替换序列。该替换序列将导致被重写地址的**用户名**部分被替换到模板的输出中。因此，如果使用此模板来重写 `jdoe@mailhost.siroe.com`，则结果输出将为 `jdoe@siroe.com`，并且用 `$U` 替换了原地址的**用户名**部分 `jdoe`，如下所示：

```
$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 格式的信封 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。
$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。
$W	在随机、唯一的字符串中替换。
$]...[	LDAP 搜索 URL 查找。
$.	建立一个字符串，临时 LDAP 查找失败时会将此字符串作为映射条目结果处理。
$(text)	常规数据库替换；如果查找失败则规则失败。

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
${...}	将指定的映射应用于提供的字符串。
$[...]	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	如果主机在符号的右侧则适用
$B	只适用于标题/正文地址
$C *channel*	如果发送到 *channel*，则将失败
$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* 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	只适用于反向指引的（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，重写模式的剩余部分（紧跟主机名后面的字符之后）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

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
$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，重写模式的剩余部分（紧跟主机名后面的字符之后）将会被 MTA 选项字符串 DOMAIN_FAILURE 替换。
$*n*T	覆盖默认的 ALIAS_MAGIC 设置，其中 *n* 是 MTA 选项 ALIAS_MAGIC 的相应值。在扩展别名期间，如果规则匹配，则覆盖域的设置。
$?*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。
$*number*?*errmsg*	如果重写失败，将返回 *errmsg* 而不是默认的错误消息，并将 SMTP 扩展错误代码设置为 *a.b.c*： ■ *a* 为 *number*/1000000（第一个数字） ■ *b* 为 (*number*/1000) 除以 1000 的余数（第 2 个到第 4 个数字的值） ■ *c* 是 *number* 除以 1000 的余数（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`

11.6.1 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" 格式的用户名将被 "a.b" 格式的用户名替换，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。

11.6.2 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
```

结果地址是 jdoe@siroe.com，TCP-DAEMON 将用作外发通道。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）开始匹配的部分中进行替换，因此在 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。

11.6.3 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）。

11.6.4 LDAP 查询 URL 替换，$]...[

`$]ldap-url[` 格式的替换被解释为 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` 是必需的标识名，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）。范围可以是任何基准（默认设置）、某个基准或子基准。所需的过滤器可能会要求返回其 `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地址路由到哪个系统的可能的重写规则可能显示如下，其中 LDAP URL 替换序列 $D 用于将当前域名替换到构建的 LDAP 查询中：

```
.siroe.com \
  $U%$H$D@$]ldap:///o=siroe.com?mailRoutingSystem?sub? \
  (mailDomain=$D)
```

为了便于阅读，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

表 11–5 LDAP URL 替换序列 （续）

替换序列	说明
$.	建立一个字符串，临时 LDAP 查找失败时会将此字符串作为映射条目结果处理。默认情况下，临时失败字符串仅在当前规则的持续时间内保持已设置状态。"$.." 可以用于返回到默认状态，此时不设置临时失败字符串，并且临时 LDAP 失败会导致映射条目或重写规则失败。请注意，除了无法匹配目录中的条目之外，其他所有错误都被认为是临时错误；通常无法区分由不正确的 LDAP URL 所引起的错误和由目录服务器配置问题所引起的错误。
$~*account*	用户帐户的主目录
$A	地址
$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。这一新的 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）。

11.6.5 常规数据库替换，$(...)

$(text) 格式的替换是经过特殊处理的。文本部分被用作访问特殊的常规文本数据库的密匙。该数据库包括在 *msg-svr-base* /config/imta_tailor 文件中通过 IMTA_GENERAL_DATABASE 选项指定的文件，此文件通常为 *msg-svr-base*/db/generaldb。

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”与数据库中的任何条目均不匹配，则重写过程失败；这就相当于重写规则从未匹配过。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 $(text) 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（如果有）将用于重写规则的模板。假设查找 siroe 的结果为 $u%eng.siroe.com@siroenet，则模板的输出将是 jdoe@eng.siroe.com（即用户名为 jdoe，主机/域说明为 eng.siroe.com），且路由系统将是 siroenet。

如果常规文本数据库存在，则它应该是全局可读的，以确保正常运行。有关更多信息，请参见第 232 页中的 “10.9.1 MTA 文本数据库” 。

11.6.6 应用指定的映射，${...}

.SIROENET $($H) `${mapping,argument}` 格式的替换用于查找并应用 MTA 映射文件中的映射。`mapping` 字段指定要使用的映射表的名称，而 `argument` 指定要传递给映射的字符串。若要重写成功，映射必须存在并必须在其输出中设置 $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 重写过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 重写过程所具有的功能。

11.6.7 用户提供的例程替换，$[...]

`$[`*image* `,`*routine*`,`*argument* `]` 格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中指定的例程。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* 将作为指针传递到字符串（例如，在 C 中，作为 `char*`），*arglength* 和 *reslength* 是由引用传递的有符号型长整数。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，而其长度应放在 *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。

此机制允许重写过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` 的正向定位地址（例如 To: 地址）的目录服务查找，可以使用以下重写规则并按如下方式执行。第 271 页中的 “11.6.12 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定位地址：

```
siroe.com $F$[LOOKUP_IMAGE,LOOKUP,$U]
```

正向定位地址 `jdoe@siroe.com` 与该重写规则匹配时，将导致 `LOOKUP_IMAGE`（UNIX 上的共享库）被装入内存，并导致例程 `LOOKUP` 被调用（使用 `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，以表示重写规则成功。结果字符串中的百分比符号（请参见第 256 页中的 “11.4.2 重复的重写模板 A%B”）`John.Doe@eng.siroe.com` 将作为要被重写的地址。

在 UNIX 系统上，站点提供的共享库映像应该是全局可读的。

11.6.8 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。

11.6.9 唯一字符串替换

每次使用 $W 控制序列时均会插入一个由大写字母和数字组成的文本字符串，这些大写字母和数字都是唯一并且不可重复的。在必须构造非重复的地址信息时，$W 很有用。

11.6.10 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。如果在与正执行重写的 MTA 组件相关联的通道上指定了 norules，将不会进行特定于通道的重写检查。如果在通道上指定了规则，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没有关联。该重写仅取决于执行重写的 MTA 组件以及该组件的通道表格条目。

特定于通道的重写检查由规则模板部分中的 $N 或 $M 控制序列触发。$N 或 $M 与 at 符号 (@)、百分比符号 (%) 或后续 $N、$M、$Q、$C、 $T 或 $? 之间的字符被解释为通道名称。

例如，如果 *channel* 当前没有执行重写，则 $M*channel* 将导致规则失败。如果 *channel* 正在执行重写，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。如多个 $N 子句中的任何一个子句匹配，则规则将失败。

11.6.11 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要处理邮件并将邮件移出队列的通道，以及该通道上的通道关键字 rules 和 norules 关联。如果在目标通道上指定了 norules，则不会执行特定于通道的重写检查。如果在目标通道上指定了 rules，则会强制执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。将邮件加入队列时，首先重写其信封 To: 地址以确定邮件要加入队列的通道。在重写**信封** To: 地址过程中，将忽略所有 $C 和 $Q 控制序列。重写了**信封** To: 地址以及确定了目标通道之后，$C 和 $Q 控制序列才生效，因为与该邮件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模板部分中的 $C 或 $Q 控制序列触发。$C 或 $Q 与 at 符号 (@)、百分比符号 (%) 或后续 $N、$M、$C、$Q、$T 或 $? 之间的字符都被解释为通道名称。

例如，如果 *channel* 不是目标通道，则 $Q*channel* 将会导致规则失败。再如，如果 *channel* 是目标通道，则 $C*channel* 将会导致规则失败。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。

11.6.12 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正文的地址，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。正向定位地址源自 To:、Cc:、Resent-to: 或其他标题，或源自引用了目标的信封行。反向定位地址如 From:、Sender: 或 Resent-From:，指的是源。如果地址是正向定位的，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。

11.6.13 特定于主机位置的重写 ($A, $P, $S, $X)

有时需要重写主机名在地址中出现的敏感位置。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。

四个控制序列用于根据地址中主机的位置来控制匹配。

- $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，规则将与在源路由中或 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。

11.6.14 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 与 at 符号、百分比符号、$N、$M、$Q、$C、$T 或 $? 之间的文本均被视为新标记。

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，并强制使结果地址与 TCP-DAEMON 通道匹配。

这可以通过类似以下规则（假定 localhost 为本地主机的正式名称）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。

11.6.15 控制与重写相关联的错误消息 ($?)

重写和通道匹配失败时，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邮箱，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。如果此次重写的结果与任何通道均不匹配，则 $? 与 at 符号 (@)、百分比符号 (%)、$N、$M、$Q、$C、$T 或 $? 之间的文本均被视为要打印的错误消息的文本。错误消息的设置具有“黏性”并将贯穿重写过程始终。

包含 $? 的规则与其他任何规则的操作方式相同。规则中只包含 $?（而没有任何其他符号）的特殊情况需要特别注意—重写过程将终止，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
```

此示例中，可能失败的任何不可识别的主机或域说明在失败过程中都会生成错误消息：`Unrecognized address; contact postmaster@siroe.com`。

11.7 处理大量的重写规则

MTA 始终从 imta.cnf 文件中读取所有重写规则，并将它们以散列表的形式存储在内存中。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。每次读取常规配置文件时，MAT 都将检查域数据库是否存在。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。

11.8 测试重写规则

可以使用 `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之前，测试对配置文件所做的更改。

您会发现使用此带有 `-debug` 限定符的实用程序来重写一些地址十分有用。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《Sun Java System Messaging Server 6.3 Administration Reference》。

11.9 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 的配置文件中包含以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 显示了一些样例地址，以及如何根据重写规则来重写和路由这些地址。

表 11–7 样例地址和重写

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
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—route inserted
user@b.cs.sesta.edu	user@b.cs.sesta.edu	gate.adm.siroe.edu—route inserted
user@[1.2.3.4]	user@[1.2.3.4]	gate.adm.siroe.edu—route inserted

基本上，这些重写规则的意思是：如果主机名是我们的简短格式名称之一（`sc`、`sc1` 或 `sc2`），或者是我们的完整名称（`sc.cs.siroe.edu` 等）之一，则将其扩展为完整名称并路由给我们。将 `cs.cmu.edu` 附加至一部分简短格式的名称并重试。将后面为 `.cs` 的一部分转换为后面为 `.cs.siroe.edu` 的一部分，并重试。同时将 `.cs.siroe` 转换为 `.cs.siroe.edu` 并重试。

如果名称为 `sd.cs.siroe.edu`（可能是我们直接连接至的某个系统），则执行重写并将其路由至那里。如果主机名为 `.cs.siroe.edu` 子域中的任何其他名称，则将其路由至 `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，则将其路由至 `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，则将其路由至 `gate.adm.siroe.edu`（假定其可以将邮件路由至正确的目标）。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

12 配置通道定义

本章将介绍如何在 MTA 配置文件 `imta.cnf` 中使用通道关键字定义。在阅读本章之前，请先阅读第 10 章、第 173 页中的 “8.5.3 通道定义” 和第 205 页中的 “10.2 MTA 配置文件” 。本章包含以下各节：

注 – 如果在 `imta.cnf` 中更改了通道定义，则必须使用 `imsimta restart` 命令重新启动仅在启动时才装入一次配置数据的所有程序或通道（例如，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更多信息，请参见 《Sun Java System Messaging Server 6.3 Administration Reference》 。

12.1 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的所有通道块都将继承行中指定的关键字：

```
defaults keyword1 keyword2 keyword3 ...
```

defaults 行可看作无需实际指定通道即可更改关键字默认值的一个特殊通道块。defaults 行也不需要任何附加的通道块信息行（将忽略指定的信息行）。

对于可以指定的 defaults 行数没有限制，多个 defaults 行的影响可以累积，最后遇到的（从上向下读取）行具有较高的优先级。

从配置文件的某个点（例如，外部文件中通道块的独立部分的开始处）开始无条件消除 defaults 行的影响可能很有用。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，只有 defaults 和 nodefaults 通道块能出现在本地通道之前。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。

12.2 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列表

关键字	有关更多信息...
733	第 343 页中的 “12.6.1 地址类型和约定”
822	第 343 页中的 “12.6.1 地址类型和约定”
addreturnpath	第 348 页中的 “12.6.11 生成 Return-path 标题行”
addresssrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件”
addrsperfile	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送”
Aliasdetourhost	第 370 页中的 “12.12.6 地址验证之后扩展之前的路由”
aliaslocal	第 350 页中的 “12.6.15 指定别名文件和别名数据库探测”
aliaspostmaster	第 245 页中的 “邮寄主管返回的邮件内容”
allowetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持”
allowswitchchannel	第 330 页中的 “12.4.3.8 外来邮件的备用通道（切换通道）”
alternatechannel	第 362 页中的 “12.9.3 重新定向超过大小限制或收件人限制的邮件”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
alternateblocklimit	第 362 页中的 “12.9.3 重新定向超过大小限制或收件人限制的邮件”
alternatelinelimit	第 362 页中的 “12.9.3 重新定向超过大小限制或收件人限制的邮件”
alternaterecipientlimit	第 362 页中的 “12.9.3 重新定向超过大小限制或收件人限制的邮件”
authrewrite	第 325 页中的 “12.4.3 TCP/IP 连接和 DNS 查找支持”
backoff	第 337 页中的 “12.5.3 为传送失败的邮件指定重试频率”
bangoverpercent	第 345 页中的 “12.6.3 在地址中添加路由信息”
bangstyle	第 343 页中的 “12.6.1 地址类型和约定”
bidirectional	第 337 页中的 “12.5.1 设置通道方向性”
blocketrn	第 321 页中的 “12.4.2.3 ETRN 命令支持”
blocklimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制”
cacheeverything	第 327 页中的 “12.4.3.2 缓存通道连接信息”
cachefailures	第 327 页中的 “12.4.3.2 缓存通道连接信息”
cachesuccesses	第 327 页中的 “12.4.3.2 缓存通道连接信息”
caption	第 374 页中的 “12.12.9 设置 Monitoring Framework 的通道显示”
channelfilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
charset7	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
charset8	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
charsetesc	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
checkehlo	第 321 页中的 “12.4.2.2 EHLO 命令支持”
chunkingclient	第 334 页中的 “12.4.6 支持 SMTP Chunking”
chunkingserver	第 334 页中的 “12.4.6 支持 SMTP Chunking”
commentinc	第 349 页中的 “12.6.13 处理地址标题行中的注释”
commentmap	第 349 页中的 “12.6.13 处理地址标题行中的注释”
commentomit	第 349 页中的 “12.6.13 处理地址标题行中的注释”
commentstrip	第 349 页中的 “12.6.13 处理地址标题行中的注释”
commenttotal	第 349 页中的 “12.6.13 处理地址标题行中的注释”
connectalias	第 346 页中的 “12.6.5 邮件出队后的地址重写”
connectcanonical	第 346 页中的 “12.6.5 邮件出队后的地址重写”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
copysendpost	第 244 页中的 “返回的失败邮件”
copywarnpost	第 244 页中的 “警告消息”
daemon	第 331 页中的 “12.4.3.10 目标主机选择”
datefour	第 354 页中的 “12.7.4 将日期转换为两位数或四位数”
datetwo	第 354 页中的 “12.7.4 将日期转换为两位数或四位数”
dayofweek	第 355 页中的 “12.7.5 在日期中指定星期几”
defaulthost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名”
defaultmx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持”
defaultnameservers	第 330 页中的 “12.4.3.6 名称服务器查找”
deferralrejectlimit	第 374 页中的 “12.12.8 对错误的 RCPT TO 地址设置限制”
deferred	第 337 页中的 “12.5.2 实现延迟传送日期”
defragment	第 357 页中的 “12.8.2 Message/Partial 邮件的自动片段整理”
dequeue_removeroute	第 352 页中的 “12.6.18 删除源路由”
description	第 374 页中的 “12.12.9 设置 Monitoring Framework 的通道显示”
destinationfilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
destinationnosolicit	第 373 页中的 “12.12.7 NO-SOLICIT SMTP 扩展支持”
destinationspamfilterX	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字”
destinationspamfilterXoptin	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字”
destinationsrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件”
disabledestinationspamfilterX	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字”
disableetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持”
disablesourcespamfilterX	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字”
dispositionchannel	第 368 页中的 “12.12.1 进程通道覆盖”
disconnectbadauthlimit	第 361 页中的 “12.9.1 对不成功验证尝试的次数的限制”
disconnectbadcommandlimit	第 366 页中的 “12.10.3 设置会话限制”
domainetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持”
domainvrfy	第 322 页中的 “12.4.2.4 VRFY 命令支持”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
dropblank	第 347 页中的 “12.6.8 删除非法的空收件人标题”
ehlo	第 321 页中的 “12.4.2.2 EHLO 命令支持”
eightbit	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
eightnegotiate	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
eightstrict	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
errsendpost	第 244 页中的 “返回的失败邮件”
errwarnpost	第 244 页中的 “警告消息”
expandchannel	第 342 页中的 “12.5.9 多个地址扩展”
expandlimit	第 342 页中的 “12.5.9 多个地址扩展”
expnallow	第 323 页中的 “12.4.2.5 EXPN 支持”
expndisable	第 323 页中的 “12.4.2.5 EXPN 支持”
expndefault	第 323 页中的 “12.4.2.5 EXPN 支持”
exproute	第 345 页中的 “12.6.3 在地址中添加路由信息”
fileinto	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
filesperjob	第 339 页中的 “12.5.5 服务作业限制”
filter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
forwardcheckdelete	第 328 页中的 “12.4.3.3 反向 DNS 查找”
forwardchecknone	第 328 页中的 “12.4.3.3 反向 DNS 查找”
forwardchecktag	第 328 页中的 “12.4.3.3 反向 DNS 查找”
header_733	第 343 页中的 “12.6.1 地址类型和约定”
header_822	第 343 页中的 “12.6.1 地址类型和约定”
header_uucp	第 343 页中的 “12.6.1 地址类型和约定”
headerlabelalign	第 355 页中的 “12.7.7 标题对齐和折叠”
headerlimit	第 365 页中的 “12.9.8 限制标题大小”
headerlinelength	第 355 页中的 “12.7.7 标题对齐和折叠”
headerread	第 353 页中的 “12.7.2 删除选定的邮件标题行”
headertrim	第 353 页中的 “12.7.2 删除选定的邮件标题行”
holdexquota	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
holdlimit	第 342 页中的 “12.5.9 多个地址扩展”
identnone	第 328 页中的 “12.4.3.4 IDENT 查找”
identnonelimited	第 328 页中的 “12.4.3.4 IDENT 查找”
identnonenumeric	第 328 页中的 “12.4.3.4 IDENT 查找”
identnonesymbolic	第 328 页中的 “12.4.3.4 IDENT 查找”
identtcp	第 328 页中的 “12.4.3.4 IDENT 查找”
identtcplimited	第 328 页中的 “12.4.3.4 IDENT 查找”
identtcpsymbolic	第 328 页中的 “12.4.3.4 IDENT 查找”
ignoreencoding	第 357 页中的 “12.8.1 忽略 Encoding 标题行”
ignoremessageencoding	第 360 页中的 “12.8.5 解释 Multiparts 和 Message/RFC822 部分的内容传输编码字段”
ignoremultipartencoding	第 360 页中的 “12.8.5 解释 Multiparts 和 Message/RFC822 部分的内容传输编码字段”
immnonurgent	第 337 页中的 “12.5.2 实现延迟传送日期”
improute	第 345 页中的 “12.6.3 在地址中添加路由信息”
includefinal	第 244 页中的 “10.10.4.4 在状态通知邮件中包含已变更的地址”
inenttcpnumeric	第 328 页中的 “12.4.3.4 IDENT 查找”
inner	第 353 页中的 “12.7.1 重写嵌入式标题”
innertrim	第 353 页中的 “12.7.2 删除选定的邮件标题行”
interfaceaddress	第 327 页中的 “12.4.3.1 TCP/IP 端口号和接口地址”
interpretencoding	第 357 页中的 “12.8.1 忽略 Encoding 标题行”
interpretmessageencoding	第 360 页中的 “12.8.5 解释 Multiparts 和 Message/RFC822 部分的内容传输编码字段”
interpretmultipartencoding	第 360 页中的 “12.8.5 解释 Multiparts 和 Message/RFC822 部分的内容传输编码字段”
language	第 356 页中的 “12.7.10 设置标题中的默认语言”
lastresort	第 330 页中的 “12.4.3.7 最后可用的主机”
linelength	第 360 页中的 “12.8.4 实施邮件行长度限制”
linelimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
localvrfy	第 322 页中的 “12.4.2.4 VRFY 命令支持”
logging	第 366 页中的 “12.11.1 记录关键字”
logheader	第 366 页中的 “12.11.1 记录关键字”
loopcheck	第 367 页中的 “12.11.3 设置 Loopcheck”
mailfromdnsverify	第 323 页中的 “12.4.2.6 DNS 域验证”
master	第 337 页中的 “12.5.1 设置通道方向性”
master_debug	第 367 页中的 “12.11.2 调试关键字”
maxblocks	第 359 页中的 “12.8.3 大型邮件的自动分段”
maxheaderaddrs	第 355 页中的 “12.7.6 自动分割长标题行”
maxheaderchars	第 355 页中的 “12.7.6 自动分割长标题行”
maxjobs	第 339 页中的 “12.5.5 服务作业限制”
maxlines	第 359 页中的 “12.8.3 大型邮件的自动分段”
maxprocchars	第 355 页中的 “12.7.7 标题对齐和折叠”
maysaslserver	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS”
maytls	第 334 页中的 “12.4.8 传输层安全性”
maytlsclient	第 334 页中的 “12.4.8 传输层安全性”
maytlsserver	第 334 页中的 “12.4.8 传输层安全性”
missingrecipientpolicy	第 347 页中的 “12.6.7 使缺少收件人标题行的邮件合法化”
msexchange	第 334 页中的 “12.4.7 指定 Microsoft Exchange 网关通道”
multiple	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送”
mustsaslserver	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS”
musttls	第 334 页中的 “12.4.8 传输层安全性”
musttlsclient	第 334 页中的 “12.4.8 传输层安全性”
musttlsserver	第 334 页中的 “12.4.8 传输层安全性”
mx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持”
namelengthlimit	第 364 页中的 “12.9.6 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”
nameservers	第 330 页中的 “12.4.3.6 名称服务器查找”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
noaddresssrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件”
noaddreturnpath	第 348 页中的 “12.6.11 生成 Return-path 标题行”
nobangoverpercent	第 345 页中的 “12.6.3 在地址中添加路由信息”
noblocklimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制”
nocache	第 327 页中的 “12.4.3.2 缓存通道连接信息”
nochannelfilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
nochunkingclient	第 334 页中的 “12.4.6 支持 SMTP Chunking”
nochunkingserver	第 334 页中的 “12.4.6 支持 SMTP Chunking”
nodayofweek	第 355 页中的 “12.7.5 在日期中指定星期几”
nodefaulthost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名”
nodeferred	第 337 页中的 “12.5.2 实现延迟传送日期”
nodefragment	第 357 页中的 “12.8.2 Message/Partial 邮件的自动片段整理”
nodestinationfilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
nodestinationsrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件”
nodropblank	第 347 页中的 “12.6.8 删除非法的空收件人标题”
noehlo	第 321 页中的 “12.4.2.2 EHLO 命令支持”
noexproute	第 345 页中的 “12.6.3 在地址中添加路由信息”
noexquota	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送”
nofileinto	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
nofilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
noheaderread	第 353 页中的 “12.7.2 删除选定的邮件标题行”
noheadertrim	第 353 页中的 “12.7.2 删除选定的邮件标题行”
noimproute	第 345 页中的 “12.6.3 在地址中添加路由信息”
noinner	第 353 页中的 “12.7.1 重写嵌入式标题”
noinnertrim	第 353 页中的 “12.7.2 删除选定的邮件标题行”
nolinelimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
nologging	第 366 页中的 “12.11.1 记录关键字”
noloopcheck	第 367 页中的 “12.11.3 设置 Loopcheck”
nomailfromdnsverify	第 323 页中的 “12.4.2.6 DNS 域验证”
nomaster_debug	第 367 页中的 “12.11.2 调试关键字”
nomsexchange	第 325 页中的 “12.4.3 TCP/IP 连接和 DNS 查找支持”
nomx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持”
norandomemx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持”
nosourcesrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件”
nonurgentbackoff	第 337 页中的 “12.5.3 为传送失败的邮件指定重试频率”
nonurgentblocklimit	第 341 页中的 “12.5.7 基于大小的邮件优先级”
nonurgentnotices	第 243 页中的 “10.10.4.3 设置通知邮件传送间隔”
noreceivedfor	第 349 页中的 “12.6.12 从信封 To 和 From 地址构建 Received 标题行”
noreceivedfrom	第 349 页中的 “12.6.12 从信封 To 和 From 地址构建 Received 标题行”
noremotehost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名”
norestricted	第 348 页中的 “12.6.10 启用限制的邮箱编码”
noreturnaddress	第 245 页中的 “邮寄主管返回的邮件内容”
noreturnpersonal	第 245 页中的 “邮寄主管返回的邮件内容”
noreverse	第 348 页中的 “12.6.9 启用特定于通道的反向数据库使用”
normalbackoff	第 337 页中的 “12.5.3 为传送失败的邮件指定重试频率”
normalblocklimit	第 341 页中的 “12.5.7 基于大小的邮件优先级”
normalnotices	第 243 页中的 “10.10.4.3 设置通知邮件传送间隔”
norules	第 351 页中的 “12.6.17 启用特定于通道的重写规则检查”
nosasl	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS”
nosaslserver	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS”
nosaslswitchchannel	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS”
nosendetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持”
nosendpost	第 244 页中的 “返回的失败邮件”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
noservice	第 343 页中的 “12.5.10 启用服务转换”
noslave_debug	第 367 页中的 “12.11.2 调试关键字”
nosmtp	第 320 页中的 “12.4.2.1 通道协议选定和行终止符”
nosourcefilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
noswitchchannel	第 330 页中的 “12.4.3.8 外来邮件的备用通道（切换通道）”
notices	第 243 页中的 “10.10.4.3 设置通知邮件传送间隔”
notificationchannel	第 368 页中的 “12.12.1 进程通道覆盖”
notls	第 334 页中的 “12.4.8 传输层安全性”
notlsclient	第 334 页中的 “12.4.8 传输层安全性”
notlsserver	第 334 页中的 “12.4.8 传输层安全性”
novrfy	第 322 页中的 “12.4.2.4 VRFY 命令支持”
nowarnpost	第 244 页中的 “警告消息”
nox_env_to	第 354 页中的 “12.7.3 生成/删除 X-Envelope-to 标题行”
parameterlengthlimit	第 364 页中的 “12.9.6 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”
percentonly	第 345 页中的 “12.6.3 在地址中添加路由信息”
percents	第 343 页中的 “12.6.1 地址类型和约定”
personalinc	第 350 页中的 “12.6.14 处理地址标题行中的个人名称”
personalmap	第 350 页中的 “12.6.14 处理地址标题行中的个人名称”
personalomit	第 350 页中的 “12.6.14 处理地址标题行中的个人名称”
personalstrip	第 350 页中的 “12.6.14 处理地址标题行中的个人名称”
pool	第 339 页中的 “12.5.4 用于通道执行作业的处理池”
port	第 327 页中的 “12.4.3.1 TCP/IP 端口号和接口地址”
postheadbody	第 245 页中的 “邮寄主管返回的邮件内容”
postheadonly	第 245 页中的 “邮寄主管返回的邮件内容”
randommx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持”
receivedfor	第 349 页中的 “12.6.12 从信封 To 和 From 地址构建 Received 标题行”
receivedfrom	第 349 页中的 “12.6.12 从信封 To 和 From 地址构建 Received 标题行”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
recipientcutoff	第 364 页中的 “12.9.7 对邮件收件人进行限制”
recipientlimit	第 364 页中的 “12.9.7 对邮件收件人进行限制”
rejectsmtplonglines	第 364 页中的 “12.9.5 处理包含超过 1000 个字符的行的 SMTP 邮件”
remotehost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名”
restricted	第 348 页中的 “12.6.10 启用限制的邮箱编码”
returnaddress	第 245 页中的 “邮寄主管返回的邮件内容”
returnenvelope	第 245 页中的 “空的信封返回地址”
returnpersonal	第 245 页中的 “邮寄主管返回的邮件内容”
reverse	第 348 页中的 “12.6.9 启用特定于通道的反向数据库使用”
routelocal	第 346 页中的 “12.6.4 禁用显式路由地址的重写”
rules	第 351 页中的 “12.6.17 启用特定于通道的重写规则检查”
saslswitchchannel	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS”
sendetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持”
sendpost	第 244 页中的 “返回的失败邮件”
sensitivitycompanyconfidential	第 356 页中的 “12.7.9 敏感度检查”
sensitivitynormal	第 356 页中的 “12.7.9 敏感度检查”
sensitivitypersonal	第 356 页中的 “12.7.9 敏感度检查”
sensitivityprivate	第 356 页中的 “12.7.9 敏感度检查”
service	第 343 页中的 “12.5.10 启用服务转换”
sevenbit	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
silentetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持”
single	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送”
single_sys	第 331 页中的 “12.4.3.10 目标主机选择”
slave	第 337 页中的 “12.5.1 设置通道方向性”
slave_debug	第 367 页中的 “12.11.2 调试关键字”
smtp	第 320 页中的 “12.4.2.1 通道协议选定和行终止符”
smtp_cr	第 320 页中的 “12.4.2.1 通道协议选定和行终止符”
smtp_crlf	第 320 页中的 “12.4.2.1 通道协议选定和行终止符”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
smtp_crorlf	第 320 页中的 “12.4.2.1 通道协议选定和行终止符”
smtp_lf	第 320 页中的 “12.4.2.1 通道协议选定和行终止符”
sourceblocklimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制”
sourcecommentinc	第 349 页中的 “12.6.13 处理地址标题行中的注释”
sourcecommentmap	第 349 页中的 “12.6.13 处理地址标题行中的注释”
sourcecommentomit	第 349 页中的 “12.6.13 处理地址标题行中的注释”
sourcecommentstrip	第 349 页中的 “12.6.13 处理地址标题行中的注释”
sourcecommenttotal	第 349 页中的 “12.6.13 处理地址标题行中的注释”
sourcefilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”
sourcenosolicit	第 373 页中的 “12.12.7 NO-SOLICIT SMTP 扩展支持”
sourcepersonalinc	第 350 页中的 “12.6.14 处理地址标题行中的个人名称”
sourcepersonalmap	第 350 页中的 “12.6.14 处理地址标题行中的个人名称”
sourcepersonalomit	第 350 页中的 “12.6.14 处理地址标题行中的个人名称”
sourcepersonalstrip	第 350 页中的 “12.6.14 处理地址标题行中的个人名称”
sourceroute	第 343 页中的 “12.6.1 地址类型和约定”
sourcespamfilterX	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字”
sourcespamfilterXoptin	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字”
sourcesrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件”
streaming	第 325 页中的 “12.4.2.8 协议流”
subaddressexact	第 351 页中的 “12.6.16 子地址处理”
subaddressrelaxed	第 351 页中的 “12.6.16 子地址处理”
subaddresswild	第 351 页中的 “12.6.16 子地址处理”
subdirs	第 366 页中的 “12.10.2 分布通道邮件队列到多个子目录”
submit	第 368 页中的 “12.12.2 通道操作类型”
suppressfinal	第 244 页中的 “10.10.4.4 在状态通知邮件中包含已变更的地址”
switchchannel	第 330 页中的 “12.4.3.8 外来邮件的备用通道（切换通道）”
threaddepth	第 341 页中的 “12.5.8 SMTP 通道线程”

表 12–1 按字母顺序排列的通道关键字列表 （续）

关键字	有关更多信息...
tlsswitchchannel	第 334 页中的 “12.4.8 传输层安全性”
transactionlimit	第 340 页中的 “12.5.6 设置连接事务限制”
truncatesmtplonglines	第 364 页中的 “12.9.5 处理包含超过 1000 个字符的行的 SMTP 邮件”
unrestricted	第 348 页中的 “12.6.10 启用限制的邮箱编码”
urgentbackoff	第 337 页中的 “12.5.3 为传送失败的邮件指定重试频率”
urgentblocklimit	第 341 页中的 “12.5.7 基于大小的邮件优先级”
urgentnotices	第 243 页中的 “10.10.4.3 设置通知邮件传送间隔”
useintermediate	第 244 页中的 “10.10.4.4 在状态通知邮件中包含已变更的地址”
user	第 368 页中的 “12.12.3 Pipe 通道”
userswitchchannel	第 331 页中的 “12.4.3.9 基于用户或域设置的源通道切换”
uucp	第 343 页中的 “12.6.1 地址类型和约定”
viaaliasoptional	第 352 页中的 “12.6.19 必须从别名指定地址”
viaaliasrequired	第 352 页中的 “12.6.19 必须从别名指定地址”
vrfyallow	第 322 页中的 “12.4.2.4 VRFY 命令支持”
vrfydefault	第 322 页中的 “12.4.2.4 VRFY 命令支持”
vrfyhide	第 322 页中的 “12.4.2.4 VRFY 命令支持”
warnpost	第 244 页中的 “警告消息”
wrapsmtplonglines	第 364 页中的 “12.9.5 处理包含超过 1000 个字符的行的 SMTP 邮件”
x_env_to	第 354 页中的 “12.7.3 生成/删除 X-Envelope-to 标题行”

12.3 按功能分类的通道关键字

以下各表是分类后的关键字列表。表和类别如下所示：

- 表 12–2 地址处理关键字
- 表 12–3 附件和 MIME 处理
- 表 12–4 字符集和八位数据
- 表 12–5 MTA 队列区域中的文件创建
- 表 12–6 标题关键字
- 表 12–7 传入通道匹配和切换关键字
- 表 12–8 日志记录和调试通道关键字
- 表 12–9 长型地址列表或标题通道关键字
- 表 12–10 邮箱过滤器通道关键字

表 12–2 地址处理关键字

关键字	页 定义
地址处理	
733	在信封中使用 % 路由；与 `percents` 同义。第 343 页中的 “12.6.1 地址类型和约定”
822	第 343 页中的 “12.6.1 地址类型和约定” 在信封中使用源路由；与 `sourceroute` 相同。
addreturnpath	第 348 页中的 “12.6.11 生成 Return-path 标题行” 向加入此通道队列的邮件添加 `Return-path:` 标题。
aliaslocal	第 350 页中的 “12.6.15 指定别名文件和别名数据库探测” 在别名文件和别名数据库中查找重写的地址。
authrewrite	第 325 页中的 “12.4.3 TCP/IP 连接和 DNS 查找支持” 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	第 345 页中的 “12.6.3 在地址中添加路由信息” 将 A!B%C 分组为 A!(B%C)
bangstyle	第 343 页中的 “12.6.1 地址类型和约定” 在信封中使用 UUCP ! 路由；与 `uucp` 同义。
defaulthost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名” 指定用于完成地址的域名
dequeue_removeroute	第 352 页中的 “12.6.18 删除源路由” 从信封 `To:` 地址中删除源路由。
exproute	第 345 页中的 “12.6.3 在地址中添加路由信息” 将地址传递到远程系统时，要求显式路由。

表 12–2 地址处理关键字 （续）

关键字	页 定义
holdlimit	第 342 页中的 “12.5.9 多个地址扩展”
	当信封收件人地址的数量超过此限制时，将保留邮件。
improute	第 345 页中的 “12.6.3 在地址中添加路由信息”
	此通道地址的隐式路由
missingrecipientpolicy	第 347 页中的 “12.6.7 使缺少收件人标题行的邮件合法化”
	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	第 348 页中的 “12.6.11 生成 Return-path 标题行”
	使邮件入队时不要添加 `Return-path:` 标题。
nobangoverpercent	第 345 页中的 “12.6.3 在地址中添加路由信息”
	将 A!B%C 分组为 (A!B)%C
nodefaulthost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名”
	不指定用于完成地址的域名
noexproute	第 345 页中的 “12.6.3 在地址中添加路由信息”
	没有用于此通道地址的显式路由
noimproute	第 345 页中的 “12.6.3 在地址中添加路由信息”
	没有用于此通道地址的隐式路由
noreceivedfrom	第 349 页中的 “12.6.12 从信封 To 和 From 地址构建 Received 标题行”
	构建 `Received:` 标题行，不包含原始信封的 From: 地址。
noremotehost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名”
	使用本地主机的域名作为默认域名来完成地址
norestricted	第 348 页中的 “12.6.10 启用限制的邮箱编码”
	与 `unsrestricted` 相同。
noreverse	第 348 页中的 “12.6.9 启用特定于通道的反向数据库使用”
	使邮件地址免受地址反向处理
norules	第 351 页中的 “12.6.17 启用特定于通道的重写规则检查”
	不对此通道强制执行特定于通道的重写规则检查。
percentonly	第 345 页中的 “12.6.3 在地址中添加路由信息”
	忽略 bang 路径。在信封中使用 % 路由。

表 12–2 地址处理关键字 （续）

关键字	页 定义
percents	第 343 页中的 “12.6.1 地址类型和约定”
	在信封中使用 % 路由；与 733 同义。
remotehost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名”
	使用远程主机的名称作为默认域名来完成地址
restricted	第 348 页中的 “12.6.10 启用限制的邮箱编码”
	通道连接到需要编码的邮件系统。
reverse	第 348 页中的 “12.6.9 启用特定于通道的反向数据库使用”
	已根据地址反向数据库或 REVERSE 映射检查地址
routelocal	第 346 页中的 “12.6.4 禁用显式路由地址的重写”
	向通道重写地址时，使 MTA 尝试让地址中的所有显式路由“短路”。
rules	第 351 页中的 “12.6.17 启用特定于通道的重写规则检查”
	对此通道强制执行针对通道的重写规则检查。
sourceroute	第 343 页中的 “12.6.1 地址类型和约定”
	与 822 同义。
subaddressexact	第 351 页中的 “12.6.16 子地址处理”
	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	第 351 页中的 “12.6.16 子地址处理”
	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。
subaddresswild	第 351 页中的 “12.6.16 子地址处理”
	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	第 348 页中的 “12.6.10 启用限制的邮箱编码”
	通知 MTA 不执行 RFC 1137 编码和解码。
uucp	第 343 页中的 “12.6.1 地址类型和约定”
	在信封中使用 UUCP! 路由；与 bangstyle 同义。
viaaliasoptional	第 352 页中的 “12.6.19 必须从别名指定地址”
	不要求别名生成与通道相匹配的最终收件人地址。
viaaliasrequired	第 352 页中的 “12.6.19 必须从别名指定地址”
	与通道匹配的最终收件人地址必须由别名生成。

表 12–3 附件和 MIME 处理

关键字	定义
defragment	第 357 页中的 “12.8.2 Message/Partial 邮件的自动片段整理”
	将在通道排队的部分邮件放置到片段整理通道队列中。
ignoreencoding	第 357 页中的 “12.8.1 忽略 Encoding 标题行”
	忽略外来邮件中的“**编码**:”标题。
ignoremessageencoding	第 360 页中的 “12.8.5 解释 Multiparts 和 Message/RFC822 部分的内容传输编码字段”
	忽略外来邮件 message/rfc822 部分的内容传输编码字段。
ignoremultipartencoding	第 360 页中的 “12.8.5 解释 Multiparts 和 Message/RFC822 部分的内容传输编码字段”
	忽略外来邮件 multiparts 部分的内容传输编码字段。
interpretencoding	第 357 页中的 “12.8.1 忽略 Encoding 标题行”
	解释外来邮件中的“**编码**:”标题（如果需要）。
interpretmessageencoding	第 360 页中的 “12.8.5 解释 Multiparts 和 Message/RFC822 部分的内容传输编码字段”
	解释外来邮件 message/rfc822 部分的内容传输编码字段。
interpretmultipartencoding	第 360 页中的 “12.8.5 解释 Multiparts 和 Message/RFC822 部分的内容传输编码字段”
	解释外来邮件 multiparts 部分的内容传输编码字段。
nodefragment	第 357 页中的 “12.8.2 Message/Partial 邮件的自动片段整理”
	禁用片段整理。

表 12–4 字符集和八位数据

关键字	定义
charset7	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
	与 7 位文本邮件关联的默认字符集
charset8	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
	与 8 位文本邮件关联的默认字符集
charsetesc	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
	与包含换码符的 7 位文本关联的默认字符集
eightbit	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据”
	通道支持八位字符。

表 12–4 字符集和八位数据 （续）

关键字	定义
eightnegotiate	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据” 如果可能，通道应对使用八位传输进行协商。
eightstrict	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据” 拒绝包含未经协商的八位数据标题的邮件。
sevenbit	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据” 不支持 8 位字符；必须对 8 位字符进行编码。

表 12–5 MTA队列区域中的文件创建

关键字	页 定义
addrsperfile	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送” 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	第 342 页中的 “12.5.9 多个地址扩展” 指定由于应用 expandlimit 而在其中执行延迟扩展的通道。
expandlimit	第 342 页中的 “12.5.9 多个地址扩展” 地址数目超过此限制时，“脱机”处理外来邮件。
multiple	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送” 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	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送” 为通道中每个目标地址分别创建一个邮件副本。
single_sys	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送” 为所用的每个目标系统创建一个邮件副本。
subdirs	第 366 页中的 “12.10.2 分布通道邮件队列到多个子目录” 指定将在其中分布通道队列的邮件的子目录的数量。

表 12–6 标题关键字

关键字	定义
authrewrite	第 325 页中的 “12.4.3 TCP/IP 连接和 DNS 查找支持” 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。

表 12–6 标题关键字 （续）

关键字	定义
commentinc	第 349 页中的 “12.6.13 处理地址标题行中的注释” 完好保留邮件标题行中的注释。
commentmap	第 349 页中的 “12.6.13 处理地址标题行中的注释” 通过 COMMENT_STRINGS 映射表运行邮件标题行中的注释字符串。
commentomit	第 349 页中的 “12.6.13 处理地址标题行中的注释” 从邮件标题行中删除注释。
commentstrip	第 349 页中的 “12.6.13 处理地址标题行中的注释” 从邮件标题行的注释字段中删除有问题的字符。
commenttotal	第 349 页中的 “12.6.13 处理地址标题行中的注释” 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	第 354 页中的 “12.7.4 将日期转换为两位数或四位数” 将所有年份字段扩展为四位数。
datetwo	第 354 页中的 “12.7.4 将日期转换为两位数或四位数” 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	第 355 页中的 “12.7.5 在日期中指定星期几” 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	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名” 指定用于完成地址的域名
deletemessagehash	第 356 页中的 “12.7.11 控制 Message-hash: 标题” 删除所有现有 Message-hash: 字段。
dropblank	第 347 页中的 “12.6.8 删除非法的空收件人标题” 删除外来邮件中的非法空标题。
generatemessagehash	第 356 页中的 “12.7.11 控制 Message-hash: 标题” 如果在目标通道中指定该关键字，将导致 Message-hash: 标题字段被插入到邮件中。
header_733	第 343 页中的 “12.6.1 地址类型和约定” 在邮件标题中使用 % 路由。

表 12–6 标题关键字 （续）

关键字	定义
header_822	第 343 页中的 “12.6.1 地址类型和约定” 在邮件标题中使用源路由。
headerlabelalign	第 355 页中的 “12.7.7 标题对齐和折叠” 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	第 355 页中的 “12.7.7 标题对齐和折叠” 控制加入此通道队列的标题行的长度。
headerread	第 353 页中的 “12.7.2 删除选定的邮件标题行” 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	第 353 页中的 “12.7.2 删除选定的邮件标题行” 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	第 343 页中的 “12.6.1 地址类型和约定” 在标题中使用!路由
inner	第 353 页中的 “12.7.1 重写嵌入式标题” 分析邮件并重写内部标题。
innertrim	第 353 页中的 “12.7.2 删除选定的邮件标题行” 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）。
keepmessagehash	第 356 页中的 “12.7.11 控制 `Message-hash:` 标题” 保留所有现有 `Message-hash:` 字段。
language	第 356 页中的 “12.7.10 设置标题中的默认语言” 指定标题的默认语言。
maxheaderaddrs	第 355 页中的 “12.7.6 自动分割长标题行” 控制一行中可以显示的地址数量。
maxheaderchars	第 355 页中的 “12.7.6 自动分割长标题行” 控制一行中可以显示的字符数量。
missingrecipientpolicy	第 347 页中的 “12.6.7 使缺少收件人标题行的邮件合法化” 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。

表 12–6 标题关键字 （续）

关键字	定义
nodayofweek	第 355 页中的 “12.7.5 在日期中指定星期几” 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	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名” 不指定用于完成地址的域名
nodropblank	第 347 页中的 “12.6.8 删除非法的空收件人标题” 不删除外来邮件中的非法空标题。
noheaderread	第 353 页中的 “12.7.2 删除选定的邮件标题行” 不应用选项文件中的标题剪裁规则。
noheadertrim	第 353 页中的 “12.7.2 删除选定的邮件标题行” 不应用选项文件中的标题剪裁规则。
noinner	第 353 页中的 “12.7.1 重写嵌入式标题” 不重写内部邮件标题行。
noinnertrim	第 353 页中的 “12.7.2 删除选定的邮件标题行” 不对内部邮件标题应用标题剪裁。
noreceivedfor	第 349 页中的 “12.6.12 从信封 To 和 From 地址构建 Received 标题行” 构建 `Received:` 标题行而不包含任何信封收件人信息。
noreceivedfrom	第 349 页中的 “12.6.12 从信封 To 和 From 地址构建 Received 标题行” 构建 `Received:` 标题行，不包含原始信封的 From: 地址。
noremotehost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名” 使用本地主机的域名作为默认域名来完成地址
noreverse	第 348 页中的 “12.6.9 启用特定于通道的反向数据库使用” 使在此通道排队的邮件地址免受地址反向处理
norules	第 351 页中的 “12.6.17 启用特定于通道的重写规则检查” 不对此通道强制执行特定于通道的重写规则检查。
nox_env_to	第 354 页中的 “12.7.3 生成/删除 X-Envelope-to 标题行” 删除 `X-Envelope-to` 标题行。
personalinc	第 350 页中的 “12.6.14 处理地址标题行中的个人名称” 完好保留邮件标题行中的个人名称字段。

表 12–6 标题关键字 （续）

关键字	定义
personalmap	第 350 页中的 “12.6.14 处理地址标题行中的个人名称” 通过 PERSONAL_NAMES 映射表运行个人名称。
personalomit	第 350 页中的 “12.6.14 处理地址标题行中的个人名称” 从邮件标题行中删除个人名称字段。
personalstrip	第 350 页中的 “12.6.14 处理地址标题行中的个人名称” 从标题行的个人名称字段中删除有问题的字符。
receivedfor	第 349 页中的 “12.6.12 从信封 To 和 From 地址构建 Received 标题行” 如果邮件只发送给一个信封收件人，则将该信封的 `To:` 地址包含在它构建的 Received: 标题行中。
receivedfrom	第 349 页中的 “12.6.12 从信封 To 和 From 地址构建 Received 标题行” 如果 MTA 已更改信封的 `From:` 地址，则为外来邮件构建 `Received:` 标题行时，应包含原始信封的 `From:` 地址。
remotehost	第 346 页中的 “12.6.6 指定修正不完整地址时使用的主机名” 使用远程主机的名称作为默认域名来完成地址
restricted	第 348 页中的 “12.6.10 启用限制的邮箱编码” 通道连接到需要此编码的邮件系统。
reverse	第 348 页中的 “12.6.9 启用特定于通道的反向数据库使用” 根据地址反向数据库或 REVERSE 映射检查地址
rules	第 351 页中的 “12.6.17 启用特定于通道的重写规则检查” 对此通道强制执行针对通道的重写规则检查。
sensitivitycompanyconfidential	第 356 页中的 “12.7.9 敏感度检查” `Companyconfidential` 是所接受的邮件的敏感度上限。
sensitivitynormal	第 356 页中的 “12.7.9 敏感度检查” `Normal` 是所接受的邮件的敏感度上限。
sensitivitypersonal	第 356 页中的 “12.7.9 敏感度检查” `Personal` 是所接受的邮件的敏感度上限。
sensitivityprivate	第 356 页中的 “12.7.9 敏感度检查” `Private` 是所接受的邮件的敏感度上限。

表 12–6 标题关键字 （续）

关键字	定义
sourcecommentinc	第 349 页中的 “12.6.13 处理地址标题行中的注释” 保留外来邮件标题行中的注释。
sourcecommentmap	第 349 页中的 “12.6.13 处理地址标题行中的注释” 通过源通道运行标题行中的注释字符串。
sourcecommentomit	第 349 页中的 “12.6.13 处理地址标题行中的注释” 删除来自外来邮件标题行（例如，To:、、From: 和 Cc: 标题）删除所有注释。
sourcecommentstrip	第 349 页中的 “12.6.13 处理地址标题行中的注释” 从外来标题行的注释字段中删除有问题的字符。
sourcecommenttotal	第 349 页中的 “12.6.13 处理地址标题行中的注释” 删除外来邮件中的注释（扩号中的内容）。
sourcepersonalinc	第 350 页中的 “12.6.14 处理地址标题行中的个人名称” 完好保留外来邮件标题行中的个人名称。
sourcepersonalmap	第 350 页中的 “12.6.14 处理地址标题行中的个人名称” 通过源通道中运行个人名称。
sourcepersonalomit	第 350 页中的 “12.6.14 处理地址标题行中的个人名称” 从外来邮件标题行中删除个人名称字段。
sourcepersonalstrip	第 350 页中的 “12.6.14 处理地址标题行中的个人名称” 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	第 348 页中的 “12.6.10 启用限制的邮箱编码” 通知 MTA 不执行 RFC 1137 编码和解码。
x_env_to	第 354 页中的 “12.7.3 生成/删除 X-Envelope-to 标题行” 启用生成 `X-Envelope-to` 标题行。

表 12–7 传入通道匹配和切换关键字

关键字	定义
allowswitchchannel	第 330 页中的 “12.4.3.8 外来邮件的备用通道（切换通道）” 允许从 `switchchannel` 通道切换到此通道
nosaslswitchchannel	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS” SASL 验证成功完成后，不切换到此通道

表 12–7 传入通道匹配和切换关键字 （续）

关键字	定义
noswitchchannel	第 330 页中的 “12.4.3.8 外来邮件的备用通道（切换通道）” 不应该切换到此通道或从此通道切换到其他通道。
switchchannel	第 330 页中的 “12.4.3.8 外来邮件的备用通道（切换通道）” 从服务器通道切换到与发件主机关联的通道。
saslswitchchannel	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS” 使外来连接在客户端成功使用 SASL 后切换到指定的通道。
tlsswitchchannel	第 334 页中的 “12.4.8 传输层安全性” TLS 协商成功后，切换到其他通道。
userswitchchannel	第 331 页中的 “12.4.3.9 基于用户或域设置的源通道切换” 根据用户或域设置，切换源通道。

表 12–8 日志记录和调试通道关键字

关键字	定义
日志记录	第 366 页中的 “12.11.1 记录关键字” 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	第 367 页中的 “12.11.3 设置 Loopcheck” 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	第 367 页中的 “12.11.2 调试关键字” 在通道的主程序输出中创建调试输出。
nologging	第 366 页中的 “12.11.1 记录关键字” 不将邮件入队和出队信息记录到日志文件中。
noloopcheck	第 367 页中的 “12.11.3 设置 Loopcheck” 不在 SMTP EHLO 响应标题中放入字符串。
nomaster_debug	第 367 页中的 “12.11.2 调试关键字” 通道的主程序输出中无调试输出。
noslave_debug	第 367 页中的 “12.11.2 调试关键字” 不生成从属调试输出。
slave_debug	第 367 页中的 “12.11.2 调试关键字” 生成从属调试输出。

表 12–9 长型地址列表或标题通道关键字

关键字	定义
expandchannel	第 342 页中的 “12.5.9 多个地址扩展” 指定由于应用 expandlimit 而在其中执行延迟扩展的通道。
expandlimit	第 342 页中的 “12.5.9 多个地址扩展” 地址数目超过此限制时，“脱机”处理外来邮件。
holdlimit	第 342 页中的 “12.5.9 多个地址扩展” 地址数量超过此限制时保留邮件。
maxprocchars	第 355 页中的 “12.7.7 标题对齐和折叠” 可以处理和重写的最大长度的标题。

表 12–10 邮箱过滤器通道关键字

关键字	定义
channelfilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 通道过滤器文件的位置；与 `destinationfilter` 相同。
destinationfilter	应用到外发邮件的通道过滤器文件的位置。
destinationspamfilterX	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字” 通过垃圾邮件过滤软件 X 运行发送到此通道的邮件。不接受垃圾邮件过滤软件参数。
destinationspamfilterXoptin	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字” 通过垃圾邮件过滤软件 X 运行发送到此通道的邮件。
disabledestinationspamfilterX	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字” 对发送到此通道的邮件禁用垃圾邮件过滤器 X。
disablesourcespamfilterX	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字” 对来自此通道的邮件禁用垃圾邮件过滤器 X。
fileinto	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 指定应用邮箱过滤器 `fileinto` 操作时对地址的影响。
filter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 指定用户过滤器文件的位置。
nochannelfilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 不对外发邮件进行通道过滤。也称为 `nodestinationfilter`。

表 12–10 邮箱过滤器通道关键字 （续）

关键字	定义
nodestinationfilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 不对外发邮件执行通道过滤。
nofileinto	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 邮箱过滤器 fileinto 操作无影响。
nofilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 不执行用户邮箱过滤。
nosourcefilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 不对外来邮件执行通道过滤。
sourcefilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 为外来邮件指定通道过滤器文件的位置。
sourcespamfilterX	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字” 通过垃圾邮件过滤软件 X 运行源自此通道的邮件。不接受垃圾邮件过滤软件参数。
sourcespamfilterXoptin	第 369 页中的 “12.12.5 垃圾邮件过滤器关键字” 通过垃圾邮件过滤软件 X 运行源自此通道的邮件。接受垃圾邮件过滤软件参数。

表 12–11 NO-SOLICIT SMTP 扩展支持关键字

关键字	定义
sourcenosolicit	第 373 页中的 “12.12.7 NO-SOLICIT SMTP 扩展支持” 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。
destinationnosolicit	第 373 页中的 “12.12.7 NO-SOLICIT SMTP 扩展支持” 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。

表 12–12 通知和邮寄主管邮件关键字

关键字	定义
（有关完整的通知过程，请参见第 237 页中的 “10.10 控制传送状态通知邮件”）	
aliaspostmaster	第 245 页中的 “邮寄主管返回的邮件内容” 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	第 244 页中的 “返回的失败邮件” 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。

表 12–12 通知和邮寄主管邮件关键字 （续）

关键字	定义
copywarnpost	第 244 页中的 “警告消息”
	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	第 244 页中的 “返回的失败邮件”
	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	第 244 页中的 “警告消息”
	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	第 244 页中的 “10.10.4.4 在状态通知邮件中包含已变更的地址”
	传送通知时包含收件人地址的最终格式。
nonurgentnotices	第 243 页中的 “10.10.4.3 设置通知邮件传送间隔”
	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	第 245 页中的 “邮寄主管返回的邮件内容”
	将 RETURN_ADDRESS 选项值用作邮寄主管地址名称。
noreturnpersonal	第 245 页中的 “邮寄主管返回的邮件内容”
	将 RETURN_PERSONAL 选项值用作邮寄主管个人名称。
normalnotices	第 243 页中的 “10.10.4.3 设置通知邮件传送间隔”
	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	第 244 页中的 “返回的失败邮件”
	禁用向邮寄主管发送所有失败邮件的副本。
notices	第 243 页中的 “10.10.4.3 设置通知邮件传送间隔”
	指定在发送通知和返回邮件之前可能经过的时间。
nowarnpost	第 244 页中的 “警告消息”
	禁用向邮寄主管发送警告消息的副本。
postheadbody	第 245 页中的 “邮寄主管返回的邮件内容”
	同时返回邮件的标题和内容。
postheadonly	第 245 页中的 “邮寄主管返回的邮件内容”
	仅向邮寄主管返回标题。
returnaddress	第 245 页中的 “邮寄主管返回的邮件内容”
	指定本地邮寄主管的返回地址。

表 12–12 通知和邮寄主管邮件关键字 （续）

关键字	定义
returnenvelope	第 245 页中的 “空的信封返回地址” 控制空的信封返回地址的使用。
returnpersonal	第 245 页中的 “邮寄主管返回的邮件内容” 设置本地邮寄主管的个人名称。
sendpost	第 244 页中的 “返回的失败邮件” 启用向邮寄主管发送所有失败邮件的副本。
suppressfinal	第 244 页中的 “10.10.4.4 在状态通知邮件中包含已变更的地址” 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	第 243 页中的 “10.10.4.3 设置通知邮件传送间隔” 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	第 244 页中的 “10.10.4.4 在状态通知邮件中包含已变更的地址” 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	第 244 页中的 “警告消息” 启用向邮寄主管发送警告消息的副本。

表 12–13 处理控制和作业提交关键字

关键字	定义
（有关功能说明的详细信息，请参见第 335 页中的 “12.5 配置邮件处理和传送”）	
backoff	第 337 页中的 “12.5.3 为传送失败的邮件指定重试频率” 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	第 337 页中的 “12.5.1 设置通道方向性” 主程序和从程序为其服务的通道。
deferred	第 337 页中的 “12.5.2 实现延迟传送日期” 识别 `Deferred-delivery:` 标题行并使其生效。
expandchannel	第 342 页中的 “12.5.9 多个地址扩展” 指定由于应用 expandlimit 而在其中执行延迟扩展的通道。
expandlimit	第 342 页中的 “12.5.9 多个地址扩展” 地址数目超过此限制时，“脱机”处理外来邮件。

表 12–13 处理控制和作业提交关键字 （续）

关键字	定义
filesperjob	第 339 页中的 “12.5.5 服务作业限制”
	将由单个作业处理的队列条目的数量。
immnonurgent	第 337 页中的 “12.5.2 实现延迟传送日期”
	紧急、正常和不紧急邮件提交后，立即开始传送。
master	第 337 页中的 “12.5.1 设置通道方向性”
	主程序 (`master`) 所服务的通道。
maxjobs	第 339 页中的 “12.5.5 服务作业限制”
	可以同时为通道运行的作业的最大数量。
nodeferred	第 337 页中的 “12.5.2 实现延迟传送日期”
	指定不使 `Deferred-delivery:` 标题行生效。
nonurgentbackoff	第 337 页中的 “12.5.3 为传送失败的邮件指定重试频率”
	尝试重新传送非紧急邮件的频率。
nonurgentblocklimit	第 341 页中的 “12.5.7 基于大小的邮件优先级”
	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	第 337 页中的 “12.5.3 为传送失败的邮件指定重试频率”
	尝试重新传送普通邮件的频率。
normalblocklimit	第 341 页中的 “12.5.7 基于大小的邮件优先级”
	将超过此大小的邮件强制降到非紧急优先级。
noservice	第 343 页中的 “12.5.10 启用服务转换”
	必须通过 `CHARSET-CONVERSION` 启用进入此通道的邮件的服务转换。
pool	第 339 页中的 “12.5.4 用于通道执行作业的处理池”
	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	第 343 页中的 “12.5.10 启用服务转换”
	无条件启用服务转换，不考虑 `CHARSET-CONVERSION` 条目。
slave	第 337 页中的 “12.5.1 设置通道方向性”
	由从程序（从）提供服务的通道。
threaddepth	第 341 页中的 “12.5.8 SMTP 通道线程”
	使用多线程 SMTP 客户端触发新线程的邮件的数目。

表 12–13 处理控制和作业提交关键字 （续）

关键字	定义
transactionlimit	限制每个连接允许的邮件数目。
urgentbackoff	第 337 页中的 “12.5.3 为传送失败的邮件指定重试频率” 尝试重新传送紧急邮件的频率。
urgentblocklimit	第 341 页中的 “12.5.7 基于大小的邮件优先级” 将超过此大小的邮件强制降至普通优先级。
user	第 368 页中的 “12.12.3 Pipe 通道” 用于 pipe 通道中，指明通道将在其下运行的用户名称。

表 12–14 敏感度限制关键字

关键字	定义
sensitivitycompanyconfidential	第 356 页中的 “12.7.9 敏感度检查” 所接受的邮件的敏感度上限。
sensitivitynormal	第 356 页中的 “12.7.9 敏感度检查” `Normal` 是所接受的邮件的敏感度上限。
sensitivitypersonal	第 356 页中的 “12.7.9 敏感度检查” `Personal` 是所接受的邮件的敏感度上限。
sensitivityprivate	第 356 页中的 “12.7.9 敏感度检查” `Private` 是所接受的邮件的敏感度上限。

表 12–15 对邮件、用户配额、权限和验证尝试次数的限制关键字

关键字	定义
alternatechannel	第 362 页中的 “12.9.3 重新定向超过大小限制或收件人限制的邮件” alternateblocklimit、alternatelinelimit 及 alternaterecipientlimit 的备用目标通道。
alternateblocklimit	第 362 页中的 “12.9.3 重新定向超过大小限制或收件人限制的邮件” 指定将邮件发送到 alternativechannel 之前邮件中的块数限制。
alternatelinelimit	第 362 页中的 “12.9.3 重新定向超过大小限制或收件人限制的邮件” 指定将邮件发送到 alternativechannel 之前邮件中的行数限制。
alternaterecipientlimit	第 362 页中的 “12.9.3 重新定向超过大小限制或收件人限制的邮件” 指定将邮件发送到 alternativechannel 之前邮件中收件人数量的限制。

表 12–15 对邮件、用户配额、权限和验证尝试次数的限制关键字 （续）

关键字	定义
blocklimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制” 每个邮件中允许的 MTA 块的最大数量。
disconnectbadauthlimit	第 361 页中的 “12.9.1 对不成功验证尝试的次数的限制” 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	第 366 页中的 “12.10.3 设置会话限制” 限制会话错误命令的数量。
disconnectrecipientlimit	第 366 页中的 “12.10.3 设置会话限制” 限制会话收件人的数量。
disconnectrejectlimit	第 366 页中的 “12.10.3 设置会话限制” 限制被拒绝的收件人的数量。
disconnecttransactionlimit	第 366 页中的 “12.10.3 设置会话限制” 限制事务的数量。
headerlimit	第 365 页中的 “12.9.8 限制标题大小” 限制主（最外层）邮件标题的最大大小
holdexquota	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送” 为超过配额的用户保留邮件。
holdlimit	第 342 页中的 “12.5.9 多个地址扩展” 地址数目超过此限制时保留外来邮件。
linelength	第 360 页中的 “12.8.4 实施邮件行长度限制” 基于各个通道限制允许的最大邮件行长度。
linelimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制” 每个邮件中允许的最大行数。
maxblocks	第 359 页中的 “12.8.3 大型邮件的自动分段” 指定邮件中允许的最大块数。
maxlines	第 359 页中的 “12.8.3 大型邮件的自动分段” 指定邮件中允许的最大行数。
nameparameterlengthlimit	第 364 页中的 “12.9.6 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” 控制 name content-type 和 filename content-disposition 参数的截断点。

表 12–15 对邮件、用户配额、权限和验证尝试次数的限制关键字 （续）

关键字	定义
noblocklimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制” 不限制每个邮件中允许的 MTA 块的数量。
noexquota	第 363 页中的 “12.9.4 处理对超过配额用户的邮件传送” 将发给超过配额的用户的所有邮件返回创始者。
nolinelimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制” 不对每个邮件中允许的行数指定限制。
nonurgentblocklimit	第 341 页中的 “12.5.7 基于大小的邮件优先级” 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	第 341 页中的 “12.5.7 基于大小的邮件优先级” 将超过此大小的邮件强制降到非紧急优先级。
parameterlengthlimit	第 364 页中的 “12.9.6 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” 控制通用内容类型和内容处理参数的截断点。
recipientcutoff.	第 364 页中的 “12.9.7 对邮件收件人进行限制” 如果收件人超过此值，则拒绝邮件。
recipientlimit	第 364 页中的 “12.9.7 对邮件收件人进行限制” 限制接受的邮件收件人地址的数量。
rejectsmtplonglines	第 364 页中的 “12.9.5 处理包含超过 1000 个字符的行的 SMTP 邮件” 拒绝包含超过 1000 个字符（包括 CRLF）的行的邮件。
sourceblocklimit	第 361 页中的 “12.9.2 指定绝对邮件大小限制” 每个外来邮件中允许的 MTA 块的最大数量。
truncatesmtplonglines	第 364 页中的 “12.9.5 处理包含超过 1000 个字符的行的 SMTP 邮件” 当行超过 1000 个字符时，将其截断。
wrapsmtplonglines	第 364 页中的 “12.9.5 处理包含超过 1000 个字符的行的 SMTP 邮件” 当行超过 1000 个字符时换行。
urgentblocklimit	第 341 页中的 “12.5.7 基于大小的邮件优先级” 将超过此大小的邮件强制降至普通优先级。

表 12–16 SMTP 验证、SASL 和 TLS 关键字

关键字	定义
（有关功能说明的详细信息，请参见第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS”）	
authrewrite	第 325 页中的 “12.4.3 TCP/IP 连接和 DNS 查找支持” 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	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS” 允许客户端尝试使用 SASL 验证。
maytls	第 334 页中的 “12.4.8 传输层安全性” 使 MTA 向外来连接提供 TLS，并对外发连接尝试 TLS。
maytlsclient	第 334 页中的 “12.4.8 传输层安全性” 发送外发邮件时，如果是发送到支持 TLS 的 SMTP 服务器，MTA SMTP 客户端将尝试使用 TLS。
maytlsserver	第 334 页中的 “12.4.8 传输层安全性” 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	第 334 页中的 “12.4.7 指定 Microsoft Exchange 网关通道” 用于 TCP/IP 通道，通知 MTA 此通道是与 Microsoft Exchange 网关及客户端通信的通道。
mustsaslserver	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS” 除非远程客户端验证成功，否则 SMTP 服务器不接收邮件。
musttls	第 334 页中的 “12.4.8 传输层安全性” 坚持在外发和外来连接中使用 TLS。
musttlsclient	第 334 页中的 “12.4.8 传输层安全性” MTA SMTP 客户端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	第 334 页中的 “12.4.8 传输层安全性” 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。
nomsexchange	第 325 页中的 “12.4.3 TCP/IP 连接和 DNS 查找支持” 默认设置。
nosasl	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS” 不允许或不尝试 SASL 验证。
nosaslserver	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS” 不允许 SASL 验证。

表 12–16 SMTP 验证、SASL 和 TLS 关键字 （续）

关键字	定义
notls	第 334 页中的 “12.4.8 传输层安全性” 不允许或不尝试 TLS。
notlsclient	第 334 页中的 “12.4.8 传输层安全性” MTA SMTP 客户端不对外发连接尝试使用 TLS（外发连接期间不发出 STARTTLS 命令）。
notlsserver	第 334 页中的 “12.4.8 传输层安全性” 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	第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS” 使外来连接在客户端成功使用 SASL 后切换到指定的通道。
tlsswitchchannel	第 334 页中的 “12.4.8 传输层安全性” 使外来连接在客户端的 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。

表 12–17 SMTP 命令和协议关键字

关键字	定义
（有关功能说明的详细信息，请参见第 318 页中的 “12.4.2 SMTP 命令和协议支持”）	
allowetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持” 执行 ETRN 命令。
blocketrn	第 321 页中的 “12.4.2.3 ETRN 命令支持” 阻止 ETRN 命令。
checkehlo	第 321 页中的 “12.4.2.2 EHLO 命令支持” 检查 SMTP 响应标题，以确定使用 EHLO 还是 HELO。
chunkingclient	第 334 页中的 “12.4.6 支持 SMTP Chunking” 启用服务器 chunking 支持（默认）。
chunkingserver	第 334 页中的 “12.4.6 支持 SMTP Chunking” 启用服务器 chunking 支持（默认）。
disableetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持” 禁用对 ETRN SMTP 命令的支持。
domainetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持” 仅执行指定域的那些 ETRN 命令。

表 12–17 SMTP 命令和协议关键字 （续）

关键字	定义
domainvrfy	第 322 页中的 “12.4.2.4 VRFY 命令支持” 使用完整地址发出 VRFY 命令。
ehlo	第 321 页中的 “12.4.2.2 EHLO 命令支持” 在初始连接中使用 SMTP EHLO 命令。
eightbit	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据” 通道支持八位字符。
eightnegotiate	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据” 如果可能，通道应对使用八位传输进行协商。
eightstrict	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据” 拒绝包含未经协商的八位数据标题的邮件。
expnallow	第 323 页中的 “12.4.2.5 EXPN 支持” 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	第 323 页中的 “12.4.2.5 EXPN 支持” 无条件禁用 `EXPN`。
expndefault	第 323 页中的 “12.4.2.5 EXPN 支持” 如果已将 SMTP 服务器设置为允许 EXPN，则允许 `EXPN`。
localvrfy	第 322 页中的 “12.4.2.4 VRFY 命令支持” 使用本地地址发出 VRFY 命令。
mailfromdnsverify	第 323 页中的 “12.4.2.6 DNS 域验证” 验证 `MAIL FROM:` 命令中使用的域存在于 DNS 中。
nochunkingclient	第 334 页中的 “12.4.6 支持 SMTP Chunking” 禁用服务器 chunking 支持。
nochunkingserver	第 334 页中的 “12.4.6 支持 SMTP Chunking” 禁用服务器 chunking 支持。
noehlo	第 321 页中的 “12.4.2.2 EHLO 命令支持” 不使用 EHLO 命令。
nomailfromdnsverify	第 323 页中的 “12.4.2.6 DNS 域验证” 不验证 `MAIL FROM:` 命令中使用的域存在于 DNS 中。

表 12–17 SMTP 命令和协议关键字 （续）

关键字	定义
nosendetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持” 不发送 ETRN 命令。
nosmtp	第 320 页中的 “12.4.2.1 通道协议选定和行终止符” 不支持 SMTP 协议。该值为默认值。
novrfy	第 322 页中的 “12.4.2.4 VRFY 命令支持” 不发出 VRFY 命令。
sendetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持” 发送 ETRN 命令。
sevenbit	第 323 页中的 “12.4.2.7 字符集标记和 8 位数据” 不支持 8 位字符；必须对 8 位字符进行编码。
silentetrn	第 321 页中的 “12.4.2.3 ETRN 命令支持” 执行 ETRN 命令，不回显通道信息。
smtp	第 320 页中的 “12.4.2.1 通道协议选定和行终止符” 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_crlf`。）
smtp_cr	第 320 页中的 “12.4.2.1 通道协议选定和行终止符” 接受以回车 (CR)（不跟换行符 [LF]）终止的行。
smtp_crlf	第 320 页中的 “12.4.2.1 通道协议选定和行终止符” 必须以回车 (CR) 加换行符 (LF) 序列终止行。
smtp_crorlf	第 320 页中的 “12.4.2.1 通道协议选定和行终止符” 可以使用回车 (CR)、换行符 (LF) 序列或完整的 CRLF 终止行。
smtp_lf	第 320 页中的 “12.4.2.1 通道协议选定和行终止符” 接受以换行符 (LF)（前面没有 CR）终止的行。
streaming	第 325 页中的 “12.4.2.8 协议流” 控制与通道关联的协议中使用的协议流的程度。
vrfyallow	第 322 页中的 “12.4.2.4 VRFY 命令支持” 向 VRFY 命令提供信息响应。
vrfydefault	第 322 页中的 “12.4.2.4 VRFY 命令支持” 根据通道的 HIDE_VERIFY 选项设置向 VRFY 命令提供默认响应。

表 12–17 SMTP 命令和协议关键字 （续）

关键字	定义
vrfyhide	第 322 页中的 “12.4.2.4 VRFY 命令支持”
	向 SMTP VRFY 命令提供模糊的响应。

表 12–18 TCP/IP 连接和 DNS 查找支持关键字

关键字	定义
TCP/IP 连接和 DNS 查找支持	
（有关功能说明的详细信息，请参见第 325 页中的 “12.4.3 TCP/IP 连接和 DNS 查找支持”）	
cacheeverything	第 327 页中的 “12.4.3.2 缓存通道连接信息”
	缓存所有连接信息。
cachefailures	第 327 页中的 “12.4.3.2 缓存通道连接信息”
	仅缓存连接失败信息。
cachesuccesses	第 327 页中的 “12.4.3.2 缓存通道连接信息”
	仅缓存连接成功信息。
connectalias	第 346 页中的 “12.6.5 邮件出队后的地址重写”
	传送到收件人地址中列出的任意主机。
connectcanonical	第 346 页中的 “12.6.5 邮件出队后的地址重写”
	连接到 MTA 原本应该连接的系统的主机别名。
daemon	第 331 页中的 “12.4.3.10 目标主机选择”
	连接到特定主机系统而不考虑信封地址。
defaultmx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持”
	通道确定是否从网络中查找 MX。
defaultnameservers	第 330 页中的 “12.4.3.6 名称服务器查找”
	查看 TCP/IP 栈选择的名称服务器。
forwardcheckdelete	第 328 页中的 “12.4.3.3 反向 DNS 查找”
	如果已执行反向 DNS 查找，则接下来对返回的名称执行正向查找，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	第 328 页中的 “12.4.3.3 反向 DNS 查找”
	DNS 反向查找后不执行正向查找。

表 12–18 TCP/IP 连接和 DNS 查找支持关键字 （续）

关键字	定义
forwardchecktag	第 328 页中的 “12.4.3.3 反向 DNS 查找” 如果已执行反向 DNS 查找，则接下来对返回的名称执行正向查找，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	第 328 页中的 “12.4.3.4 IDENT 查找” 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	第 328 页中的 “12.4.3.4 IDENT 查找” 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	第 328 页中的 “12.4.3.4 IDENT 查找” 不执行 IDENT 查找或 IP 到主机名的转换。
identnonesymbolic	第 328 页中的 “12.4.3.4 IDENT 查找” 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	第 328 页中的 “12.4.3.4 IDENT 查找” 对外来 SMTP 连接执行 IDENT 查找并执行 IP 到主机名的转换；在 `Received:` 标题中包含主机名和 IP 地址。
identtcplimited	第 328 页中的 “12.4.3.4 IDENT 查找” 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	第 328 页中的 “12.4.3.4 IDENT 查找” 对外来 SMTP 连接执行 IDENT 查找，但不执行 IP 到主机名的转换。
identtcpsymbolic	第 328 页中的 “12.4.3.4 IDENT 查找” 对外来 SMTP 连接执行 IDENT 查找并执行 IP 到主机名的转换；在 `Received:` 标题中仅包含主机名。
interfaceaddress	第 327 页中的 “12.4.3.1 TCP/IP 端口号和接口地址” 绑定到指定的 TCP/IP 接口地址。
lastresort	第 330 页中的 “12.4.3.7 最后可用的主机” 指定最后可用的主机。
mailfromdnsverify	第 323 页中的 “12.4.2.6 DNS 域验证” 验证 `MAIL FROM:` 命令中使用的域存在于 DNS 中。
mx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持” TCP/IP 网络和软件支持 MX 记录查找。

表 12–18 TCP/IP 连接和 DNS 查找支持关键字 （续）

关键字	定义
nameservers	第 330 页中的 “12.4.3.6 名称服务器查找” 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 需要用于名称服务器且以空格分隔的 IP 地址列表。
nocache	第 327 页中的 “12.4.3.2 缓存通道连接信息” 不缓存任何连接信息。
nomailfromdnsverify	第 323 页中的 “12.4.2.6 DNS 域验证” 不验证 MAIL FROM: 命令中使用的域存在于 DNS 中。
nomx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持” TCP/IP 网络不支持 MX 查找。
nonrandomemx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持” 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	第 327 页中的 “12.4.3.1 TCP/IP 端口号和接口地址” 指定用于 SMTP 连接的默认端口号。标准端口为 25。
randommx	第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持” 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	第 331 页中的 “12.4.3.10 目标主机选择” 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	第 331 页中的 “12.4.3.10 目标主机选择” 为所用的每个目标系统创建一个邮件副本。
threaddepth	第 341 页中的 “12.5.8 SMTP 通道线程” 使用多线程 SMTP 客户端触发新线程的邮件的数目。

表 12–19 其他关键字

关键字	定义
addresssr	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件” 控制 SRS 编码。
deferralrejectlimit	第 374 页中的 “12.12.8 对错误的 RCPT TO 地址设置限制” 设置错误 RCPT TO: 的数量限制地址

表 12–19 其他关键字 （续）

关键字	定义
caption	第 374 页中的 “12.12.9 设置 Monitoring Framework 的通道显示” 设置 Monitoring Framework 的短通道显示字符串
description	第 374 页中的 “12.12.9 设置 Monitoring Framework 的通道显示” 设置 Monitoring Framework 的通道显示字符串
destinationsrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件” 控制 SRS 编码。
dispositionchannel	第 368 页中的 “12.12.1 进程通道覆盖” 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	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 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	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 使用一个必需的 URL 参数，该参数说明过滤器文件的位置
noaddresssrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件” 控制 SRS 编码。
nodestinationfilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 通道的两个方向都没有启用通道邮箱过滤器。
nodestinationsrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件” 控制 SRS 编码。
nosourcefilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 没有为源通道启用通道邮箱过滤器。
nosourcesrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件” 控制 SRS 编码。
nofilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 没有为通道启用用户邮箱过滤的默认值和方法。
notificationchannel	第 368 页中的 “12.12.1 进程通道覆盖” 将进程通道替换为用于初始队列邮件处理通知 (MDN) 的位置。

表 12–19 其他关键字 （续）

关键字	定义
sourcefilter	第 369 页中的 “12.12.4 指定邮箱过滤器文件位置” 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。
sourcesrs	第 458 页中的 “15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件” 控制 SRS 编码。
submit	第 368 页中的 “12.12.2 通道操作类型” 用于将通道标记为仅用来提交的通道。
user	第 368 页中的 “12.12.3 Pipe 通道” 用于 pipe 通道中，指明通道将在其下运行的用户名称。

12.4 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 12–20 SMTP 通道

通道	定义
`tcp_local`	接收来自远程 SMTP 主机的入站邮件。根据是否使用智能主机/防火墙配置，将出站邮件直接发送到远程 SMTP 主机，或者将出站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）上接受邮件提交（通常来自用户代理）。
`tcp_tas`	各站点用来进行统一邮件服务的 IA 特殊通道。

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，还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* 为通道的名称。有关详细信息，请参阅《Sun Java System Messaging Server 6.3 Administration Reference》中的“Option File”。

本节分为以下小节：

12.4.1 配置 SMTP 通道选项

TCP/IP 通道选项文件控制 TCP/IP 通道的各种特性。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件列表扩展。

使用其他选项文件关键字可以进行以下设置：

- 对每个邮件允许的收件人数量设置限制 (`ALLOW_RECIPIENTS_PER_TRANSACTION`)
- 对每个连接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`）
- 指定客户端通道程序允许的同时出站连接的最大数量 (`MAX_CLIENT_THREADS`)

有关所有通道选项关键字和语法的信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》。

12.4.2 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：

表 12–21 汇总了本节中说明的关键字。

表 12–21 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 12–21 SMTP 命令和协议关键字 （续）

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。

12.4.2.1 通道协议选定和行终止符

关键字：smtp、nosmtp、smtp_crlf 、smtp_cr、smtp_crorlf、smtp_lf

smtp 和 nosmtp 关键字指定通道是否支持 SMTP 协议。smtp 关键字或其变量之一对所有 SMTP 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 将接受为行终止符的字符序列。关键字 smtp_crlf 的意思是必须以回车 (Carriage Return, CR) 加换行符 (Line Feed, 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 邮件并拒绝所有带有非标准行终止符的邮件，则可以指定 stmp_crlf。

12.4.2.2 EHLO 命令支持

关键字：ehlo、noehlo、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 服务器通过提供其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，然后客户端发送旧的 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 客户端实现尝试重新连接并使用 HELO 的策略。但是，如果远程服务器在收到 EHLO 时断开连接并且出现问题，则该策略可能不起作用。

提供了通道关键字 ehlo、noehlo 和 checkehlo，用于处理此类情况。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"。如果找到该字符串，则使用 EHLO；否则，使用 HELO。默认行为将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。

12.4.2.3 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 客户端和服务器可以交互操作，从而使服务器有机会启动对将进入给定主机的邮件队列的处理。

SMTP 客户端可以使用 ETRN 请求远程 SMTP 服务器启动对将发送到 SMTP 客户端的邮件队列的处理。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 客户端在 SMTP ETRN 命令行中指定要向其发送邮件的系统的名称（通常为 SMTP 客户端系统自身的名称）。如果远程 SMTP 服务器支持 ETRN 命令，它将触发一个单独进程的执行过程，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 客户端发出 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，但不回显域所匹配且 MTA 将尝试运行的通道的名称。domainetrn 关键字指定 MTA 仅执行指定了域的 ETRN 命令；另外它还使 MTA 不回显域所匹配且 MTA 将尝试运行的通道的名称。

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。

12.4.2.4 VRFY 命令支持

关键字：domainvrfy、localvrfy、vrfyallow、vrfydefault、vrfyhide

VRFY 命令使 SMTP 客户端能够向 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) 作为其参数。localvrfy 关键字使 MTA 发出仅带有地址中本地部分 (user) 的 VRFY 命令。

响应 VRFY 命令

当发送邮件的 SMTP 客户端发出 SMTP VRFY 命令时，vrfyallow、vrfydefault 和 vrfyhide 关键字将控制 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。除非已经指定通道选项 HIDE_VERIFY=1，否则 vrfydefault 将通知 MTA 提供具有详细信息的响应。vrfyhide 关键字通知 MTA 只发出模糊的响应。上述关键字允许控制每个通道的 VRFY 响应，与 HIDE_VERIFY 选项相反，而后者通常适用于通过同一 SMTP 服务器处理的所有外来 TCP/IP 通道。

12.4.2.5 EXPN 支持

关键字：expnallow、expndisable、expndefault

即使已使用 DISABLE_EXPAND SMTP 通道选项在 SMTP 服务器级别禁用 EXPN，expnallow 也允许 EXPN。expndisable 无条件禁用 EXPN。如果 SMTP 服务器设置为允许 EXPN（默认设置），expndefault 将允许 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。

12.4.2.6 DNS 域验证

关键字：mailfromdnsverify、nomailfromdnsverify

在外来 TCP/IP 通道中设置 mailfromdnsverify 会导致 MTA 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)。

因为 COM 和 ORG 顶层域中引入 DNS 通配符条目导致 mailfromdnsverify 作用减少，所以修改了 mailfromdnsverify 代码。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。

12.4.2.7 字符集标记和 8 位数据

关键字：charset7、charset8、charsetesc、sevenbit、eightbit、eightnegotiate、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 charset= 参数指定为 Content-type: 标题行的一部分。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转义符，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 位数据是绝对非法的）。如果未指定 charset8 值，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，此关键字还将添加该标题行。

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转义符，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。如果不存在此类限制，通道应标记为 eightbit。

SMTP 协议不允许使用 eightbit，“除非远程 SMTP 服务器明确声称支持允许 eightbit 的 SMTP 扩展”。事实上，某些传输（如扩展的 SMTP）可能会支持某种形式的协商，以确定是否可以传输八位字符。因此，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。

12.4.2.8 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。

12.4.3 TCP/IP 连接和 DNS 查找支持

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 327 页中的 “12.4.3.1 TCP/IP 端口号和接口地址”
- 第 327 页中的 “12.4.3.2 缓存通道连接信息”
- 第 328 页中的 “12.4.3.3 反向 DNS 查找”
- 第 328 页中的 “12.4.3.4 IDENT 查找”
- 第 329 页中的 “12.4.3.5 TCP/IP MX 记录支持”
- 第 330 页中的 “12.4.3.6 名称服务器查找”
- 第 330 页中的 “12.4.3.7 最后可用的主机”
- 第 330 页中的 “12.4.3.8 外来邮件的备用通道（切换通道）”
- 第 331 页中的 “12.4.3.9 基于用户或域设置的源通道切换”
- 第 331 页中的 “12.4.3.10 目标主机选择”

表 12–22 列出了本节说明的 TCP/IP 连接和 DNS 查找关键字。

表 12–22 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。

表 12–22 TCP/IP 连接和 DNS 查找关键字 （续）

通道关键字	说明
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	**指定如何对外来 SMTP 连接处理反向 DNS 查找。**
forwardcheckdelete	如果已执行反向 DNS 查找，则接下来对返回的名称执行正向查找，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 反向查找后不执行正向查找。
forwardchecktag	如果已执行反向 DNS 查找，则接下来对返回的名称执行正向查找，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 查找并执行 IP 到主机名的转换；在 Received: 标题中包含主机名和 IP 地址。
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 查找并执行 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 需要用于名称服务器且以空格分隔的 IP 地址列表。

表 12–22 TCP/IP 连接和 DNS 查找关键字 （续）

通道关键字	说明
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。
switchchannel	从服务器通道切换到与发件主机关联的通道。
userswitchchannel	基于用户或域设置的源通道切换。
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。

12.4.3.1 TCP/IP 端口号和接口地址

关键字：port、interfaceaddress

发送邮件时，基于 TCP/IP 的 SMTP 通道通常连接到端口 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 侦听用于接受 SMTP 连接的端口。

interfaceaddress 关键字控制 TCP/IP 通道绑定为出站连接源地址的地址；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，该关键字控制哪些地址将用作源 IP 地址。请注意，该关键字是分发程序选项 INTERFACE_ADDRESS 的补充，该选项控制 TCP/IP 通道侦听用于接受外来连接和邮件的接口地址。

12.4.3.2 缓存通道连接信息

关键字：cacheeverything、nocache、cachefailures、cachesuccesses

使用 SMTP 协议的通道保留一个包含以前连接尝试的历史记录的高速缓存。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，仅存在于出站 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。

默认情况下，`cacheeverything` 关键字将启用所有形式的高速缓存。`nocache` 关键字禁用所有高速缓存。

`cachefailures` 关键字启用连接失败的高速缓存，但不启用连接成功的高速缓存—这比 `cacheeverything` 对重试的限制更严。最后，`cachesuccesses` 只对成功连接进行高速缓存。对于 SMTP 通道，该关键字与 `nocache` 的效果相同。

12.4.3.3 反向 DNS 查找

关键字：`forwardchecknone`、`forwardchecktag`、`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 是否正向查找使用 DNS 反向查找发现的 IP 名，如果请求正向查找，则指定当 IP 名称的正向查找与原来的连接 IP 号不匹配时 MTA 要执行的操作。

`forwardchecknone` 关键字是默认设置，表示不进行正向查找。`forwardchecktag` 关键字通知 MTA 在每次反向查找后进行正向查找，如果使用正向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正向查找，如果该名称的正向查找与原来的连接 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 – 在很多站点中正向查找与原来的 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。

12.4.3.4 IDENT 查找

关键字：`identnone`、`identnonelimited`、`identtnonnumeric`、`identnonesymbolic`、`identtcp`、`identtcpnumeric`、`identtcpsymbolic`、`identtcplimited`

`IDENT` 关键字控制 MTA 使用 `IDENT` 协议处理连接和查找的方式。在 RFC 1413 中有对 `IDENT` 协议的说明。

`identtcp`、`identtcpsymbolic` 和 `identtcpnumeric` 关键字通知 MTA 使用 IDENT 协议执行连接和查找。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。

将 identtcp、indenttcplimited 或 identtcpsymbolic 与 identtcpnumeric 进行比较时，会出现另一个性能方面的因素。使用 identtcp、identtcplimited 或 identtcpsymbolic 调用的 DNS 反向查找（为了获取更加友好的主机名）会导致额外的系统开销。

identnone 关键字禁用 IDENT 查找，但会指定 IP 到主机名的转换，并在邮件的 Received: 标题中包含 IP 号和主机名。

identnonesymbolic 关键字禁用 IDENT 查找，但会进行 IP 到主机名的转换；在邮件的 Received: 标题中仅包含主机名。

identnonenumeric 关键字禁用此 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 相同。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。

12.4.3.5 TCP/IP MX 记录支持

关键字：mx、nomx、defaultmx、randommx、nonrandommx

某些 TCP/IP 网络支持使用 MX（邮件转发）记录，另外一些网络则不支持。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、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。

12.4.3.6 名称服务器查找

关键字：nameservers、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。

为了在 UNIX 中防止名称服务器查找，可以修改 nsswitch.conf 文件。在 NT 中，请修改 TCP/IP 配置。

12.4.3.7 最后可用的主机

关键字：lastresort

lastresort 关键字用于指定要连接的主机，即使所有其他连接尝试均失败。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
```

12.4.3.8 外来邮件的备用通道（切换通道）

关键字：switchchannel、allowswitchchannel、noswitchchannel。另请参见 第 332 页中的 “12.4.4 SMTP 验证、SASL 和 TLS” 中的 saslswitchchannel、第 334 页中的 “12.4.8 传输层安全性”中的 tlsswitchchannel 和第 331 页中的 “12.4.3.9 基于用户或域设置的源通道切换”中的 userswitchchannel

以下关键字控制对外来邮件的备用通道的选择：
switchchannel、allowswitchchannel、noswitchchannel。

MTA 在接受来自远程系统的外来连接时，必须选择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，则无法再使用该约定。发生这种情况时，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 switchchannel，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。

12.4.3.9 基于用户或域设置的源通道切换

关键字：userswitchchannel。另请参见第 330 页中的 “12.4.3.8 外来邮件的备用通道（切换通道）”中的 switchchannel

现在可以根据用户或域设置来切换源通道。涉及到三个新设置：

1. 一个新通道关键字 userswitchchannel。要发生用户通道切换，此关键字必须出现在初始源通道中。
2. 一个新的 MTA 选项 LDAP_DOMAIN_ATTR_SOURCE_CHANNEL，该选项指定一个域级别属性的名称，该属性中包含要切换到的通道的名称。
3. 一个新的 MTA 选项 LDAP_SOURCE_CHANNEL，该选项指定一个用户级别属性的名称，该属性中包含要切换到的通道的名称。

另外，要切换到的通道必须设置为允许通道切换。即，不能使用 noswitchchannel 关键字进行标记。基于通过重写 MAIL FROM 地址返回的信息完成切换。请注意，MAIL FROM 地址很容易伪造，所以使用此功能时要极其小心。

12.4.3.10 目标主机选择

关键字：daemon、single、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，出站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。

12.4.4 SMTP 验证、SASL 和 TLS

关键字：
maysaslserver、mustsaslserver、nosasl、nosaslserver、saslswitchchannel、nosaslswitchchannel

您可以控制 Messaging Server 是否支持使用 SASL（Simple Authentication and Security Layer，简单验证和安全层）对 SMTP 服务器进行验证。在 RFC 2222 中定义了 SASL，有关 SASL、SMTP 验证和安全性的更多信息，请参见第 23 章。

maysaslserver、mustsaslserver、nosasl、nosaslserver、switchchannel 和 saslswitchchannel 通道关键字用于 SMTP 协议期间配置 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 服务器允许客户端尝试使用 SASL 验证。指定 mustsaslserver 使 SMTP 服务器坚持让客户端使用 SASL 验证；除非远程客户端验证成功，否则 SMTP 服务器不接受邮件。

使用 saslswitchchannel 使外来连接在客户端成功使用 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。

12.4.5 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 关键字根据表 12–23 使用要求的位值。

表 12–23 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* 是信封的 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，而 *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 添加适当的 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 添加适当的 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。

12.4.6 支持 SMTP Chunking

关键字：chunkingclient、chunkingserver、nochunkingclient 、nochunkingserver

SMTP 客户端和服务器中都添加了对 SMTP chunking (RFC 3030) 的支持。 默认情况下已启用此支持。可以使用 4 个新的通道关键字控制是否允许 chunking。这些文件如下所示：

- chunkingclient - 启用客户端 chunking 支持（默认）。
- chunkingserver - 启用服务器 chunking 支持（默认）。
- nochunkingclient - 禁用客户端 chunking 支持。
- nochunkingserver - 禁用服务器 chunking 支持。

扩展了日志文件操作字段，可指示是否使用了 chunking 传输给定邮件。具体的说，如果使用了 chunking，将附加一个 C。请注意，必须使用 ESMTP，chunking 才能起作用，因此您通常会看到类似 EEC 或 DEC 的字段值。

12.4.7 指定 Microsoft Exchange 网关通道

关键字：msexchange 、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 网关及客户端通信的通道。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，不是基于更正后的较新 AUTH 规范）。例如，某些 Microsoft Exchange 客户端不能识别正确的 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。

12.4.8 传输层安全性

关键字：maytls、maytlsclient、maytlsserver、musttls、musttlsclient、musttlsserver、notls、notlsclient、notlsserver、tlsswitchchannel

maytls、maytlsclient、maytlsserver、musttls、musttlsclient、musttlsserver、notls、notlscl
和 tlsswitchchannel 通道关键字用于 SMTP 协议期间配置基于 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 客户端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，也不接受命令本身）。

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 客户端将尝试使用 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，必须具备以下条件：

- 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 客户端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，将不接受来自未能成功协商 TLS 使用的客户端的邮件。

tlsswitchchannel 关键字用于使外来连接在客户端的 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。

12.5 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：

有关邮件处理和传送的概念信息，请参见表 12–24。

第 335 页中的 “12.5 配置邮件处理和传送” 汇总了本节中说明的关键字。

表 12–24 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。

表 12–24 邮件处理和传送关键字 （续）

关键字	定义
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**
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	**指定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	识别 Deferred-delivery: 标题行并使其生效。
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	**定义基于邮件大小的邮件优先级。**
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	**指定用于处理有各种作业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 客户端触发新线程的邮件的数目。
多个地址扩展	**定义对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。

表 12–24 邮件处理和传送关键字 （续）

关键字	定义
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。
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。

12.5.1 设置通道方向性

关键字：master、slave、bidirectional

这些关键字用于指定通道是由主程序 (master) 或从程序 (slave) 还是这两者 (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。

12.5.2 实现延迟传送日期

关键字：deferred、nodeferred、immnonurgent

deferred 通道关键字实现 Deferred-delivery: 标题行的识别和生效。将来传送日期被 deferred 的邮件将保留在通道队列中，直到过期并返回，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，请参见 RFC 1327。

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作其磁盘配额的扩展。

提交紧急、正常和不紧急邮件后，关键字 immnonurgent 将立即开始传送。

12.5.3 为传送失败的邮件指定重试频率

关键字：backoff、nonurgentbackoff、normalbackoff、urgentbackoff、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：

```
urgent: 30, 60, 60, 120, 120, 120, 240
normal: 60, 120, 120, 240, 240, 240, 480
nonurgent: 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 243 页中的 “10.10.4.3 设置通知邮件传送间隔” 。）

backoff 关键字可以使您能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给发件人。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给发件人。

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给发件人。

12.5.4 用于通道执行作业的处理池

关键字：pool

通过让各种通道在同一池中运行，可以将各种通道配置为共享资源。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 341 页中的 “12.5.7 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应置于该池中。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更多信息，请参阅第 223 页中的 “10.4.8 作业控制器文件” 、第 223 页中的 “10.4.8 作业控制器文件” 以及第 339 页中的 “12.5.5 服务作业限制” 。

12.5.5 服务作业限制

关键字：maxjobs、filesperjob

每次将邮件加入通道队列时，作业控制器将确保一个作业处于运行状态，以便传送邮件。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更多信息，请参阅第 223 页中的 “10.4.8 作业控制器文件” 、第 339 页中的 “12.5.4 用于通道执行作业的处理池” 和第 174 页中的 “8.7 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）
- 为一组通道启动的最大进程数（作业控制器配置文件中的相关池部分的 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的最大线程数（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 341 页中的 “12.5.8 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。

12.5.6 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的电子邮件地址。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 客户端对收件人限制、事务限制或二者的响应相当差。需要对这些客户端设置例外。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。

12.5.7 基于大小的邮件优先级

关键字：urgentblocklimit、normalblocklimit、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。

12.5.8 SMTP 通道线程

关键字：threaddepth

多线程 SMTP 客户端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 客户端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），也对这些邮件使用附加线程。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（出站）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` 对于在守护进程路由器 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。

12.5.9 多个地址扩展

关键字：`expandlimit`、`expandchannel`、`holdlimit`

大多数通道支持在每个入站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。

例如，通过结合使用普通的 `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。

12.5.10 启用服务转换

关键字：service 、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。

12.6 配置地址处理

本节说明了涉及地址处理的关键字。其中包含以下各节：

12.6.1 地址类型和约定

关键字：822、733、uucp、header_822、header_733、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。

12.6.1.1 822 (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。

12.6.1.2 733 (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。

12.6.1.3 uucp (bangstyle)

bang 样式的信封地址。此通道在信封中使用符合 RFC 976 bang 样式地址约定的地址（例如，这是 UUCP 通道）。也可以使用关键字 `bangstyle`，它是 uucp 的同义词。

12.6.1.4 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。

12.6.1.5 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。

12.6.1.6 header_uucp

UUCP 或 bang 样式标题地址。不建议使用此关键字。使用此关键字违反 RFC 976。

12.6.2 解释使用 ! 和 % 的地址

关键字：`bangoverpercent`、`nobangoverpercent`、`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，格式为 `A!B%C` 的地址可以解释为：

- `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 指出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 – 此关键字不影响对格式 A!B@C 地址的处理。这些地址将始终处理为 (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。

12.6.3 在地址中添加路由信息

关键字：exproute、noexproute、improute、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。

当通道地址传递到远程系统时，exproute 关键字（"explicit routing" 的缩写）通知 MTA 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 选项可用于将 exproute 操作限制为反向指向地址。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 选项可用于将 improute 操作限制为反向指向地址。

exproute 和 improute 关键字应谨慎使用。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。显式和隐式路由的控制却是以每个通道为基础，插入的路由地址始终是本地系统。

12.6.4 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（使用字符 !、% 或 @）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。

12.6.5 邮件出队后的地址重写

关键字：connectalias、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。

12.6.6 指定修正不完整地址时使用的主机名

关键字：remotehost、noremotehost、defaulthost、nodefaulthost

MTA 常收到来自配置错误或不兼容的邮件程序和 SMTP 客户端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 主机名和客户端 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 客户端时，使用远程主机的域名比较合适。当处理轻量远程邮件客户端（例如使用 SMTP 收发邮件的 POP 或 IMAP 客户端）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端（例如 POP 或 IMAP 客户端），则客户端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。它必须后接用于完成进入相应通道的地址（信封 From: 和标题中）的域名。（如果提交通道，defaulthost 关键字的第一个参数还将影响缺少域名的信封 To: 地址。）可以指定用于完成信封 To: 地址的第二个可选域名（其中至少有一个句点）。nodefaulthost 是默认设置。

如前面的第 330 页中的 “12.4.3.8 外来邮件的备用通道（切换通道）”一节所述，switchchannel 关键字可用于将外来 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端进行分组，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端（即使多个不兼容的客户端正在使用中），这比尝试解决 MTA 主机中网络范围的问题简单。

12.6.7 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，该值指定用于处理此类邮件的方法；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 12–25 missingrecipientpolicy 的值

值	操作
0	使用每个 RFC 2822 建议的当前最佳实践。此值当前等效于值 1。
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: 收件人置于单一 Bcc: 标题行。
4	生成一个组构建（例如 ";"）To: 标题行，即 "To: Recipients not specified: ;"
5	生成一个空 Bcc: 标题行。
6	拒绝邮件。

请注意，MISSING_RECIPIENT_POLICY 选项可用于为此行为设置 MTA 系统默认值。初始 Messaging Server 配置将 MISSING_RECIPIENT_POLICY 设置为 1。

12.6.8 删除非法的空收件人标题

关键字：dropblank、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—这种标题不能包含空值。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，此关键字将使 MTA 删除外来邮件中所有这种非法空标题。

12.6.9 启用特定于通道的反向数据库使用

关键字：reverse 、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）检查或修改（如果可能）在此通道排队的邮件的地址。noreverse 使在此通道排队的邮件地址免受地址反向处理。reverse 关键字是默认设置。请参阅第 230 页中的 “10.9 将地址由内部格式转换为公用格式”。

12.6.10 启用限制的邮箱编码

关键字：restricted、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（或邮箱规范）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。）

12.6.11 生成 Return-path 标题行

关键字：addreturnpath、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此添加操作效率更高。addreturnpath 关键字使 MTA 在邮件加入该通道队列时添加 Return-path: 标题。

12.6.12 从信封 To 和 From 地址构建 Received 标题行

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: 地址包含在其构建的 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，如果 MTA 由于某些种类的邮件列表扩展等原因而更改了信封 From: 地址，则在为外来邮件构建 Received: 标题行时包含原来的信封 From: 地址。receivedfrom 是默认设置。noreceivedfor 关键字指示 MTA 构建 Received: 标题行，但不包含原来的信封 From: 地址。

12.6.13 处理地址标题行中的注释

关键字：commentinc、
commentmap、commentomit、commentstrip、commenttotal、sourcecommentinc、sourcecommentr

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。

可以使用关键字 commentinc、commentmap、commentomit、commentstrip 和 commenttotal 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）删除所有注释。

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，该关键字没有用处或建议不要使用。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，可以使用关键字 sourcecommentinc、sourcecommentmap、sourcecommentomit、sourcecommentstrip 和 sourcecommenttotal 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）删除所有注释。关键字 commenttotal 通知 MTA 从除 Received: 标题之外的所有标题中删除所有注释；因此，该关键字通常没有用处或建议不要使用。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。

12.6.14 处理地址标题行中的个人名称

关键字：personalinc、
personalmap、personalomit、personalstrip、sourcepersonalinc、sourcepersonalmap、sourcepers

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。

可以使用关键字 personalinc、personalmap、personalomit 和 personalstrip 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，可以使用关键字 sourcepersonalinc、sourcepersonalmap、sourcepersonalomit 或 sourcepersonalstrip 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。

12.6.15 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，以便在别名文件和别名数据库中也能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。

12.6.16 子地址处理

关键字：subaddressexact、subaddressrelaxed、subaddresswild

作为关于子地址概念的背景，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，无格式名称将转换为新名称，名称 + 子地址将转换为新名称 + 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 关键字可能很有用。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）。

12.6.17 启用特定于通道的重写规则检查

关键字：rules、norules

rules 关键字通知 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。

12.6.18 删除源路由

关键字：dequeue_removeroute

dequeue_removeroute 关键字在邮件出队列时从信封 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。

12.6.19 必须从别名指定地址

关键字：viaaliasoptional、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。

例如，viaaliasrequired 关键字可以用于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。

默认设置是 viaaliasoptional，表示不要求与通道匹配的最终收件人地址由别名生成。

12.6.20 收件人地址处理

关键字：acceptalladdresses、acceptvalidaddresses

acceptvalidaddresses 是默认值，对应于 MTA 的标准行为：SMTP 对话期间任何收件人错误都将被立即报告。如果对通道指定了关键字 acceptalladdresses，则 SMTP 对话期间将接受所有收件人地址。所有无效的地址随后将使用 DSN 发送。

12.7 配置标题处理

本节说明了涉及标题和信封信息的关键字。其中包含以下各节：

- 第 356 页中的 “12.7.9 敏感度检查”
- 第 356 页中的 “12.7.10 设置标题中的默认语言”
- 第 356 页中的 “12.7.11 控制 Message-hash: 标题”

12.7.1 重写嵌入式标题

关键字：noinner、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。

可以使用关键字 noinner 和 inner 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 对邮件进行解析，并重写内部标题。上述关键字可以应用到所有通道中。

12.7.2 删除选定的邮件标题行

关键字：
headertrim、noheadertrim、headerread、noheaderread、innertrimnoinnertrim

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 6.3 Administration Reference》中的“Header Option Files”中介绍了标题选项文件的格式。

headertrim 关键字指示 MTA **在处理原来的邮件标题之后**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 **在处理原来的邮件标题之前**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，另一方面，headertrim 标题剪裁是在处理邮件之后应用的，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 是标题选项文件与其关联的通道的名称。类似地，`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*`/config/` 中。

12.7.3 生成/删除 X-Envelope-to 标题行

关键字：`x_env_to`、`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` 标题行的生成或取消。在用 `single` 关键字标记的通道中，`x_env_to` 关键字启用上述标题的生成，而 `nox_env_to` 则从加入队列的邮件中删除上述标题。默认设置是 `nox_env_to`。

尽管这样做没有太大意义，但现在使用 `x_env_to` 关键字时不需要同时对通道设置 `single`。

12.7.4 将日期转换为两位数或四位数

关键字：`datefour`、`datetwo`

原来的 RFC 822 规范要求邮件标题中日期字段必须使用两位数年份。后来 RFC 1123 将其更改为四位数。但是某些旧邮件系统无法接受四位数日期。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。值小于 50 的两位数日期会加 2000，值大于 50 的两位数日期则加 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。

12.7.5 在日期中指定星期几

关键字：dayofweek、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。

12.7.6 自动分割长标题行

关键字：maxheaderaddrs、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。

12.7.7 标题对齐和折叠

关键字：headerlabelalign、headerlinelength

headerlabelalign 关键字控制加入此通道队列的邮件标题的对齐点；它使用整数值参数。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 是 0，表示不对齐标题。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。

12.7.8 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。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。

12.7.9 敏感度检查

关键字：sensitivitynormal、sensitivitypersonal、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。默认设置是 sensitivitycompanyconfidential；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：

邮件对所使用的一个或多个路径过于敏感

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。

12.7.10 设置标题中的默认语言

关键字：**语言**

标题中经过编码的内容可以显示为特定语言。language 关键字指定默认语言。

12.7.11 控制 Message-hash: 标题

关键字：generatemessagehash、keepmessagehash、deletemessagehash

这些关键字控制邮件中的 Message-hash: 标题。在目标通道中指定 Generatemessage 将导致 Message-hash: 标题字段被插入到邮件中。Keepmessagehash 将保留所有现有 Message-hash: 字段。Deletemessagehash 将删除所有现有 Message-hash: 字段。Deletemessagehash 是默认设置。

Message-Hash: 字段中放置的值是一个邮件的散列。几个新的 MTA 选项控制散列生成的方式：

MESSAGE_HASH_ALGORITHM - 散列算法。可以是以下的任意一个：md2、md4、 md5（默认设置）、sha1、md128（用于 RIPE-MD128）或 md160（用于 RIPE-MD160）。

MESSAGE_HASH_FIELDS - 以逗号分隔的从标题到散列（按顺序）的字段列表。可以指定任何已知标题字段。如果未指定此选项，则将其默认设置为“message-id、from、to、cc、bcc、resent-message-id、resent-from、resent-to、resent-cc、resent-bcc、subject、content-id、content-type、content-description”

12.8 附件和 MIME 处理

本节说明了涉及附件和 MIME 处理的关键字。其中包含以下各节：

12.8.1 忽略 Encoding 标题行

关键字：ignoreencoding、interpretencoding

MTA 可以用 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），此关键字是默认设置。

12.8.2 Message/Partial 邮件的自动片段整理

关键字：defragment、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。

12.8.2.1 片段整理通道

如果 defragment 关键字在目标通道中，则邮件被路由到片段整理通道。即，当 defragment 关键字出现在目标通道中时（MTA 通常将邮件置于此通道中排队），MTA 在邮件结构“内部查看”（MIME 解析），如果 MTA 看到邮件结构是一个 MIME 邮件片段，那么 MTA 自动将邮件路由到片段整理通道，而不是直接路由到（通常的）目标通道。

片段整理数据库包含有关进入 MTA 的邮件片段的信息，其中包括表明接受每个邮件片段的主机的信息。收到初始片段并在片段整理数据库中说明后，任何使用相同片段整理数据库的其他系统所收到的邮件的任何其他部分都将被路由到收到最初部分的主机。例如：

1. 由于目标/出站通道上有 defragment 关键字，因此，message/partial; id=123; part=x 会在到达主机 1 后路由到主机 1 上的片段整理通道。
2. 主机 1 上的片段整理通道检查片段整理数据库，以查看此邮件的其他部分是否已经到达。如果没有到，片段整理通道（主机 1 上的）将此部分输入片断整理数据库，并标明此部分在主机 1 上。
3. 由于目标/出站通道上有 defragment 关键字，因此，message/partial; id=123; part=y 会在到达主机 2 后路由到主机 2 上的片段整理通道。
4. 主机 2 上的片段整理通道将检查片段整理数据库，查看此邮件的第 x 部分是否已存在并存储在主机 1 上。片段整理通道可将此邮件片段重定向到主机 1（源会路由包含 @host1 的地址）。
5. message/partial’ id=123; part=y 到达主机 1，被路由到片段整理通道，片段整理通道运行并将它输入数据库，等等。

片段邮件的所有剩余部分都被重定向到收到邮件第一个部分（第一个收到的，不一定是 part=1）的主机。它们通过该主机的片段整理通道重新组合起来，最终成为组合好的、片段整理过的邮件（如果由于通知过多导致片段整理工作超时，各个片段将被原样发送出去）被发送到真正的目标通道。您可以获取邮件片段整理的部分负载平衡，具体取决于哪个主机恰好收到每个邮件的“第一个”部分。

12.8.2.2 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。将关键字 notices 的值设置为希望保留邮件的时间的两倍，以进行可能的片段整理。例如，notices 的值为 4 可以使邮件片段保留两天：

```
defragment notices 4
DEFRAGMENT-DAEMON
```

12.8.2.3 将基于 NFS 的文件系统用于片段整理和休假缓存

基于 NFS 的文件系统经常用于片段整理和休假缓存。通过让多个 MTA 系统共享同一片段整理缓存，一个应用程序可以在多个 MTA 系统之间共享片段整理数据库。要实现这一点，可以连接每个系统上的 `msg-svr-base/config/` *defragment_cache* 和希望作为共享片段整理数据库（在共享的 NFS 磁盘上）的文件。

在任何情况下，支持正确的 NFS 文件语义（尤其是那些具有锁请求的，如 Solaris NFS）的 NFS 服务器可用于休假和片段整理缓存。如果使用 NFS，请使用软加载 (soft mount) 选项。（硬加载 (hard mount) 是默认设置。）设置一个相对较短的超时值也是个不错的主意，超时值由 `mount timeo` 选项控制（请参见 `mount_nfs(1M)` 手册页）。

在 NFS 硬加载且 NFS 出现故障的情况下，将会看到各种系统上的片段整理通道挂起。在软加载的情况下，片段整理通道不会挂起，但因为它们无法打开片段整理缓存，所以不能与其他主机上的片段整理通道协作。在某个邮件的所有片段恰巧都先到达了同一主机的情况下（不太可能发生），该主机的片段整理通道应该能够重新组合邮件并将正确组合的邮件发送出去。更可能的情况是，片段在不同的主机上且不会重新组合，并且在片段整理通道的保留时间过期后，它们将被作为分离的片段发送出去。

12.8.3 大型邮件的自动分段

关键字：`maxblocks`、`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 以各个通道为基础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。

关键字 `maxblocks` 和 `maxlines` 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 和 1 之间的一个实数。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 且 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。

12.8.4 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 关键字提供了以各个通道为基础的机制，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 中可用的各种编码总是将行长度减少到少于 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减少到少于 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”自动换行的信息，请参见表 13–7 中的 "Record, text"。

12.8.5 解释 Multiparts 和 Message/RFC822 部分的内容传输编码字段

关键字：interpretmultipartencoding、ignoremultipartencoding、interpretmessageencoding、ignoremessageencoding

MIME 规范禁止在 multipart 或 message/rfc822 部分使用除 7 位、8 位和二进制以外的内容传输编码。一直以来就有些代理违反该规范而对 multiparts 和 message/rfc822 对象进行编码。因此，MTA 提供了接受和删除此类编码的代码。但是，最近又出现了另一种违反标准的情况，即存在一种具有 quoted-printable 或 base63 值的内容传输编码字段，但实际上该部分并未进行编码。如果 MTA 尝试解码此类邮件，则正如您所料，得到的结果通常是一个空白邮件。

涉及此问题的邮件已越来越多，因此添加了两对新的通道关键字以处理该问题，从而可以启用或禁用对 multiparts 和 message/rfc822 部分的内容传输编码的解释。第一对关键字是 `interpretmultipartencoding` 和 `ignoremultipartencoding`，第二对关键字是 `interpretmessageencoding` 和 `ignoremessageencoding`。默认值是 `interpretmultipartencoding` 和 `interpretmessageencoding`。

12.9 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。其中包含以下各节：

12.9.1 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。

12.9.2 指定绝对邮件大小限制

关键字：`blocklimit`、`noblocklimit`、`linelimit`、`nolinelimit`、`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（例如为了避免对服务拒绝的攻击）。

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` 适用于目标通道，而 `sourceblocklimit` 适用于源通道。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端了解这些限制。这就简化了某些协议中的邮件拒绝进程。

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。

12.9.3 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、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。此功能可以通过以下的一组通道关键字实现，这些关键字可以置于任意的目标通道中：alternatechannel、alternateblocklimit、alternatelinelimit 和 alternaterecipientlimit。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 ...other keywords... alternatechannel tcp_big alternateblocklimit 5
tcp-daemon


tcp_big smtp ...rest of keywords...
tcp-big-daemon
```

以下示例说明了如何使用 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，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，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，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《Sun Java System Messaging Server 6.3 Administration Reference》中的 `STATUS_DATA_RECV_PER_ADDR_TIME` 和 `STATUS_DATA_RECV_PER_BLOCK_TIME` 通道选项。

- 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` 与通道关键字 `maxblocks` 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，应该将所需的 `maxblocks` 大小置于常规的出站 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，则可以在出站 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仔细的检查，以防它是垃圾邮件。您可能希望以外发通道为基础进行不同的过滤（请参见第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”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这些大型邮件。

  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。

12.9.4 处理对超过配额用户的邮件传送

关键字：`holdexquota`、`noexquota`

关键字 noexquota 和 holdexquota 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 通知 MTA 将发送给超过配额用户的邮件返回邮件的发件人。holdexquota 通知 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。

12.9.5 处理包含超过 1000 个字符的行的 SMTP 邮件

关键字：rejectsmtplonglines、wrapsmtplonglines、truncatesmtplonglines

rejectsmtplonglines 添加拒收邮件选项，拒绝包含字符数超过 1000 个（包括 CRLF）的行（SMTP 中允许这种行）的邮件。此区域中的其他选项包括 wrapsmtplonglines（将过长的行自动换行）和默认的 truncatesmtplonglines（将过长的行截断）。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。

12.9.6 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 content-type 参数和 content-disposition 参数的截断点。默认值为 1024。nameparameterlengthlimit 控制 name content-type 参数和 filename content-disposition 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。

12.9.7 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，并将属性添加到发件人的用户条目或域条目。

12.9.8 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的限制。默认值为没有限制。

12.10 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。其中包含以下各节：

12.10.1 控制邮件中多个地址的处理方式

关键字：`multiple`、`addrsperfile`、`single`、`single_sys`

MTA 允许每个排队的邮件中出现多个目标地址。某些通道程序也许只能处理带有一个收件人的邮件、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。不建议对 tcp_* 通道使用 `single` 关键字，因为它会更改作业控制器管理通信的方式，并且对于普通的 SMTP 方案不适用。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文件关联的最大收件人数量，从而限制了单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。）

12.10.2 分布通道邮件队列到多个子目录

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 *msg_svr_base*/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 通道关键字提供了此功能：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
```

12.10.3 设置会话限制

关键字：
disconnectbadcommandlimit、disconnectrecipientlimit、disconnectrejectlimit、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 服务器从客户端断开连接的功能。

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。发出 MAIL FROM 或 RSET 命令后，将检查除 disconnectbadcommandlimit 外的所有这些限制。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。

12.11 配置记录和调试

本节说明了记录和调试关键字。

12.11.1 记录关键字

关键字：logging、nologging、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 以每个通道为基础控制对邮件的日志记录。默认情况下，初始配置打开所有通道的记录功能。通过在通道定义中替换 nologging 关键字，可以禁用特定通道的日志记录功能。

logheader 以每个通道为基础覆盖 MTA 选项 LOG_HEADER。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 6.3 Administration Reference》 中的“Option File”。

有关日志记录的详细信息，请参见第 25 章。

12.11.2 调试关键字

关键字：master_debug、slave_debug、nomaster_debug、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。这两个关键字是 master_debug（启用主程序中的调试输出）和 slave_debug（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，相当于启用 nomaster_debug 和 noslave_debug。

激活后，调试输出将终止于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* 是通道的名称。从程序的日志文件名称格式通常为 *x*_slave.log。

在 UNIX 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（如果用户具有对该目录的写权限，否则调试输出进入 stdout）。

12.11.3 设置 Loopcheck

关键字：loopcheck、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 客户端将公布的字符串与其 MTA 值进行比较，并立即返回信息，说明客户端实际上是否在与 SMTP 服务器通信。

12.12 其他关键字

本节说明了其他关键字。其中包含以下各节：

12.12.1 进程通道覆盖

关键字：`notificationchannel`、`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 (Delivery Status Notification, 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 (Message Disposition Notification, 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。

12.12.2 通道操作类型

关键字：`submit`

Messaging Server 支持 RFC 2476 的邮件提交协议。`submit` 关键字可以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。

12.12.3 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。

12.12.4 指定邮箱过滤器文件位置

关键字：filter、nofilter、channelfilter、nochannelfilter、destinationfilter、nodestinationfilter、sourcefilter、nosourcefilter、fileinto、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。应使用一个必需的 URL 参数说明过滤器文件的位置。nofilter 是默认设置，表示没有为通道启用用户邮箱过滤器。

关键字 sourcefilter 和 destinationfilter 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。

已作废的关键字 channelfilter 和 nochannelfilter 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（不是数字零）。

12.12.5 垃圾邮件过滤器关键字

关键字：destinationspamfilter*X*optin、sourcespamfilter*X* optin、disabledestinationspamfilter*X*、disablesourcespamfilter *X*

destinationspamfilter*X*optin 指定发送到此通道的所有邮件均通过过滤软件 X 运行，即使用户或域并没有使用 LDAP_OPTIN*X* LDAP 属性指定那些服务。（过滤软件 X 由 option.dat 中的 spamfilter*X*_library 定义。）关键字后面跟 optin 参数，可用的参数取决于过滤程序。例如，Brightmail 的参数通常为 spam、virus 或 spam,virus。SpamAssassin 的参数为 spam。

sourcespamfilter*X*optin 指定源自此通道的所有邮件均通过过滤软件 X 运行。（过滤软件 X 由 option.dat 中的 spamfilter*X*_library 定义。）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，则应将此关键字放置在 switched-to 通道上。

sourcespamfilter*X* 和 destinationspamfilter*X* 与 sourcespamfilter*X*optin 和 destinationspamfilter*X*optin 执行的操作相同，只是前者不接受 optin 参数。它们用于不传递参数，而只是进行启用或禁用的过滤软件。

disabledestinationspamfilter*X* 对发送到此通道的邮件禁用垃圾邮件过滤器 X。如果某个邮件来自启用垃圾过滤器 X 的通道（例如：destinationspamfilter*X*optin），或者通过使用用户或域 LDAP 条目中的 optin 属性启用了过滤器，则此关键字将禁用它。

disablesourcespamfilter*X* 对来自此通道的邮件禁用垃圾过滤器 X。如果某个邮件被发送到启用垃圾邮件过滤器 X 的通道（例如：destinationspamfilter*X*optin），或者通过使用用户或域 LDAP 条目中的 optin 属性启用了过滤器，则此关键字将禁用它。

有关如何使用这些关键字的完整的详细信息，请参见第 413 页中的 “指定通道级别的过滤”。

12.12.6 地址验证之后扩展之前的路由

关键字：aliasdetourhost、aliasoptindetourhost

aliasdetourhost 和 aliasoptindetourhost 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。（请注意，当我们提到 aliasdetourhost 时，我们也在描述 aliasoptindetourhost，它与 aliasdetourhost 功能相似，不同之处在于，绕行仅在用户已通过以下 LDAP 属性选择加入时发生。

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。

aliasdetourhost 的参数是主机或域名，或者是主机/域定义。（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。

不是将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），而是使用 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，指向过滤系统。将 enqueue_removeroute 也添加到此通道。在 imta.cnf 中，tcp_scanner 通道与以下通道类似：

   ```
   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. 在要扫描的所有入站源 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。以下介绍 tcp_local 和 tcp_submit 的一个示例。

   ```
   ! 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，并且将因为这些源通道均有 aliasdetourhost 而再次扫描邮件。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. 在要扫描的所有入站源 tcp 通道（可能包括 tcp_local、tcp_submit、tcp_intranet 等）上，将 aliasDetourHost tcp_scanner-daemon 添加到 tcp_local。以下介绍 tcp_local 和 tcp_submit 的一个示例。

```
! tcp_local
tcp_local smtp mx single_sys remotehost inner switchchannel
identnonenumeric subdirs 20 maxjobs 7 pool SMTP_POOL maytlsserver
maysaslserversaslswitchchannel 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 通道重新路由出站邮件。

```
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 以免再次对其扫描。

```
!
[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
```

12.12.6.1 aliasoptindetourhost

通过以下功能集，基于每个用户的 aliasdetourhost 现在成为可能：

- aliasoptindetourhost 通道关键字。此关键字在功能上与 aliasdetourhost 类似，不同之处在于，绕行仅在用户已通过以下属性选择加入时发生。关键字的值是以逗号分隔的潜在绕行主机列表。
- MTA 选项 LDAP_DETOURHOST_OPTIN 指定用于使用户选择加入绕行的属性的名称（当然假定源通道设置了 aliasoptindetourhost）。如果此属性值包含句点，则会将它们与潜在绕行主机列表比较，列表上的第一个匹配的主机会被选为绕行主机。如果该值不包含句点，将无条件使用第一个绕行主机。
- MTA 选项 ALIASDETOURHOST_NULL_OPTIN，与 SPAMFILTERx_NULL_OPTIN 类似（请参见表 14–1）。它指定一个特殊值，如果在 LDAP_DETOURHOST_OPTIN 属性中使用，将等同于省略该属性。默认值是 ""，表示忽略空属性值。

12.12.7 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请求字段值列表，在此通道提交的邮件中将阻塞这些请求字段值。值的此列表将显示在 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请求字段值列表，在此通道排队的邮件中将不接受这些请求字段值。

12.12.8 对错误的 RCPT TO 地址设置限制

关键字：deferralrejectlimit

对单次会话中允许的错误 RCPT TO: 地址设置数量限制。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，但以每个通道为基础。

12.12.9 设置 Monitoring Framework 的通道显示

关键字：caption 和 description

这些关键字采用引用字符串作为参数，用于监视框架控制台中的通道显示。如果不存在标题或描述，Monitoring Framework 代理将通过通道名称创建一个。

◆ ◆ ◆ 第 13 章

13 使用预定义的通道

首次安装 Messaging Server 时，已经定义了多个通道（请参见表 13–1）。本章介绍如何使用 MAT 中预定义的通道定义。

如果您尚未阅读第 10 章，请先阅读该章，然后再阅读本章。有关在 `imta.cnf` 文件中配置重写规则的信息，请参见第 11 章。

本章包含以下各节：

第 277 页中的 “12.1 配置通道默认值”中介绍了 `defaults` 通道。

13.1 预定义的通道

下表列出了某些预定义的通道。

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 277 页中的 “12.1 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`	执行最后的向本地存储传送邮件的操作。

表 13–1 预定义的通道 （续）

通道	定义
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 工具才能访问 /var/mail 中存储的邮件。）
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。
reprocessprocess	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时通常不可见；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 的邮件按正文部分执行转换。
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 主机的入站邮件。根据是否使用智能主机/防火墙配置，将出站邮件直接发送到远程 SMTP 主机，或者将出站邮件发送到智能主机/防火墙系统。有时 tcp_local 通过代理和防火墙从远程 SMTP 主机获取邮件。tcp_local 有时也用于内部转发活动。 tcp_intranet 在内联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，以避免遭受中继阻止限制。 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服务的特殊通道。

13.2 使用 Pipe 通道将邮件传送给程序

用户可能希望外来邮件传递给程序而不是他们的邮箱。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，必须首先将程序注册为能够通过 pipe 通道调用。可以使用 imsimta program 实用程序完成此操作。该实用程序为每个命令（注册为能够通过 pipe 通道调用）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，该程序以用户身份执行 procmail 程序（使用参数 -d *username*）：

```
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 实用程序的更多信息，请参见 《Sun Java System Messaging Server 6.3 Administration Reference》 。

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列、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，该变量参数代表用户名；对于由邮寄主管 ("inetmail") 执行的程序，该变量参数代表用户名和域。例如，以下命令行使用程序 procmail 传送收件人的邮件：

```
/usr/lib/procmail -d %s
```

13.3 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，具体情况取决于选项的要求。

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 的较新邮件工具兼容，但与其他 UNIX 邮件工具存在潜在的不兼容性。
FORWARD_FORMAT（字符串）	请指定用户 .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 (integer) SLEEP_TIME (integer)	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 选项用于指定通道程序在放弃之前尝试打开邮件文件的次数。REPEAT_COUNT 的默认值为 30（尝试 30 次）。 SLEEP_TIME 选项用于指定通道程序在两次尝试之间等待的秒数。SLEEP_TIME 的默认值为 2（两次重试之间等待 2 秒）。
SHELL_TIMEOUT（整数）	用于指定通道等待用户在 .forward 中的 shell 命令完成的时间长度（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 *user* 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

13.4 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。

保留邮件时，这些邮件将被定位到 *msg-svr-base*/queue/hold 目录中的 hold 通道，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 directory 目录中的 hold 通道队列。这可以防止作业控制器找到这些邮件，从而“保留”这些邮件。使用 imsimta qm dir -held 命令查看 HELD 文件的列表。可以使用 imsimta qm release 命令选择并释放这些邮件。释放邮件会将其名称更改为 *ZZxxx*.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 命令的更多信息，请参见 《Sun Java System Messaging Server 6.3 Administration Reference》 中的“imsimta qm”。

13.5 转换通道

conversion 通道使您可以对通过 MAT 的指定邮件执行任意的正文部分逐一处理。（请注意，正文部分不同于邮件，邮件可以包含多个正文部分，例如附件中的正文部分。此外，正文部分是由 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正文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 170 页中的 “8.5 通道”）。有关使用 conversion 通道进行病毒扫描的附加信息，请参见 Messaging Server 文档 Web 站点 http://docs.sun.com/db/coll/S1_MsgTechNotes (http://docs.sun.com/db/coll/S1_MsgTechNotes) 底部的当前版本 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) 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。

本节包含以下几个部分：

13.5.1 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，请参见 RFC 1806、2045 至 2049 和 2183 (http://www.faqs.org/rfcs/)。为方便起见，本文对 MIME 做了简要概述。

13.5.1.1 邮件结构

简单邮件由标题和正文组成。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）。正文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，邮件可以包含多个正文部分，甚至正文部分中还可以嵌套正文部分。这样的邮件称作多部分邮件，如前文中所述，转换通道对邮件按正文部分进行处理。

13.5.1.2 MIME 标题

MIME 规范为正文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`。转换通道通常使用 `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` 标题说明正文部分的内容。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 说明正文部分内容的类型。类型包括 `Text`、`Multipart`、`Message`、`Application`、`Image`、 `Audio`、`Video` 等。

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。
http://www.iana.org/assignments/media-types 中有一份列表。

parameter 特定于各 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 标题提供正文部分的显示信息。通常将其添加到附件中，指定是显示附件的正文部分 (inline) 还是显示为要复制的文件名 (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（显示正文部分）或 attachment（显示为要保存的文件）。Attachment 通常具有参数 filename，该参数有一个值用于指定被保存文件的建议名称。

有关 Content-disposition 标题的详细信息，请参见 RFC2183。

13.5.2 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* 是邮件的源通道，*destination-channel* 是邮件的目标通道，则执行 CONVERT 之后的操作（Yes 表示 MTA 将邮件从其 *destination-channel* 转移到转换通道；如果未找到匹配项，邮件将被排入常规目标通道中）。

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。

在以下示例中，将所有非内部邮件（来自或发送到 Internet 的邮件）都路由到转换通道。

```
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，因此任何其他邮件都将不经过转换通道。

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，使用多个出站到 Internet 的 tcp_* 通道的站点，或使用多个从 Internet 入站的 tcp_* 通道的站点）可能不够用。

13.5.3 控制转换处理

本部分介绍如何控制转换处理。它包含以下几个部分：

当邮件被发送到转换通道时，将按正文部分对其进行处理。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（默认设置：*msg-svr-base*`/conversions`）。`conversions` 文件由以行分隔的条目组成，这些条目控制要处理的正文部分的类型和处理方式。

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。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 `conversion` 文件条目的简单示例：

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'"
```

子句 `out-chan=ims-ms; in-type=application; in-subtype=wordperfect5.1` 限定正文部分。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。然后按顺序从头到尾扫描 `conversion` 文件中的条目；检查存在的所有 `in-*` 参数和 `OUT-CHAN` 参数。如果上述所有参数都与被处理的正文部分的相应信息匹配，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。对所有正文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` 指定仅转换要发送到 `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"
```

在示例 13–1 中的三个 conversion 文件限定参数之后，接下来的两个参数（out-type=application 和 out-subtype=msword）指定要附加到“已处理”正文部分的替换 MIME 标题行。out-type=application 和 out-subtype=msword 指定外发邮件的 MIME Content-type/subtype 必须为 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，因为默认情况下转换通道使用外发正文部分的原始 MIME 标签。可以使用其他输出参数指定外发正文部分的其他 MIME 标签。

out-mode=block（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。

示例 13–1 中的最后一个参数指定将对正文部分执行的操作。

```
command="/usr/bin/convert -in=wordp -out=msword 'INPUT_FILE' 'OUTPUT_FILE'"
```

command= 参数指定将要针对正文部分执行的程序。/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，用于指定输入文本和输出文本的格式；INPUT_FILE 和 OUTPUT_FILE 是转换通道的环境参数（请参见第 384 页中的 “13.5.3.2 使用转换通道环境变量”），用于指定将存储其被转换正文部分的程序。

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，而不是对正文部分执行命令。

注 – 只要修改了 conversions 文件，就必须重新编译配置（请参见第 203 页中的 “10.1 编译 MTA 配置”）。

13.5.3.1 转换通道信息流程

信息的流程如下：包含正文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。然后转换通道对正文部分进行限定，即通过将正文部分的 MIME 标题行与**限定参数**进行比较来确定是否对其进行处理。如果正文部分合格，则开始转换处理。如果要将 MIME 或正文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**指定的环境变量中（请参见第 384 页中的 “13.5.3.2 使用转换通道环境变量”）。

这时，将对正文部分执行由**操作参数**指定的操作。通常，该操作为删除正文部分或将其传递给脚本中包含的程序。脚本将处理正文部分，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正文部分的新的 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，转换通道将替换由**输出参数**指定的输出正文部分的标题行。

13.5.3.2 使用转换通道环境变量

对邮件正文部分进行操作时，在通道和站点提供的程序之间来回传递 MIME 标题行信息（或整个正文部分）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正文部分。通常，站点提供的程序的主要输入部分是从文件读取的邮件正文部分。对正文部分进行处理后，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进行创建（请参见第 387 页中的 “13.5.3.3 使用转换通道输出选项”）。

以下 `conversions` 文件条目和外来邮件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=*` 指定将处理来自类型 `application` 的所有输入通道的邮件正文部分。

`parameter-symbol-0=NAME` 指定将第一个 `Content-type` 参数值（在本例中为 `Draft1.doc`）存储在一个称作 `NAME` 的环境变量中。

parameter-copy-0=* 指定将输入正文部分的所有 Content-type 参数复制到输出正文部分。

dparameter-symbol-0=FILENAME 指定将第一个 Content-disposition 参数值（在本例中为 Draft1.doc）存储在一个称作 FILENAME 的环境变量中。

dparameter-copy-0=* 指定将输入正文部分的所有 Content-disposition 参数复制到输出正文部分。

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 MIME 部分中的原始 MIME 标题行。$OUTPUT_HEADERS 是转换运行时创建的应急临时文件。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正文部分时，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 指定转换通道从由 OUTPUT_OPTIONS 环境变量命名的文件读取**转换通道选项**。请参见第 387 页中的 “13.5.3.3 使用转换通道输出选项”。

command="msg-svr-base/bin/viro-scan500.sh" 指定对邮件主题部分执行的命令。

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	最初存在于正文部分中的编码。
INPUT_FILE	包含原始正文部分的文件的名称。站点提供的程序应读取此文件。
INPUT_HEADERS	包含正文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。

表 13–3 转换通道环境变量 （续）

环境变量	说明
INPUT_DISPOSITION	输入邮件部分的 MIME content-disposition。
MESSAGE_HEADERS	文件名称，此文件包含封闭邮件（不只是正文部分）的原始最外层标题，或者包含该部分的最直接封闭 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。
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 387 页中的 “13.5.3.3 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名和域级别的 LDAP 属性。这些选项都没有默认属性。

系统 Sieve 可以使用两个新的操作：addconversiontag 和 setconversiontag。两个操作都接受单参数：一个字符串或者一个转换标记列表。addconversiontag 将转换标记添加到当前的标记列表，setconversiontag 在添加新标记前清空现有列表。请注意，这

两个操作很晚才会执行，因此可以使用 setconversiontag 取消所有其他转换标记设置机制。这使您能在 Sieve 过滤器中放置转换标记。

Sieve 信封测试接受 conversiontag，将其作为信封字段说明符值。该测试检查当前的标记列表，每次检查一个。请注意，如果指定了 :count 修饰符，将能够检查活动转换标记的数量。此类型的信封测试仅限于系统 Sieve。还要注意，该测试只查看 Sieve 处理之前存在的标记集—无法看到 setconversiontag 和 addconversiontag 操作的效果。

在各种映射探测中包含转换标记信息

添加了一个新的 MTA 选项 INCLUDE_CONVERSIONTAG，可选择性地在各种映射探测中包含转换标记信息。该选项是按位编码的值。下表中显示了分配的位。在任何情况下，当前的标记集在探测中都以逗号分隔的列表的形式显示。

位置	值	映射
0	1	CHARSET_CONVERSION - 作为 ;TAG= 字段添加到 ;CONVERT 前面。
1	2	CONVERSION - 作为 ;TAG= 字段添加到 ;CONVERT 前面
2	4	FORWARD - 添加到当前地址的前面并紧接当前地址（以 | 分隔）
3	8	ORIG_SEND_ACCESS - 添加到探测结尾处（以 | 分隔）
4	16	SEND_ACCESS - 添加到探测结尾处（以 | 分隔）
5	32	ORIG_MAIL_ACCESS - 添加到探测结尾处（以 | 分隔）
6	64	MAIL_ACCESS - 添加到探测结尾处（以 | 分隔）

13.5.3.3 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，在正文部分处理期间，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 来启动的。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。脚本完成对正文部分的处理后，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 deleted' 行通知转换通道将文本 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更多信息，请参阅第 390 页中的 “13.5.4 使用转换通道输出退回、删除、保留或重试邮件”）

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 **模式**，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。

13.5.3.4 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中。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。

13.5.3.5 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，也可以在这样的文件中对其进行检索。某些客户端使用普通名称（例如 att.dat ）发送所有附件，不管附件是属于 postscript、 msword、text 还是其他任何类型，上述功能对于重命名这些客户端发送的附件很有用。这是重新标记邮件部分，以便其他客户端（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的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=* 指定要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; 指定邮件处理后的 MIME Content-type 参数为 application。

out-subtype='INPUT-SUBTYPE'; 指定正文部分处理后的 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`; 指定输出正文部分的第一个 MIME Content-type 参数为类型 `name=`。

`out-parameter-value-0='X-ATT-NAMES:\\'INPUT_SUBTYPE\\''`; 指定使用第一个 MIME `subtype` 参数值，并在映射表 `X-ATT-NAMES` 中搜索匹配的 `subtype`。如果找到匹配项，`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`，则 `name` 参数将为 `temp.DOC`。

13.5.4 使用转换通道输出退回、删除、保留或重试邮件

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`。这将通知转换通道从 `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正文部分进行的操作。
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
PMDF__FORCEDISCARD	0x0A9C86B3	178030259
PMDF__AGN	0x0A9C809A	178028698

我们将使用示例来说明这些指令的功能。

13.5.4.1 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."

13.5.4.2 有条件地删除邮件或邮件部分

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
```

类似地，可以使用以下命令删除整个邮件：

```
echo "STATUS=178030259" >> $OUTPUT_OPTIONS
```

13.5.4.3 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
```

这将请求转换通道在转换通道队列中将邮件保留为 .HELD 文件。

13.5.4.4 导致邮件被重新处理

在转换器脚本遇到临时资源问题时（例如，系统无法连接到外部服务器、需要的文件被锁定等等），您可以使用 PMDF_AGN 来通知转换通道考虑处理遇到临时错误的邮件。MTA 将在 mail.log_current 中记录 "Q" 状态的邮件，并将该邮件保留在转换通道中，在以后重新尝试处理。

将以下命令行添加到转换脚本中：

```
echo "STATUS=178028698" >> $OUTPUT_OPTIONS
```

13.5.5 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'"
```

转换参数如下所示：

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。
IN-TYPE	执行转换所需匹配的输入 MIME 类型（允许使用通配符）。仅当此字段与正文部分的 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）。仅当此字段与正文部分的 MIME 子类型匹配时，才执行此条目指定的转换。

表 13–6 转换参数 （续）

参数	说明
IN-PARAMETER-NAME-*n*	必须与转换匹配的输入 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，以通过其所包含的名称和值明确标识参数。
IN-PARAMETER-VALUE-*n*	必须与转换匹配的相应 IN-PARAMETER-NAME 的输入 MIME Content-Type 参数值。仅当此字段与正文部分的 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。正文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	要与转换匹配的输入 MIME Content-Disposition。
IN-DPARAMETER-NAME-*n*	必须与转换匹配的输入 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，以通过其所包含的名称和值明确标识参数。
IN-DPARAMETER-VALUE-*n*	必须与转换匹配的相应 IN-DPARAMETER-NAME 的输入 MIME Content-Disposition 参数值。仅当此字段与正文部分的 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。正文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	要与转换匹配的输入 MIME Content-Description。
IN-SUBJECT	来自封闭 MESSAGE/RFC822 部分的输入 Subject。
TAG	输入标记，由邮件列表 CONVERSION_TAG 参数所设置。
输出参数（指定正文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*	与 OUT-PARAMETER-NAME-*n* 相对应的输出 MIME Content-Type 参数值。
PARAMETER-COPY-*n*	要从输入正文部分的 Content-Type 参数列表复制到输出正文部分的 Content-Type: 参数列表的 Content-Type 参数列表； *n*=0、1、2... 使用与要复制的 MIME 参数相同的名称，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...
OUT-DPARAMETER-VALUE-*n*	与 OUT-DPARAMETER-NAME-*n* 相对应的输出 MIME Content-Disposition 参数值。

表 13–6 转换参数 （续）

参数	说明
DPARAMETER-COPY-*n*	要从输入正文部分的 Content-Disposition: 参数列表复制到输出正文部分的 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 * 表示复制所有原始 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（二进制文件和可执行文件）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（指定要对邮件部分执行的操作。）	
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。使用 / 指定路径，而不是 \。例如 : 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 将执行站点提供的步骤，这些步骤将对整个 MIME 邮件（MIME 标题和内容正文部分）进行。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，而在字符集转换处理期间执行 SERVICE-COMMAND 条目。使用 / 指定路径，而不是 \。例如：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 参数要转换成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，将把直接封闭的正文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，将把封闭的 MESSAGE/RFC822 部分（不只是正文部分）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 正文部分的编号。

13.5.6 自动检测 Arabic 字符集

为了自动检测 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多数未标记或未正确标记的文本邮件（以 Arabic 字符集显示）。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，许多邮件客户端就不能正确显示邮件。

如果邮件包含 MIME content-type 标题，则 auto_ef 程序将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 content-type 标题标记的，则 auto_ef 将无条件地增加文本/纯文本内容类型。

要激活或启用此程序，必须：

▼ 自动检测 Arabic 字符集

1 **编辑 *msg-svr-base* /config 目录下的映射文件来启用要用于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，该文件由当前版本 Messaging Server 的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

13.6 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，本节中的某些示例涉及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，但并不表示这些示例仅适用于 DEC 或 d 通道。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（发出邮件的通道），*out-channel* 是目标通道的名称（邮件将进入的通道）。如果存在匹配项，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	即使邮件即将在进入 *out-channel* 之前通过转换通道，也强制进行转换。
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。该关键字仅适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 正文部分（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 正文部分（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。

表 13–7 CHARSET-CONVERSION 映射表关键字 （续）

关键字	说明
Top	将所有 message/rfc822 正文部分（转发的邮件）“转变”为标题部分和邮件内容部分。
UUENCODE	将 MIME 编码转换为 X-UUENCODE。
Yes	启用转换。

13.6.1 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* 指定应将 in-char-set 转换成的字符集的名称。请注意，这两个字符集都必须在位于 MTA 表格目录中的字符集定义表 charsets.txt 中进行定义。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 只是替换 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 13–2 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。特别地，假定是通过 `tcp_local` 连接到 Internet，并且 `tcp_internal` 和 `ims-ms` 分别是内部邮件的源通道和传送通道。以下显示的 `CHARSET-CONVERSION` 表是以上述假定为前提进行的转换。请注意，每个 `IN-CHAN` 条目都必须单成一行。反斜杠 (\) 用于表示这一点。

```
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 13–3 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 之间的相互转换。

```
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
```

13.6.2 邮件的重新格式化

如上所述，`CHARSET-CONVERSION` 映射表对附件在 MIME 和若干专用邮件格式之间的转换也起作用。

以下各节给出了可以使用 `CHARSET-CONVERSION` 映射表进行的其他类型的邮件重新格式化的示例。

13.6.2.1 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。如果具有 tcp_local 通道，则此通道通常是来自 Microsoft Mail SMTP 网关的邮件的外来通道，以下命令将对传送到本地用户的邮件进行转换：

```
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，对于只是通过您的系统却未必属于您自己的站点的邮件，这种不加选择的转换会使系统在转换方面变得迟疑不决或无能为力，在这种情况下系统应该只起传输作用，不必更改除邮件信封和相关传输信息以外的其他信息。

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映射文件中：

```
CHARSET-CONVERSION

  IN-CHAN=*;OUT-CHAN=tcp_msmail;CONVERT        RFC1154
```

13.6.2.2 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何 MIME 重新标记操作。有关 conversions 文件条目的信息，请参见第 382 页中的 “13.5.3 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 conversion 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，如果最初到达时的 MIME 标记为 application/octet-stream，但文件名参数带有扩展名 ps 或 msw，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，可用于将这样生成的 MIME 类型转换回相应的 MRTYPE 标记（这类标记需要进行精确的 MIME 标记才能以最佳方式运行）；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。

利用以上示例组合以及包括以下内容的 MIME-CONTENT-TYPES-TO-MR 映射表条目

```
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也很有用，亦即将特定的 MIME 附件标记“降级”为通用二进制数据标记 application/octet-stream。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（从而可应用 convert_octet_stream）。

13.6.2.3 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 用于通知 MTA 将其他 MacMIME 结构化部分分别转换为 MIME 结构 multipart/appledouble、application/applefile、application/mac-binhex40 或 application/macbinary。此外，如果非 MacMIME 格式部分的 MIME Content-type: 标题中包含 X-MAC-TYPE 和 X-MAC-CREATOR 参数，则 Binhex 或 Macbinary 关键字还可以请求将该部分转换成指定的格式。CHARSET-CONVERSION 关键字 Block 通知 MTA 仅从 MacMIME 格式部分中提取数据部分，放弃资源部分（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。

转换为 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 部分的数据部分中的特定 MIME 标签，具体情况取决于原始 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，则正确的表会是 :

```
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样例条目。

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）。

13.6.3 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用于处理邮件，以生成新格式的邮件。上述类型的 `CHARSET-CONVERSION` 操作和 `conversion` 通道操作都是在个别 MIME 邮

件部分的内容中进行的，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 邮件中进行的。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 映射表的第一次探测产生了 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，则予以执行。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 通道的所有邮件均被压缩。

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 的值分别为 a.in 和 a.out，则在 UNIX 上有如下声明：

```
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

14 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 379 页中的 “13.5 转换通道”）所提供的技术更加强大。Messaging Server 支持 Symantec Brightmail AntiSpam、SpamAssassin、Milter 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**功能的信息也可用于**反病毒**或**病毒过滤**功能（如果适用）。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，`spam` 通常用于配置参数。

本章分为以下几节：

14.1 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 读取结论并对邮件进行 Sieve 操作（请参见第 415 页中的 “14.2.3 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。协议可能是标准协议（在 Symantec AntiVirus Scan Engine 等基于 ICAP 的程序中）、专用协议（在 Brightmail 中）或只是非标准协议（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。

14.2 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执行五个操作：

1. **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 允许您最多使用八种不同的垃圾邮件/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。
2. **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。
3. **装入和配置过滤客户端库**。此操作包括在 MTA `option.dat` 文件中指定客户端库和配置文件，以及在过滤软件的配置文件中设置所需选项。请参见第 409 页中的 “14.2.1 装入和配置垃圾邮件过滤软件客户端库”
4. **指定要过滤的邮件**。用户、域或通道均可以过滤邮件。请参见第 410 页中的 “14.2.2 指定要过滤的邮件”。
5. **指定如何处理垃圾邮件**。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 415 页中的 “14.2.3 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。现在这些关键字和选项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。

14.2.1 装入和配置垃圾邮件过滤软件客户端库

每个垃圾邮件过滤程序都应为 Messaging Server 提供客户端库文件和配置文件。装入和配置客户端库包括以下两个操作：

- 在 `option.dat` 文件中指定垃圾邮件过滤软件库的路径 (`spamfilter`*X*`_library`) 和配置文件 (`spamfilter`*X*`_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 419 页中的 “14.3 使用 Symantec Brightmail Anti-Spam” 和第 435 页中的 “14.5 使用 Symantec Anti-Virus Scanning Engine (SAVSE)”

14.2.1.1 指定垃圾邮件过滤软件库的路径

Messaging Server 最多可为邮件调用八种不同的过滤系统。例如，您可以通过 Symantec AntiVirus Scan Engine 和 SpamAssassin 运行邮件。每个过滤软件均由 1 到 4 之间的数字进行标识。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，`sourcespamfilter`*X*`optin` 或 `spamfilter`*X*`_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` 设置可指定 Messaging Server 同时通过 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` 将引用 SpamAssassin。`sourcespamfilter1optin` 将引用 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，您可以只注释掉 `spamfilter1_library` 配置文件。

14.2.2 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 可以配置为基于用户、域或通道过滤邮件。以下每节介绍了一种方案：

- 第 410 页中的 “指定用户级别的过滤”
- 第 410 页中的 “14.2.2.1 用户级别的过滤示例”

注 – 表达式 *optin* 表示选择用户、域或通道来接收邮件过滤。

▼ 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，则您可以指定哪些用户可以和不可以接收该服务。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
```

注 – 默认情况下，模式中不存在 `SymantecAV` 或 `SpamAssassin` 之类的属性。无论使用何种新属性，都需要将其添加到目录模式中。有关说明，请参见相应的 Directory Server 文档。

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，如果将 Brightmail 的过滤器属性设置为 `Brightmail`，则条目为：

```
Brightmail: spam
Brightmail: virus
```

14.2.2.1 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。第 410 页中的 “14.2.2.1 用户级别的过滤示例” 显示了 Otis Fanning 的 Brightmail 用户条目。

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
```

请参见第 419 页中的 “14.3 使用 Symantec Brightmail Anti-Spam”、第 423 页中的 “14.4 使用 SpamAssassin”或第 435 页中的 “14.5 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
```

注 – 默认情况下，模式中不存在 `SymantecAV` 或 `SpamAssassin` 之类的属性。无论使用何种新属性，都需要将其添加到目录模式中。有关说明，请参见相应的 Directory Server 文档。

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值条目。例如，如果将 `LDAP_DOMAIN_ATTR_OPTIN1` 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。此外，还假定在 `option.dat` 文件中将 `LDAP_DOMAIN_ATTR_OPTIN1` 设置为 `Brightmail`。在 Sun LDAP Schema 1 DC 树的 `sesta.com` 域条目中，将 Brightmail 属性设置为 `spam` 和 `virus`。对于 Sun LDAP Schema 2，也在接收垃圾邮件过滤的域条目中对 `Brightmail` 进行设置。

Brightmail 将对所有发送到 `sesta.com` 的邮件进行垃圾邮件和病毒过滤。下面显示了第 412 页中的 “域级别过滤示例”。

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:*
```

示例 14–2 Brightmail 的示例 LDAP 域条目 （续）

```
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，请参见第 419 页中的 “14.3 使用 Symantec Brightmail Anti-Spam” 、第 423 页中的 “14.4 使用 SpamAssassin” 或第 435 页中的 “14.5 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 中继发送到后端消息存储的邮件
- 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 允许您按照源通道或目标通道指定过滤。第 369 页中的 “12.12.5 垃圾邮件过滤器关键字” 中所述的通道关键字是实现此过滤的机制。以下示例说明如何设置通道级别的过滤。

1 **在所有入站 SMTP 服务器（负责向后端消息存储主机发送邮件）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
msg_store1.siroe.com
```

通道级别过滤示例

这些示例均假定过滤程序由数字 1 指定。有关可用于垃圾邮件过滤的关键字，请参见第 369 页中的 “12.12.5 垃圾邮件过滤器关键字” 。

▼ 过滤从 MTA 中继发送到后端消息存储的邮件

此示例对所有从 MTA 中继发送到称为 `msg_store1.siroe.com` 的后端消息存储的邮件进行垃圾邮件和病毒过滤。

1 在 `imta.cnf` 文件（负责向后端消息存储主机发送邮件）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 \
destinationspamfilter 1optin 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 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 \
destinationspamfilter1optin 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 \
sourcespamfilter1optin spam destinationspamfilter1optin spam
tcp-daemon
```

示例 5。过滤所有发送到两层系统中本地消息存储的邮件，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 \
destinationspamfilter1optin 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和病毒过滤）：

```
tcp_local smtp mx single_sys remotehost inner switchchannel \
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \
maytlsserver maysaslserver saslswitchchannel tcp_auth \
destinationspamfilter1optin spam,virus sourcespamfilter1optin \
spam,virus
tcp-daemon
```

14.2.3 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 的当前版本返回结论说明邮件是否为垃圾邮件。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 14–1 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`（指定返回的垃圾邮件结论为空值时要执行的 Sieve 规则）和 `SpamfilterX_string_action`（指定返回的垃圾邮件结论为字符串时要执行的 Sieve 规则）。

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。有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）命名的文件中。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。此行将向通过字符串结论值确定为垃圾邮件的每封邮件中添加标题 `Spam-test: FAIL`：

```
spamfilter1_string_action=data:,require ["addheader"];addheader "Spam-test:
FAI";
```

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。如果标题包含 `resent-from` 和 `User-1`，则此行假定结论值为字符串，并且将垃圾邮件归档到邮箱 `testspam` 中。如果邮件不包含此标题，则此行将邮件归档到 `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 14–1 MTA 垃圾邮件过滤器选项 (option.dat)

用于 Spam Assassin 的 MTA 选项	说明
`Spamfilter`*X*`_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
`Spamfilter`*X*`_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

表 14–1 MTA 垃圾邮件过滤器选项 (option.dat) （续）

用于 Spam Assassin 的 MTA 选项	说明
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。0 指定垃圾邮件过滤问题将导致临时处理故障。1 会导致在某些（可能并非全部）过滤库发生故障的情况下，系统将跳过垃圾邮件过滤处理。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。-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，此设置会导致发送系统日志消息。3 将导致垃圾邮件过滤器无法接受邮件，但会将其排入重新处理通道队列等待稍后处理。4 与 3 的功能相同，但还会将垃圾邮件过滤器临时故障记录到 syslog。 默认值：0
LDAP_optinX	指定基于每个用户激活过滤软件 X 所使用的 LDAP 属性名称。过滤是基于目标地址的。也就是说，使用此属性定向到用户的邮件将进行垃圾邮件过滤。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
LDAP_SOURCE_OPTIN X	LDAP_SOURCE_OPTIN1 到 LDAP_SOURCE_OPTIN8 提供基于创始者地址的每个用户垃圾邮件过滤器 optin 值，这些值类似于 LDAP_optinX。也就是说，从该用户发出的邮件将进行垃圾邮件过滤。
LDAP_domain_attr_optinX	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。除了应位于对象类 mailDomain 中之外，其余与 LDAP_optin 相同。 默认值：无
SpamfilterX_null_optin	指定一个字符串，如果发现该字符串为 LDAP_optinX 或 LDAP_domain_attr_optinX 定义的属性值，将导致 MTA 执行该属性不存在时所执行的操作。也就是说，该字符串禁用了此条目的过滤。请参见第 410 页中的 “14.2.2 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 spamfilterX_null_optin 设置为实际始终不会出现的字符串来恢复 5.2 版的这种行为。）
SpamfilterX_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 reject 操作拒绝垃圾邮件，因为这样做会向无辜的一方（其地址被用于发送垃圾邮件）发送不能传递的通知。默认值：data:,discard;
SpamfilterX_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一方（其服务器被用于发送垃圾邮件）发送不能传递的通知。 默认值：data:,require "fileinto"; fileinto "$U; 其中 $U 是 verdict 返回的字符串。

表 14–1 MTA 垃圾邮件过滤器选项 (option.dat) （续）

用于 Spam Assassin 的 MTA 选项	说明

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，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 拒绝操作：
	
	`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	某些过滤库可以基于收件人地址执行一组操作。spamfilter*X*_final 可以指定传递到过滤库的收件人地址的类别。设置为 `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`
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 传递选项，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站点的安全策略。 没有一个答案在所有情况下均正确。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。）

14.3 使用 Symantec Brightmail Anti-Spam

Brightmail 解决方案由 Brightmail 服务器和下载至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。除以下各节外，请参阅《Configuring Brightmail with Sun Java System Messaging Server》。

14.3.1 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。

14.3.1.1 Brightmail 体系结构

图 14–1 说明了 Brightmail 的体系结构。

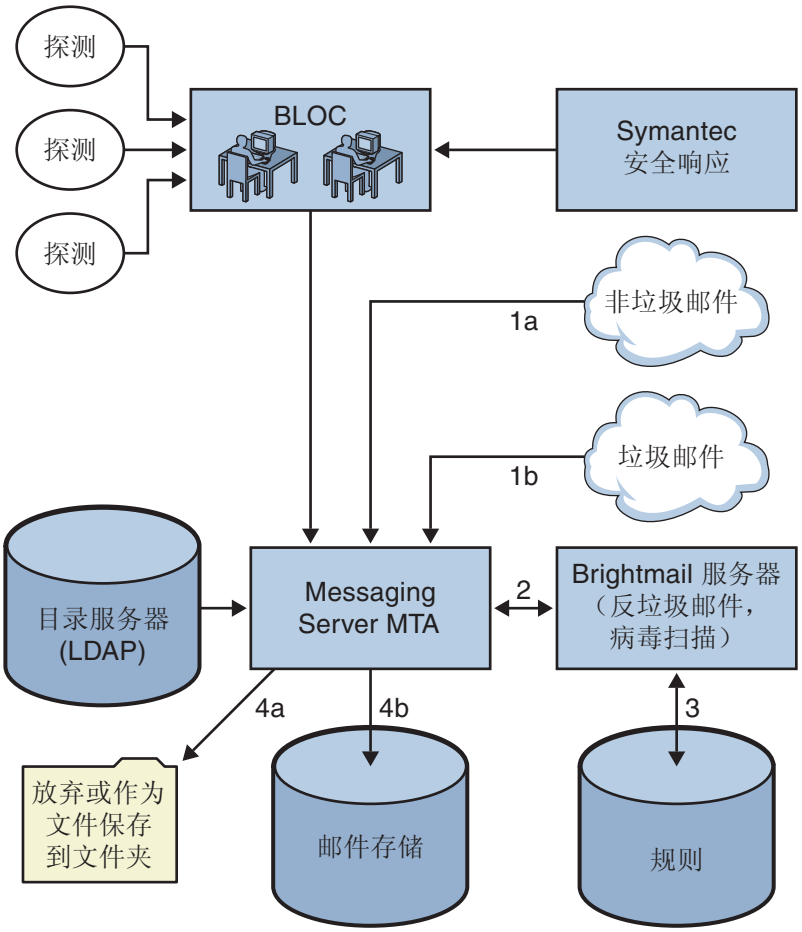


图 14–1 Brightmail 和 Messaging Server 体系结构

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 还提供了“内容过滤”服务，但此功能是使用 Sieve 提供的，因此让 Brightmail 进行 Sieve 过滤并不会带来任何附加值。

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、将其归档到文件夹中、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。

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。

14.3.2 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 执行垃圾邮件和病毒检查，则 MTA 邮件吞吐量可能会降低 50%。要保持 MTA 总处理能力，可能需要为每个 MTA 配置两台 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。

14.3.3 部署 Brightmail

执行以下步骤部署 Brightmail。

- **安装和配置 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 422 页中的 “14.3.4 Brightmail 配置选项”中显示了选定的 Brightmail 配置选项，但最新、最完整的信息位于 Brightmail 文档中。
- **装入和配置 Brightmail 客户端库**。此操作包括向 MTA 指定 Brightmail 客户端库 `libbmiclient.so` 和配置文件 `config`。请参见第 409 页中的 “14.2.1 装入和配置垃圾邮件过滤软件客户端库”
- **指定要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 410 页中的 “14.2.2 指定要过滤的邮件”。
- **指定要对垃圾邮件执行的操作**。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 415 页中的 “14.2.3 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**。请参见表 14–1。

14.3.4 Brightmail 配置选项

表 14–2 中显示了选定的 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 14–2 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，然后再进行垃圾邮件处理。将 Brightmail 和 Sun Java System Messaging Server 结合使用时，建议使用此设置。
`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，因此应将值指定为 `inbox`。没有默认值。
`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。 请参见下面的 `blSWClientDestinationLocal` 和 `blSWClientDestinationForeign`。例如，您可以指定 `blSWLocalDomain=siroe.com`

表 14–2 选定的 Brightmail 配置文件选项 （续）

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 | 右侧没有内容）的默认解释为放弃邮件。因此在上述示例中，如果结论为 virus，则放弃邮件。如果结论为 spam，上述示例将把邮件归档至名为 spambox 的文件夹中。如果邮件既不是垃圾邮件，又不包含病毒，则结论不匹配，将根据上述 blSWClientDestinationDefault 设置中的设置正常传送邮件。 使用与 MTA 分开的 Brightmail 服务器时，可以通过使用 Brightmail_verdict_n、Brightmail_action_n、Brightmail_null_action 和 Brightmail_string_action MTA 选项自定义每个 MTA 执行的操作，以覆盖 Brightmail 服务器返回的操作和结论。在此示例中，您可以使用 MTA 中不同的 Brightmail_null_action 来覆盖 Virus 操作（放弃邮件），或使用 Brightmail_verdict_0=spambox 和 Brightmail_action_0=data:,require "fileinto";fileinto "Junk"; 将邮件归档至名为 Junk 而不是 spambox 的文件夹。
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

14.4 使用 SpamAssassin

本节包含以下几个部分：

14.4.1 SpamAssassin 概述

Messaging Server 支持使用 SpamAssassin，SpamAssassin 是一种用于识别垃圾邮件的免费邮件过滤器软件。SpamAssassin 由一个使用 Perl 编写的库和一组可用于将 SpamAssassin 集成到邮件服务系统的应用程序和实用程序组成。

SpamAssassin 通过对邮件标题和正文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 结果字符串的示例为：

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所使用的同一机制也可以用于连接到 SpamAssassin `spamd` 服务器。Messaging Server 中提供的模块称为 `libspamass.so`。

14.4.2 SpamAssassin/Messaging Server 操作原理

`spamd` 是 SpamAssassin 的守护进程版本，可以从 MTA 中调用。`spamd` 侦听套接字上的请求并产生子进程来测试邮件。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 安装中的客户端部分 `spamc`。相反，客户端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。装入 `libspamass.so` 的方法与装入 Brightmail SDK 的方法相同。

从 MTA 的角度来看，您几乎可以在用于垃圾邮件过滤的 SpamAssassin 和 Brightmail 之间进行透明地切换。但并非完全透明，因为二者的功能不同。例如，Brightmail 还可以进行病毒过滤，但是 SpamAssassin 仅用于垃圾邮件过滤。这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` 选项允许您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 433 页中的 “14.4.7 SpamAssassin 选项”。

14.4.3 SpamAssassin 要求和使用注意事项

- SpamAssassin 为免费软件。可以在 http//www.spamassassin.org 上找到该软件和相关文档。
- 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 没有提供安全套接口层 (Secure Socket Layer, SSL) 版本的 `libspamass.so`，但是可以通过建立 SpamAssassin 来使用 openSSL。
- 需要 Perl 5.6 或更高版本。

14.4.3.1 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 和消息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。不能从消息存储中调用过滤。如果在 MTA 和消息存储之间使用 SMTP，则既可以从 MTA 也可以从消息存储中调用过滤，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。

14.4.4 部署 SpamAssassin

执行以下步骤部署 SpamAssassin。

- **安装和配置 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 433 页中的 “14.4.7 SpamAssassin 选项”。
- **装入和配置 SpamAssassin 客户端库**。此操作包括向 MTA 指定客户端库 `libspamass.so` 和配置文件（必须创建此文件）。请参见第 409 页中的 “14.2.1 装入和配置垃圾邮件过滤软件客户端库”
- **指定要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 410 页中的 “14.2.2 指定要过滤的邮件”。
- **指定要对垃圾邮件执行的操作**。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 415 页中的 “14.2.3 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**。请参见表 14–1

14.4.5 SpamAssassin 配置示例

本节介绍了一些通用的 SpamAssassin 配置示例：

- 第 426 页中的 “将垃圾邮件归档到单独的文件夹”
- 第 427 页中的 “向垃圾邮件添加包含 SpamAssassin 分数的标题”
- 第 428 页中的 “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。请参阅第 369 页中的 “12.12.5 垃圾邮件过滤器关键字” 和表 14–1。

▼ 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消息存储的邮件，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` 是个很好的名称。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 `spamd` 的系统的名称，以及 `spamd` 侦听外来请求的端口。`mode=0` 指定如果系统将邮件识别为垃圾邮件，则返回一个由 `verdict` 指定的字符串。`debug=1` 指定在 SpamAssassin 库中启用调试。请参见表 14–3

2 向 `option.dat` 文件中添加以下各行：

```
! for Spamassassin
spamfilter1_config_file=/opt/SUNWmsgsr/config/spamassassin.opt
spamfilter1_library=/opt/SUNWmsgsr/lib/libspamass.so
spamfilter1_optional=1
spamfilter1_string_action=data:,require "fileinto"; fileinto "$U";
```

`spamfilter1_config_file` 指定 SpamAssassin 配置文件。

`spamfilter1_library` 指定 SpamAssassin 共享库。

`spamfilter1_optional=1` 指定 spamd 失败时，MTA 将继续运行。

`spamfilter1_string_action` 指定对垃圾邮件采取的 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 返回的值由 spamassassin.opt 中的 verdict 选项指定。（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。**

要过滤传入到本地消息存储的所有邮件，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 守护进程。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 SpamAssassin 和 Messaging Server 是在不同的系统中运行，则需要此语法：

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，因为 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* 添加至已由 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: 为文字，其后的内容为结果字符串。True 表示邮件为垃圾邮件（false 表示非垃圾邮件）。7.3 为 SpamAssassin 分数。5.0 为阈值。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。请参见表 14–3 中的 USE_CHECK。

1. **指定要过滤的邮件。第 426 页中的“ 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。**

   此文件的名称和位置是使用 `spamfilter_configX_file` 指定的（见下一步）。其中包含以下各行：

   ```
   host=127.0.0.1
   port=2000
   mode=1
   field=
   debug=1
   ```

   `host` 和 `port` 分别指定运行 `spamd` 的系统的名称，以及 `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=` 指定 SpamAssassin 结果字符串的字符串前缀。在此示例中，由于我们要在 Sieve 脚本中指定字符串前缀，因此无需前缀。`debug=1` 指定在 SpamAssassin 库中启用调试。

3. **向 `option.dat` 文件中添加以下各行：**

   ```
   !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。因为在上一步中指定了 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，然后启动 `spamd` 守护进程。**

   请参见第 426 页中的 “14.4.5 SpamAssassin 配置示例” 。

▼ 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 433 页中的 “14.4.7 SpamAssassin 选项”）。因为此列表可能会很长，所以最好将 USE_CHECK 设置为 1。

1 **指定要过滤的邮件。**

请参见第 426 页中的 “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 426 页中的 “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 分别指定运行 spamd 的系统的名称，以及 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。debug=1 指定在 SpamAssassin 库中启用调试。

3 **向 option.dat 文件中添加以下各行：**

```
!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]";
```

指定要向 Subject: 行添加标记。此标记的文字前缀为 SPAM detected，后跟字段字符串（默认值：Spam-Test），其后是 SpamAssassin 返回的 "[*result string*]"。因为已在第 426 页中的 “14.4.5 SpamAssassin 配置示例”中指定 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
```

可设置 spamassassin.opt 中的 field= 来删除 Spam-Test 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，然后启动 spamd 守护进程。**

请参见第 426 页中的 “将垃圾邮件归档到单独的文件夹”。

▼ 基于 SpamAssassin 分数过滤邮件

本示例介绍了如何基于 SpamAssassin 分数过滤邮件。它使用 spamadjust 和 spamtest Sieve 过滤器操作。在本示例中，包含 SpamAssassin 分数的标题被添加到所有邮件。SpamAssassin 软件管理员可以使用此标题来调整 SpamAssassin 以改进垃圾电子邮件检测。如果邮件的 SpamAssassin 分数在 5 和 10 之间，则邮件被过滤到用户帐户内的 spam 文件夹。如果邮件的 SpamAssassin 分数大于 10，则邮件将被放弃。请注意，在默认情况下，SpamAssassin 认为分数大于等于 5 的邮件为垃圾邮件。

1 **指定要过滤的邮件。**

第 426 页中的 “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。**

此文件的名称和位置是使用 spamfilter_configX_file 指定的（见下一步）。其中包含以下各行：

```
debug=1
host=127.0.0.1
port=783
mode=2
field=
```

host 和 port 分别指定运行 spamd 的系统的名称，以及 spamd 侦听外来请求的端口。mode=2 指定始终返回 SpamAssassin 结果字符串，无论分数是多少。field= 指定 SpamAssassin 结果字符串的字符串前缀。在此示例中，由于我们要在 Sieve 脚本中指定字符串前缀，因此无需前缀。debug=1 指定在 SpamAssassin 库中启用调试。

3 **向 option.dat 文件中添加以下各行：**

```
! For SpamAssassin
spamfilter1_config_file=/opt/SUNWmsgsr/config/spamassassin.opt
spamfilter1_library=/opt/SUNWmsgsr/lib/libspamass.so
spamfilter1_optional=1
spamfilter1_string_action=data:, require ["addheader","spamtest"]; \
spamadjust "$U"; addheader "Spam-test: $U"
```

如前面示例所述，前三行指定 SpamAssassin 配置文件、共享库，以及在共享库出现故障时继续执行 MTA 操作。后两行指定应从 SpamAssassin 的返回字符串 ($U) 中提取 SpamAssassin 分数（用于 spamtest 操作中），并向所有邮件添加垃圾邮件分数标题（例如，Spam-test: True; 7.3/5.0）

4 **创建通道级别过滤器，以基于垃圾邮件分数处理电子邮件。**

请参阅第 507 页中的 “创建通道级别的过滤器”。向该文件添加以下规则：

```
require ["spamtest","relational","comparator-i;ascii-numeric","fileinto"];
if spamtest :value "ge" :comparator "i;ascii-numeric" "10" {discard;}
elsif spamtest :value "ge" :comparator "i;ascii-numeric" "5" {fileinto "spam";}
else {keep;}
```

第二行放弃 SpamAssassin 分数大于等于 10 的垃圾电子邮件。第三行将分数大于等于 5 的电子邮件归档到用户的 “垃圾邮件” 文件夹。最后一行 `else {keep;}` 保留所有得分小于 5 的邮件。

5 **重新编译配置，重新启动服务器，然后启动 `spamd` 守护进程。**

请参见第 426 页中的 “将垃圾邮件归档到单独的文件夹”中的最后几步。

14.4.6 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/log/tcp_local_slave.log*` 文件应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
```

如果日志文件中不包含类似以上内容的行，或者 spamd 未运行，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。就像未启用垃圾邮件过滤功能一样，并会在 tcp_local_slave.log* 中显示以下行：

```
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 服务器收到整个邮件之后（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接受邮件之前，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 来发送样例垃圾邮件。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
```

14.4.7 SpamAssassin 选项

本节包含了 SpamAssassin 选项表。

表 14–3 SpamAssassin 选项 (spamassassin.opt)

选项	说明	默认值
`debug`	指定是否在 `libspamass.so` 中启用调试。对 `spamd` 本身的调试由调用 `spamd` 的命令行控制。请设置为整数值。0 为关闭，1 为打开，大于等于 2 的设置将报告从 spamd 接收的精确内容。	0
`field`	指定 SpamAssassin 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` 选项提供用于更改结果中 `Spam-Test:` 部分的方法。请注意，如果指定 `field` 的值为空，则将删除 ":"。 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 14–3 SpamAssassin 选项 (spamassassin.opt) （续）

选项	说明	默认值
mode	控制 SpamAssassin 过滤器结果向结论信息的转换。即指定在处理邮件之后要返回的结论信息。可以使用以下四种模式。有关详细说明，请参见第 435 页中的“14.4.7.1 SpamAssassin mode 选项”。 0—如果邮件为垃圾邮件，则返回**结论字符串**（由 verdict 选项指定）。MTA 选项 spamfilter*X*_string_action 可用于指定返回 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，并且邮件为垃圾邮件，则返回**空结论**。MTA 选项 spamfilter*X*_null_action 可用于指定返回空结论时要执行的操作。 如果不为垃圾邮件，则返回 *SpamAssassin* **默认结果字符串**。（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**。如果不为垃圾邮件，则返回 *SpamAssassin* **默认结果字符串**。（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）。不返回默认结论或空结论，并且从未使用 verdict 选项。 3—如果发现邮件为垃圾邮件，则返回 SpamAssassin 结果字符串；否则，将返回由 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 命令用于返回 SpamAssassin 分数。 0—启用 SYMBOLS 命令，此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）。	""
USERNAME_MAPPING	指定插件从 MTA 接收收件人地址时使用地址信息进行探测的映射的名称。探测的格式为： *current-username*|*current-recipient-address*|*current-optin-string* 如果映射设置了 $Y 标志，则输出字符串将作为更新的用户名传递给 spamd。	""

表 14–3 SpamAssassin 选项 (spamassassin.opt) （续）

选项	说明	默认值
verdict	指定用于 MODE 0 的结论字符串。	""

14.4.7.1 SpamAssassin mode 选项

处理完邮件后，SpamAssassin 将确定邮件是否为垃圾邮件。mode 允许您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 14–4 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	默认	SpamAssassin 结果	默认
verdict=string	是	verdict *string*	SpamAssassin 结果	SpamAssassin 结果	SpamAssassin 结果
	否	默认	默认	SpamAssassin 结果	verdict *string*

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。

14.5 使用 Symantec Anti-Virus Scanning Engine (SAVSE)

本节除了介绍如何部署 SAVSE 之外，对部署其他支持 ICAP 的反垃圾邮件/反病毒程序也很有用。本节包含以下几个部分：

14.5.1 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 的当前版本仅支持 SAVSE 的扫描功能。不支持修复或删除功能。

14.5.2 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。

14.5.2.1 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 和消息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。不能从消息存储中调用过滤。如果在 MTA 和消息存储之间使用 SMTP，则既可以从 MTA 也可以从消息存储中调用过滤，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 SAVSE 服务器地址。

14.5.3 部署 SAVSE

可执行以下步骤来部署 SAVSE。

- **安装和配置 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 438 页中的 “14.5.5 SAVSE 选项” 。
- **装入和配置 SAVSE 客户端库**。此操作包括向 MTA 指定客户端库 `libicap.so` 和配置文件（必须创建此文件）。请参见第 409 页中的 “14.2.1 装入和配置垃圾邮件过滤软件客户端库”
- **指定要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 410 页中的 “14.2.2 指定要过滤的邮件” 。
- **指定要对病毒邮件执行的操作**。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 415 页中的 “14.2.3 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 415 页中的 “14.2.3 指定要对垃圾邮件执行的操作”的表 14–1。

14.5.4 SAVSE 配置示例

以下示例将测试传入到本地消息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。

▼ 配置 SAVSE

1 创建 SAVSE 配置文件。

下一步骤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 的默认端口为 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（此示例中该字符串为 `virus`）。`debug=1` 启用调试。有关 ICAP 配置参数的说明，请参见第 438 页中的 “14.5.5 SAVSE 选项”。

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 SAVSE 配置文件。

`spamfilter1_library` 指定 SAVSE 共享库的位置。

`spamfilter1_optional=1` 指定 SAVSE 程序失败时，MTA 将继续运行。

`spamfilter1_string_action` 指定对垃圾邮件采取的 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，除非您要更改此值。

3 指定要过滤的邮件。

要过滤传入本地消息存储的所有邮件，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`**

14.5.4.1 其他可能的配置

将 `mode` 设置为 `0` 可以与 `spamfilterX_null_option` 一起使用，以进行其他操作（例如，将被确定为垃圾邮件的邮件归档至特定文件夹）。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，可以将垃圾邮件结果包含到拒绝邮件中，方法是将 `mode` 设置为 1，并将 MTA 中的 `spamfilter`*X*`_string_action` 选项设置如下：

```
spamfilter1_string_action=data:,require "reject"; reject "Message contained a
virus [$U]";
```

与 `fileinto` 一样，使用 `reject` 操作来处理病毒并不是一个好的方法，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，来向垃圾邮件标题中添加标记。示例：

```
spamfilter1_string_action=data:,addtag "[SPAM detected!]";
```

无需考虑邮件是否被确认带有病毒而尽管采取操作的情况下，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"
```

14.5.5 SAVSE 选项

SAVSE 选项文件是更为通用的 ICAP 选项文件。其名称和位置由 `option.dat` 中的 `spamfilterX_config_file` 进行设置。它由多个 `option=value` 格式的行组成。必须设置的一个选项为 `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 14–5 ICAP 选项

选项	说明	默认值
`debug`	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` 此选项提供一种用于更改结果中 `Virus-Test:` 部分的方法。请注意，如果指定 `field` 的值为空，则将删除 ":"。	Virus-test
`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，指定在处理邮件后要返回的字符串信息。可以使用以下四种模式。有关详细说明，请参见第 440 页中的 “14.5.5.1 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）。MTA 选项 `spamfilterX_string_action` 可用于指定返回 `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**。MTA 选项 `spamfilterX_null_action` 可用于指定返回结论为空并要覆盖“放弃邮件”的默认操作时所要采取的操作。 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: FALSEVIRUS-TEST: TRUE;` W32.Mydoom.A@mm.enc 2—无条件返回 ICAP 结果字符串；不返回默认结论或空结论，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： spamfilter*X*_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；否则，将返回由 `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。可以通过使用 `spamfilterX_verdict_`*n* 和 `spamfilterX_action_`*n* 匹配对来控制针对 ICAP 结果字符串所采取的操作。可以通过使用 `spamfilterX_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。	""

表 14–5 ICAP 选项 （续）

选项	说明	默认值
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。	""

14.5.5.1 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` 允许您指定由 ICAP 程序返回的表示结论的字符串。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，而是由程序返回的其他不可配置的字符串。下表概述了 `mode` 操作。

表 14–6 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	默认	ICAP 结果	默认
verdict=字符串	是	verdict *string*	ICAP 结果	ICAP 结果	ICAP 结果
	否	默认	默认	ICAP 结果	verdict *string*

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!`

14.6 使用 ClamAV

Messaging Server 支持使用常见且可免费获取的第三方病毒扫描程序 ClamAV，以检测邮件是否感染了病毒和特洛伊木马。可以使用 ClamAV 软件包随附的 `freshclam` 实用程序自动更新 ClamAV 用于检测新建病毒的病毒签名。

可以在 ClamAV 的 Web 站点上找到有关 ClamAV 的更多信息。

- 第 441 页中的 “14.6.1 ClamAV/Messaging Server 操作原理”
- 第 441 页中的 “14.6.2 ClamAV 要求和使用注意事项”
- 第 441 页中的 “14.6.3 部署 ClamAV”
- 第 442 页中的 “使用 ClamAV 丢弃被病毒或特洛伊木马感染的电子邮件”
- 第 443 页中的 “14.6.4 测试 ClamAV”
- 第 444 页中的 “14.6.5 ClamAV 选项”

14.6.1 ClamAV/Messaging Server 操作原理

Messaging Server 中的 ClamAV 集成使用了作为 ClamAV 软件包一部分提供的 `clamd` 守护进程。`clamd` 是一个多线程进程，可在套接字上侦听处理邮件的请求。处理邮件之后，它将发回响应并关闭连接。未使用 ClamAV 安装中的客户端部分 `clamdscan`。此功能由名为 `libclamav.so` 的共享库完成，该库是 Messaging Server 的一部分。

`libclamav.so` 的装入方式与 Brightmail SDK 相同。

14.6.2 ClamAV 要求和使用注意事项

ClamAV 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 和消息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。不能从消息存储中调用过滤。如果在 MTA 和消息存储之间使用 SMTP，则既可以从 MTA 也可以从消息存储中调用过滤。

如果要使用运行了 ClamAV 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 ClamAV 服务器地址。

其他注意事项。

- ClamAV 是免费提供的。可以在 `http://clamav.net` 上找到该软件和文档。
- 可以为用户、域或通道启用与 MTA 集成的 ClamAV。
- ClamAV 软件包提供一个用于定期更新病毒签名的实用程序。该实用程序名为 `freshclam`。有关更多信息，请参阅 ClamAV 软件包文档。
- Messaging Server 2006Q4 及更高版本在默认情况下包含 `libclamav.so` 库。

14.6.3 部署 ClamAV

可执行以下步骤来部署 ClamAV：

- **安装和配置 ClamAV**。请参阅 ClamAV 软件文档，以获得有关安装和配置的信息。另请参见 第 444 页中的 “14.6.5 ClamAV 选项”。
- **装入和配置 ClamAV 客户端库**。此操作包括向 MTA 指定客户端库 `libclamav.so` 和配置文件（必须创建此文件）。请参见第 409 页中的 “14.2.1 装入和配置垃圾邮件过滤软件客户端库”。
- **指定要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 410 页中的 “14.2.2 指定要过滤的邮件”。
- **指定要对病毒邮件执行的操作**。请参见第 415 页中的 “14.2.3 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 444 页中的 “14.6.5 ClamAV 选项”

▼ 使用 ClamAV 丢弃被病毒或特洛伊木马感染的电子邮件

以下示例将丢弃所有被 ClamAV 检测到包含病毒或特洛伊木马的邮件。未使用结论字符串。

1 创建 ClamAV 配置文件。

步骤 2 中指定了此文件的名称和位置。`clamav.opt` 是一个很好的文件名。本文件包含以下各行：

```
# more /opt/SUNWmsgsr/config/clamav.opt
! ClamAV Settings
debug=1
host=127.0.0.1
port=3310
mode=1
```

`debug=1` 指定在 ClamAV 库中启用调试。

`host` 和 `port` 分别指定运行 `clamd` 的系统的名称，以及 `clamd` 侦听外来请求的端口。

`mode=1` 指定在检测到被病毒感染的电子邮件时，ClamAV 插件返回 ClamAV 结果字符串作为结论。

2 修改 `option.dat` 文件。

向 `option.dat` 文件中添加以下各行：

```
! ClamAV settings
spamfilter2_config_file=/opt/SUNWmsgsr/config/clamav.opt
spamfilter2_library=/opt/SUNWmsgsr/lib/libclamav.so
spamfilter2_string_action=data:,require ["jettison"]; jettison;
```

`spamfilter2_config_file` 指定 ClamAV 配置文件。

`spamfilter2_library` 指定 ClamAV 共享库。

`spamfilter2_string_action` 指定对感染病毒的电子邮件采取的 Sieve 操作。

3 指定要过滤的邮件。

要过滤传入本地消息存储的所有邮件，请通过在 `ims-ms` 通道中添加 `destinationspamfilterXoptin` 病毒关键字来更改 `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 destinationspamfilter2optin 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 **启动 clamd 守护进程。**

14.6.4 测试 ClamAV

要测试 ClamAV，请首先在 clamav.opt 文件中设置 debug=1。（您不必在 imta.cnf. 中打开特定于通道的 master_debug 或 slave_debug）然后，向测试用户发送一个包含 EICAR 病毒字符串的文件附件 (http://www.eicar.org/anti_virus_test_file.htm)。此字符串用于触发病毒扫描程序在没有附加实际病毒的情况下识别已感染病毒的电子邮件：

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

查看测试日志。msg-svr-base/data/log/tcp_local_slave.log* 文件应具有类似以下内容的行：

```
10:39:00.85: ClamAV callout debugging enabled;
config /opt/SUNWmsgsr/config/clamav.opt
10:39:00.85: IP address 127.0.0.1 specified
10:39:00.85: Port 3310 selected
10:39:00.85: Mode 1 selected
10:39:00.85: Field "Virus-Test: " selected
10:39:00.85: Verdict "" selected
10:39:00.85: Initializing ClamAV message context
 ...
10:39:00.85: Creating socket to connect to clamd server
10:39:00.85: Binding clamd socket
10:39:00.85: Connecting to clamd server
10:39:00.85: Sending ClamAV STREAM request
10:39:00.85: Retrieving ClamAV STREAM response
10:39:00.85: STREAM response: PORT 2003
10:39:00.85: Creating socket to connect to clamd server data port
10:39:00.85: Binding clamd data socket
10:39:00.85: Connecting to clamd server data port
10:39:00.85: Sending ClamAV the message
10:39:00.85: Closing ClamAV data connection
10:39:00.85: Reading ClamAV result
10:39:00.87: Result line: stream: Eicar-Test-Signature FOUND
10:39:00.87: Scan result: Message is infected
10:39:00.87: Verdict line: Virus-Test: True ; Eicar-Test-Signature
10:39:00.87: Closing connection to ClamAV
```

```
10:39:00.87: Mode 1 verdict of Virus-Test: True ; Eicar-Test-Signature
10:39:00.87: Mode 1 verdict of Virus-Test: True ; Eicar-Test-Signature
 ...
10:39:00.87: Freeing ClamAV message context
```

如果日志文件中不包含类似以上内容的行，或者 clamd 未运行，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 - Error
connecting to ClamAV server
```

14.6.5 ClamAV 选项

ClamAV 选项文件是典型的邮件服务器样式的选项文件，由多个 option=value 格式的行组成。必须设置的一个选项为 HOST。必须将其设置为运行 clamd 的系统的名称。即使 clamd 正在本地主机上运行，也必须设置此选项。

下面列出了可用于此选项文件的更多其他选项。

表 14–7 ClamAV 选项

选项	说明	默认值
DEBUG	从 ClamAV 界面模块启用或禁用调试输出。（clamd 自身的调试输出由 clamd 命令行上的选项控制。）值越大，生成的调试输出越多。0 不生成任何输出。1 提供基本调试。2 增加来自 clamd 的 TCP 通信日志记录。	0

FIELD	指定 ClamAV 结果字符串前缀。通常，ClamAV 结果字符串看起来类似以下条目之一：
	`Virus-Test: False`
	`Virus-Test: True ; Worm.Mydoom.I`
	FIELD 选项提供用于更改结果中 Virus-Test 部分的方法。请注意，如果指定空的 FIELD 值，还将删除 ":"。
		"Virus-Test"

MESSAGE_BUFFER_SIZE	ClamAV 插件必须先在内存中缓冲邮件，然后再将邮件发送到 ClamAV，这是由 clamdscan/clamd 接口的特性所决定的。内存缓冲区大小由此选项控制。默认值为 1,048,576 个字符。长度超过此值的邮件将会被截断，而不会完整地发送到 ClamAV。为了确保完整地扫描每个邮件，此值应反映 MTA 将接受的最大邮件大小。减小此值可能有助于加快病毒扫描速度，但可能会允许未检测的病毒通过。	1048576

表 14–7 ClamAV 选项 （续）

选项	说明	默认值
MODE	控制 ClamAV 结果向结论信息的转换。可以使用四种不同的模式： 0 - 如果发现邮件包含病毒，则返回 VERDICT 选项指定的结论字符串；否则，将返回默认结论。如果 VERDICT 选项为空或未指定，则返回空结论。 1 - 如果发现邮件包含病毒，则返回 ClamAV 结果作为结论；否则，将返回默认结论。 2 - 无条件返回 ClamAV 结果字符串作为结论；不返回默认结论或空结论，并且从不使用 VERDICT 选项。 3 - 如果发现邮件包含病毒，则返回 ClamAV 结果作为结论；否则，将返回由 VERDICT 选项指定的结论字符串。	0
PORT	指定运行 clamd 的端口。	3310
SOCKS_HOST	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 clamd 连接。	3310
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。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。	""
VERDICT	指定模式 0 和 3 中使用的结论字符串。	""

14.7 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 427 页中的 “向垃圾邮件添加包含 SpamAssassin 分数的标题”以及第 428 页中的 “向主题行添加 SpamAssassin 结果字符串”中介绍了 addheader 和 addtag。

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 (ftp://ftp.isi.edu/in-notes/rfc3685.txt) 中介绍了 spamtest。

用来分隔 addtag 的多个主题行标记添加的内部分隔符已经从空格变为竖线。这将可以添加一个包含空格的标记，有些垃圾邮件过滤器需要这样做。例如，以前 addtag "[Probable Spam]" 表示 addtag "[Probable" 和 addtag "spam]"。如今它被视为一个标记，即 "[Probable Spam]"。此更改后将不允许在标记中使用竖线。

使用带有 "i;ascii-numeric" 比较器的 Sieve [RELATIONAL] 扩展，spamtest 可用于将 SpamAssassin 分数与特定值进行比较。SpamAssassin 分数通常为实数，但是 spamtest 首先将分数舍入为最接近的整数，强制此分数为介于 0 和 10 之间的整数值。将小于 0

的值强制增加为 0，大于 10 的值强制缩小为 10。最后，附加由 Messaging Server 维护的文本字符串，以产生 spamtest 测试可以得到的测试字符串。spamtest 支持 :percent（请参见 SIEVE Email Filtering: Spamtest and Virustest Extensions draft-ietf-sieve-spamtestbis-05 (http://www.ietf.org/internet-drafts/draft-ietf-sieve-spamtestbis-05.txt)）。

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"。

允许执行多次 spamadjust 操作；每次操作的结果均将被添加至当前分数。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；但是应列出 spamtest 扩展。

例如，可将 spamadjust 与设置为 2 的 SpamAssassin MODE 结合使用，如下所示：

```
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。

```
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：

```
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"
    {fileinfto "spam-likely";}
else
   {keep;}
```

14.8 使用 Milter

本节包含以下几个部分：第 447 页中的 “14.8 使用 Milter”

14.8.1 Milter 概述

Milter 是 Sendmail Content Management API 的简称。它还表示使用此 API 编写的软件。Milter 为第三方软件提供插件接口，以便在邮件通过 MTA 时验证、修改或阻止邮件。Milter 可以处理邮件的连接 (IP) 信息、信封协议元素、邮件标题和/或邮件正文内容，并且可以修改邮件的收件人、标题和正文。在垃圾邮件拒绝、病毒过滤和内容控制等过程中可能会用到过滤器。通常，Milter 尝试以可伸缩的方式来解决站点范围内的过滤问题。Milter 最初是为 sendmail 设计的，为 sendmail 编写的 Milter 现在可以与 Messaging Server 一起使用，但是会有一些限制（请参见下面的内容）。有关 Milter 的更多信息，请参阅 Internet。

14.8.2 Milter/Messaging Server 操作原理

Milter 控制对邮件执行的操作。Messaging Server 使用第 410 页中的 “14.2.2 指定要过滤的邮件”中所述的方法，控制 Milter 要对哪些邮件执行操作。

在 sendmail 中，Milter 由 sendmail 自身的支持代码和一个单独的 `libmilter` 库组成。过滤器编写者将其过滤器链接到 `libmilter` 以产生一个服务器。然后配置 Sendmail 以使其连接到这些 Milter 服务器。

Messaging Server 提供一个库，可模仿 Milter 接口的 sendmail 端。这使得为 sendmail 编写的 Milter 可以与 Messaging Server 一起使用。

以下是几点注意事项。Milter 协议由文本和二进制元素混合组成，且未妥善记录。另外，Milter 语义与 sendmail 处理邮件的方式紧密联系在一起。尤其是，Milter 可以并且通常会访问 sendmail 配置中所定义的宏的子集。Messaging Server 的 Milter 客户端库尝试提供一个合理的 sendmail 宏集，但完全可以根据当前未实现的 sendmail 配置的特定方面来编写 Milter。最终结果是，从网络获取的任意 Milter 不一定能与此客户端库结合使用。如果问题严重，我们将尝试解决，但不能保证每个 Milter 都会成功。

14.8.3 Milter 要求和使用注意事项

Milter 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 和消息存储之间使用 LMTP，则必须从 MTA 中调用过滤，而不能从消息存储中调用过滤。如果在 MTA 和消息存储之间使用 SMTP，则既可以从 MTA 也可以从消息存储中调用过滤，并且 Milter 服务器可以在上述系统或单独的第三方系统中运行。

Messaging Server 支持连接到多个 Milter 服务器。如果您指定的域名转换为多个 IP 地址，系统将按照从 DNS 接收的顺序尝试所有地址，直到其中一个地址有效为止。某些 DNS 服务器允许按任意顺序返回地址，从而提供了基本的负载平衡/故障转移功能。

14.8.3.1 支持的 Milter 邮件修改操作

Milter 接口当前支持添加标题 (`SMFIF_ADDHDRS`)、更改或删除标题 (`SMFIF_CHGHDRS`) 以及隔离邮件 (`SMFIF_QUARANTINE`) 功能。目前不支持更改邮件正文 (`SMFIF_CHGBODY`)、添加收件人 (`SMFIF_ADDRCPT`) 和删除收件人 (`SMFIF_DELRCPT`) 功能。

14.8.3.2 Milter 接口提供的宏

以下是 Milter 接口当前定义的宏：

`$j` 置于 `Received:` 标题字段 `by` 子句中的文本。在 Messaging Server 中，此宏由 MTA 选项 `RECEIVED_DOMAIN` 控制。如果未设置此选项，则使用 `local` 通道上的正式主机。

`${client_addr}` SMTP 客户端的 IP 地址，使用以点分隔的四组数值表示。仅在通过 TCP 使用 SMTP 时设置。

`$i` 当前邮件的队列 ID。Messaging Server 为每个会话生成一个唯一 ID；此 ID 即为 `$i` 宏中显示的内容。

`${mail_addr}` 当前事务的 `MAIL FROM` 地址。

`${mail_host}` 当前事务的 `MAIL FROM` 地址的主机部分。

`${rcpt_addr}` 当前事务的 `RCPT TO` 地址。

`${rcpt_host}` 当前 `RCPT TO` 地址的主机部分。

▼ 部署 Milter

可执行以下步骤来部署 Milter：

1. **获取并配置将执行所需操作的 Milter。**
   有关获取和配置信息，请参阅具体的 Milter 文档。

2 **装入并配置 Milter 客户端库。（请参见第 409 页中的“ 14.2.1 装入和配置垃圾邮件过滤软件客户端库 ”。）**

a. **指定客户端库的路径 `libmilter.so`。指定 Milter 配置文件的路径和名称。**

示例：

```
spamfilter1_library=/opt/SUNWmsgsr/lib/libmilter.so
spamfilterX_config_file=/opt/SUNWmsgsr/lib/milter.opt
```

b. **使用所需的选项创建 Milter 配置文件。**

Milter 选项文件由多个 `option=value` 格式的行组成。必须设置的两个选项为 `HOST` 和 `PORT`。`HOST` 必须设置为运行 Milter 服务器的系统的名称，而 `PORT` 必须设置为配置 Milter 服务器侦听的端口。请注意，仅支持 TCP/IP 连接；不能指定或使用 UNIX 域套接字。

此选项文件中还有几个其他选项：

`DEBUG`（整数，默认值为 0）— 启用或禁用 Milter 客户端库的调试输出。值越大，生成的调试输出越多。0 不生成任何输出。1 提供基本调试。2 增加了 TCP 通信的日志记录。（Milter 服务器的调试输出通常由命令行上用于启动服务器的设置控制。请注意，大部分 Milter 似乎只提供将调试输出直接传送到系统日志的功能。）

`TIMEOUT`（整数，默认值为 3600）— 指定与 Milter 连接有关的操作的超时时间（以百分之一秒为单位）。此选项适用于 6.3 和更高版本。

`SOCKS_HOST`（字符串，默认值为 ""）— 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 Milter 连接。

`SOCKS_PORT`（整数，默认值为 1080）— 指定运行中间 SOCKS 服务器的端口。

`SOCKS_PASSWORD`（字符串，默认值为 ""）— 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，默认值为 ""）— 指定通过 SOCKS 服务器建立连接所使用的用户名。

3 **指定发送到 Milter 的邮件。**

用户、域或通道均可以过滤邮件。请参见第 410 页中的 “14.2.2 指定要过滤的邮件”。

4 **在 `option.dat` 文件中设置 `spamfilter`*X*`_string_action` 选项：**

`spamfilter`*X*`_string_action=data:,$M`

此设置可以无条件使用，但只有在 Milter 的 MTA 选项文件中才能正常工作。

14.9 其他反垃圾邮件和拒绝服务技术

减少垃圾邮件和病毒进入用户邮箱最有效的方式是向系统添加垃圾邮件和病毒过滤软件。但是，Messaging Server 提供了许多其他技术和方法支持垃圾邮件过滤。通常，这些技术并非只用于垃圾邮件过滤，因此对这些技术的介绍贯穿了全书。以下列出介绍反垃圾邮件和拒绝服务技术的部分。

反垃圾邮件技术：

- 第 450 页中的 “14.9.1 反垃圾邮件技术： 延迟发送 SMTP 标题”
- 第 370 页中的 “12.12.6 地址验证之后扩展之前的路由”
- 第 15 章
- 第 18 章
- 第 655 页中的 “23.7 配置客户端对 POP、IMAP 和 HTTP 服务的访问”
- 第 323 页中的 “12.4.2.6 DNS 域验证”
- 第 342 页中的 “12.5.9 多个地址扩展”
- 第 508 页中的 “18.14 创建 MTA 范围内的过滤器”
- 第 497 页中的 “18.7 配置 SMTP 中继阻止”

拒绝服务技术：

- 第 19 章
- 第 361 页中的 “12.9.2 指定绝对邮件大小限制”
- 第 493 页中的 “18.3.6 限制指定 IP 地址到 MTA 的连接”
- 第 776 页中的 “27.4.1 监视邮件队列的大小”
- 第 777 页中的 “27.4.3 监视入站 SMTP 连接”

14.9.1 反垃圾邮件技术： 延迟发送 SMTP 标题

一个有用的反垃圾邮件策略是，将发送 SMTP 标题的时间向后稍做延迟（如延迟半秒钟），然后清除输入缓冲区，最后发送标题。这样做能起作用是因为，许多垃圾邮件客户端都是与标准不兼容的，它们只要一打开连接就发出大量 SMTP 命令，而忽略服务器发出的任何响应。当启用此功能时，这样做的垃圾邮件客户端将丢失 SMTP 对话中的前几个命令，从而使对话的其余部分无效。

现在已经在 Messaging Server 中实现了此功能。可以无条件地启用此功能，只需在清除和发送标题前将 `BANNER_PURGE_DELAY` SMTP 通道选项设置为要延迟的秒数。值为 0 将禁用延迟和清除。

也可以使用 `PORT_ACCESS` 映射控制此功能。在模板中指定 `$D` 将导致从模板结果的强制性 SMTP `auth rulset` 和领域之后再读取一个参数，并添加可选的应用程序信息。该值必须是一个语义与 `BANNER_PURGE_DELAY` 值相同的整数。请注意，任何 `PORT_ACCESS` 映射设置都将覆盖 `BANNER_PURGE_DELAY` SMTP 通道选项。

◆ ◆ ◆ 第 15 章

15 使用发件人策略框架处理伪造的电子邮件

垃圾邮件制造者和电子邮件诈骗者经常使用假域名和电子邮件地址（或者合法域名和电子邮件地址）伪造电子邮件来欺骗用户，使他们认为邮件来自他们熟悉的个人或公司。例如，垃圾邮件制造者可能发送来自 president@whitehouse.gov 等地址的邮件，用户可能会误认为该邮件确实来自此地址。伪造电子邮件可能会欺骗用户打开未经许可的邮件，甚至向某个假的授权机构提供信息。另外，垃圾邮件制造者喜欢从不在 RBL 列表上的合法域发送电子邮件。

发件人策略框架 (Sender Policy Framework, SPF) 是一种可以在 SMTP 对话期间检测和拒绝伪造电子邮件的技术。具体地说，SPF 是一种协议，可以允许某个域明确地授权可以使用其域名的主机。此外，可能还要配置接收主机检查此授权。这样，SPF 可以显著减少出现伪造电子邮件的情况。

15.1 操作原理

当邮件传入 Messaging Server 时，MTA 将进行 SPF 查询以确定地址是否确实来自该地址上的域。SPF 查询查阅 DNS 中属于此邮件的域的 TXT 记录 (*domain*)。 *domain* 可以是作为 HELO 或 EHLO 参数指定的域名（如果使用了 `spfhelo` 通道关键字），也可以是在 MAIL FROM: 命令中给出的邮件始发者地址中的域名（通常是 `@` 字符之后的部分）。如果没有指定的或可用的域名，则在 HELO/EHLO 期间指定的那个域名将被用作 *domain*。请注意，大部分 ISP 会发布一个与其域匹配的授权 IP 地址列表。如果 IP 地址与域名不匹配，则邮件将被认为是伪造的。

注 – 在查询 DNS 之前，我们会先检查 SPF_LOCAL 映射表中是否存在匹配的域。如果在表中找到匹配的域，则首先使用此域。

如果在映射表中找到的记录包含 `redirect =` *domain* 子句，则会通过 DNS 查询重定向到域，而跳过递归和冗余的映射文件检查。

生成的 TXT 记录示例：

```
v=spf1 +mx a:colo.siroe.com/28 -all
```

对于此 RFC 支持的 SPF 记录而言，`v=spf1` 令牌是必须的。

`+mx` 指示我们检查 *domain* 的 MX 记录，并确认此 SMTP 连接的源 IP 地址与作为 *domain* MX 查询结果给出的 IP 地址之一匹配。如果存在匹配项，则 `+` 表示此操作的结果为 `Pass`。

`a:colo.siroe.com/28` 指示我们检查 `colo.siroe.com` 的 A 记录，然后确认此 SMTP 连接的源 IP 地址与 A 记录位于同一指定的 CIDR 子网，只比较 28 位（掩码 255.255.255.240）。未指定限定字符，因此使用默认值 `+`，表示匹配导致 `Pass`。

最后，`-all` 与任何其他项匹配，并导致 `Fail`。有关 SPF 记录更完整的介绍，请参阅 `http://www.ietf.org/rfc/rfc4408.txt` 上的 RFC 4408。

SPF 处理可以得到以下结果之一。下表显示了结果及其说明。

表 15–1 SPF 处理结果

结果	说明
`Pass`	查找已通过，表示找到了 SPF 记录，并且该记录验证了始发系统有权使用 *domain*。
`Fail`	查找找到了匹配的 SPF 记录，但是，该记录明确地拒绝向 SMTP 客户端授予在 SMTP 事务期间使用 *domain* 的权限。我们 SPF 实现的默认行为是使用 5xx 回复拒绝 SMTP 命令。
`SoftFail`	查找找到了匹配的 SPF 记录并且该记录也拒绝为 SMTP 客户端授权使用 *domain*，但是，拒绝不是很严格且记录不会指向彻底失败。我们实现的默认行为是接受邮件，但是在 Received-SPF: 标题中注明 `SoftFail`，以进行后续评测，如 Sieve 处理。
`Neutral`	SPF 记录未声明授权 SMTP 客户端使用 *domain*。邮件将被接受。规范要求 `Neutral` 与下面的 `None` 处理方法一样。
`None`	未找到匹配 SPF 记录，因此不进行任何 SPF 处理。

表 15–1 SPF 处理结果 （续）

结果	说明
PermError	在 SPF 处理中遇到永久错误，例如 SPF 记录中的语法错误、处理嵌套 SPF 记录时发生 DNS 故障（由于 include: 机制或 redirect= 修饰符所致），或处理嵌套 SPF 记录时超过为 SPF 处理配置的限制。默认行为是使用 5xx 回复拒绝 SMTP 命令。
TempError	在 SPF 处理中遇到临时错误，很可能是由于查询 SPF 记录时 DNS 超时。默认行为是使用 4xx 回复拒绝 SMTP 命令。

在 SPF 处理完成后，Received-SPF: 标题将被写入记录 SPF 处理结果的邮件。然后，可以在 Sieve 处理期间查询此标题以做进一步考虑。如果启用 option.dat 文件中的 MTA 选项 MM_DEBUG (>0)，则可以使用全面的调试。

15.2 局限性

SPF 仅仅是一种用于对抗垃圾邮件的工具，并不会解决所有问题。垃圾邮件制造者可以很容易地创建域，并添加 SPF TXT 记录而使该域看起来是合法的。另一方面，SPF 只对检测自己建立的 ISP 的伪造邮件很有效，尽管很多 TXT 记录使 SPF 看起来不会失败。

15.3 预部署注意事项

由于需要对每个邮件进行 DNS 查询，因此系统中有一个非常快的 DNS 服务器很重要。

15.4 设置该技术

设置 SPF 技术分为两步：

- 将通道关键字置于外来的 TCP 通道（通常是 tcp_local 通道，但如果允许从 tcp_local 切换到另一个通道，也可能存在其他通道）。请参见表 15–2。
- 在 option.dat 文件中设置选项。请参见表 15–3。

15.5 参考信息

本节提供有关 SPF 通道关键字和 SPF MTA 选项的参考信息。SPF 支持是通过应用于外来 tcp_* 通道（通常是 tcp_local）的四个通道关键字实现的。下表显示了这些关键字及其说明。

表 15–2 SPF 关键字

关键字	说明
spfnone	禁用 SPF 处理
spfhelo	为作为 HELO 或 EHLO 参数指定的域名启用 SPF 处理。
spfmailfrom	为收到 MAIL FROM: 后提供给始发者信封地址的域名启用 SPF 处理.
spfrcptto	为收到 RCPT TO: 后提供给始发者信封地址的域名启用 SPF 处理. 处理方式与 spfmailfrom 一样，只是它在 SMTP 事务中被延迟，直到发出 RCPT TO: 命令并且收件人被确认为有效收件人后为止。

注 – spfmailfrom 和 spfrcptto 关键字会发生冲突，应该只在通道上指定其中一个关键字。但是，可以同时使用 spfhelo 和 spfmailfrom（或 spfrcptto）以执行两种 SPF 检查。

还支持建立对 SPF 处理的限制，并可以针对各种 SPF 结果，控制是接受 SMTP 命令，还是以 4xx 响应（临时故障）或 5xx 响应（永久故障）拒绝该命令，这些 SPF 结果包括：Fail、SoftFail、PermError 和 TempError。

option.dat 中的以下 MTA 选项可以用于对 SPF 处理进行限制。

表 15–3 SPF限制选项

选项	说明
SPF_MAX_RECURSION	指定由于 include: 或 redirect= 而导致的嵌套 SPF 记录中允许的递归数。超过此限制将导致 PermError。 默认值：10（由 RFC 规定）
SPF_MAX_DNS_QUERIES	指定需要 DNS 查找的机制数或修饰符数（包括 include:、a:、mx:、ptr:、exists:、redirect= 和 exp=）。请注意，此限制不会计为实际 DNS 查找的数量，因此一个机制可能会导致多个 DNS 查询。超过此限制将导致 PermError。 默认值：10（由 RFC 规定）

表 15–3 SPF限制选项 （续）

选项	说明
SPF_MAX_TIME	指定完成 SPF 处理允许的时间（以秒为单位）。超过此值将导致 TempError。默认值远大于 RFC 建议的值。 默认值：45

另外，可以配置 option.dat 中的以下 MTA 选项，以控制 SMTP 服务器在响应Fail、SoftFail、PermError 和 TempError 的 SPF 结果时所采取的行为。对于每种结果，SMTP 服务器都可发回 2xx（成功）、4xx（临时故障）或 5xx（永久故障）响应。另外，对于 Fail 和 SoftFail，MTA 能够区分 "all" 机制导致的 SPF 结果和明确引用的匹配。这样您可以区分特定结果和 SPF 记录的默认结果。上述任一选项的有效值是 2、4 或 5。值 2、4 和 5 分别对应来自 SMTP 服务器的 2xx、4xx 和 5xx 响应，这些响应是获取特定 SPF 状态的结果。因此，如果 SPF_SMTP_STATUS_FAIL=2 并且 SPF 记录明确地用 "-a:192.168.1.44"（我们的 IP 地址）阻塞我们，那么我们将使用 "250 OK" 接受该地址，而不是使用 5xx 进行响应。

表 15–4 SPF故障和错误选项

选项	说明
SPF_SMTP_STATUS_FAIL	当 SPF 记录的匹配是 "-" 标志的机制（"-all" 除外）时使用 默认值：5
SPF_SMTP_STATUS_FAIL_ALL	当匹配机制为 "-all" 时使用 默认值：5
SPF_SMTP_STATUS_SOFTFAIL	当 SPF 记录的匹配是 "~" 标志的机制（"~all" 除外）时使用 默认值：2
SPF_SMTP_STATUS_SOFTFAIL_ALL	当匹配机制为 "~all" 时使用 默认值：2
SPF_SMTP_STATUS_TEMPERROR	当有临时故障（通常与 DNS 处理问题有关）时使用。 默认值：4
SPF_SMTP_STATUS_PERMERROR	当有永久故障（通常由于语法或其他 SPF 处理期间发现的技术错误所致）时使用。（请注意，这将由非本地错误引发。） 默认值：5

15.6 使用 spfquery 测试 SPF

此测试实用程序可用于测试 SPF 处理。

注 – `spfquery` 不测试您的 SPF 配置。而测试启用 SPF 处理时会返回什么。

要求：必须作为有权运行 Messaging Server 二进制文件和访问其库的用户运行，例如，超级用户或 `mailsrv` 用户。

位置：*msg-svr-base*/sbin/

15.6.1 语法

```
spfquery [-i ip-address] [-s sender-email] [-h helo-domain]
  [-e none | neutral | pass | fail | temperror | permerror] [-v] [-V] [?] domain
```

下表显示了 `spfquery` 选项及其说明。

表 15–5 spfquery 选项

选项	说明
`-i` *ip address*	指定作为 SPF 查询远程地址使用的 IP 地址。默认值为 `127.0.0.1`。此选项也可以是 `--ip-address`。
`-s` *domain*	要使用的电子邮件地址，就像 `MAIL FROM:` 指定的一样。默认值：postmaster@*domain*。此选项也可以是 `--sender`。
`-h` *helo-domain*	域名，就像为 HELO 域指定的一样。请注意，此域自身不会受到验证，而是作为宏处理的补充信息。默认值与为 *domain* 指定的值相同。此选项也可以是 `--helo-domain`。
`-e` *result*	`spfquery` 将会比较 SPF 处理的结果与预期的结果，如果两个结果不同，将会打印一封邮件并以非零返回状态退出 `spfquery`；可能出现以下任一结果：`none`、`neutral`、`pass`、`fail`、`softfail`、`temperror` 或 `permerror`。此选项还可以是 `--expect`。
`-v`	在 SPF 处理期间，启用详细输出。此选项还可以是 `--verbose`。
`-V`	打印当前版本的 SPF 库。此选项还可以是 `--version`。
`-?`	打印此用法信息。此选项还可以是 `--help`。

15.6.2 启用了调试的示例

```
# /opt/SUNWmsgsr/sbin/spfquery -v -i 192.168.1.3 11.spf1-test.siroe.com
    Running SPF query with:
      IP address: 192.168.1.3
          Domain: 11.spf1-test.siroe.com
          Sender: postmaster@11.spf1-test.siroe.com (local-part: postmaster)
     HELO Domain: 11.spf1-test.siroe.com

    15:30:04.33: ----------------------------------------------------------------
    15:30:04.33: SPFcheck_host called:
    15:30:04.33:       source ip = 192.168.1.3
    15:30:04.33:          domain = 11.spf1-test.siroe.com
    15:30:04.33:          sender = postmaster@11.spf1-test.siroe.com
    15:30:04.33:      local_part = postmaster
    15:30:04.33:     helo_domain = 11.spf1-test.siroe.com
    15:30:04.33:
    15:30:04.33:   Looking up "v=spf1" records for 11.spf1-test.siroe.com
    15:30:04.35:     DNS query status: Pass
    15:30:04.35:       "v=spf1 mx:spf1-test.siroe.com                  -all"
    15:30:04.35:
    15:30:04.35:   Parsing mechanism: " mx : spf1-test.siroe.com"
    15:30:04.35:     Assuming a Pass prefix
    15:30:04.35:     Processing macros in spf1-test.siroe.com
    15:30:04.35:     Comparing against 192.168.1.3
    15:30:04.35:     Looking for MX records for spf1-test.siroe.com
    15:30:04.41:       mx02.spf1-test.siroe.com:
    15:30:04.41:         192.0.2.22 - No match
    15:30:04.41:         192.0.2.21 - No match
    15:30:04.41:         192.0.2.20 - No match
    15:30:04.41:         192.0.2.23 - No match
    15:30:04.41:       mx01.spf1-test.siroe.com:
    15:30:04.42:         192.0.2.13 - No match
    15:30:04.42:         192.0.2.11 - No match
    15:30:04.42:         192.0.2.12 - No match
    15:30:04.42:         192.0.2.10 - No match
    15:30:04.42:       mx03.spf1-test.siroe.com:
    15:30:04.42:         192.0.2.32 - No match
    15:30:04.42:         192.0.2.30 - No match
    15:30:04.42:         192.0.2.31 - No match
    15:30:04.42:         192.168.1.3 - Matched
    15:30:04.42:   Mechanism matched; returning Pass
    15:30:04.42:
    15:30:04.42:   Parsing mechanism: "- all : " (not evaluated)
    15:30:04.42:
    15:30:04.42: SPFcheck_host is returning Pass
    15:30:04.42: ----------------------------------------------------------------
```

15.7 在 SPF 中使用发件人重写方案 (Sender Rewriting Scheme, SRS) 处理转发邮件

如上所述，SPF 是一种尝试通过查找特定的 TXT 记录来防止电子邮件伪造的机制，这些 TXT 记录与邮件 FROM:（信封 from）地址中的域关联。此操作实际上包括几个 DNS 查找操作，最终可生成一个 IP 地址列表，这些地址被授权发送来自域的邮件。将根据此列表检查 SMTP 客户端的 IP 地址，如果没有找到该地址，则邮件可能被认为是伪造邮件。Messaging Server 6.3 版实现了 SPF 支持。

SPF 使提供邮件转发服务的站点面临严重的问题，例如大学站点（为其毕业生转发）或专业机构站点（为其成员转发）。转发者将发出来自任意发件人的邮件，这些发件人可能包括已经实现 SPF 策略的发件人，当然还包括没有列出转发系统（或可以使用其域的地址的系统）IP 地址的发件人。

发件人重写方案（或 SRS）提供了此问题的解决方案。SRS 使用转发者自己的域将原始发件人的地址封装在一个新地址中，从而解决了该问题。转发者自己的域仅在进行 SPF 检查时公开。使用地址时会将邮件（通常是通知）路由给转发者，这样可删除地址封装并将邮件发送到真正的目的地。

当然，地址封装并非全新的技术。与 percent hack 路由和 bang 路径一样，源路由是在 RFC 822 中定义的，并正好提供了此类功能。但是，在目前的 Internet 中，这些机制都存在问题，因为允许使用它们实际上是将您的系统变成了一个开放的中继。

SRS 通过向封装格式添加一个加密的散列函数和一个时间戳来处理此问题。地址只在某个时间段是有效的，过了这段时间就不能再使用了。散列函数防止修改时间戳或封装的地址。

SRS 还提供一个机制处理多次转发，而不会使地址长度过度增长。要使该方案生效，必须在所有实现 SRS 的系统中以相同的方式对 SRS 地址的某些方面进行格式化。

现在在 6.3P1 版本中已经实现了 SRS 支持。添加了以下 MTA 选项：

- SRS_DOMAIN。必须向要在 SRS 地址中使用的域设置此选项。发送到该域的电子邮件必须始终路由到能对该域进行 SRS 操作的系统。SRS 处理将覆盖常规地址处理，因此站点必定能够使用其主域作为 SRS 域。
- SRS_SECRETS。这是一个以逗号分隔的密钥列表，这些密钥用于编码和解码 SRS 地址。列表中的第一个密钥必定用于编码。解码时，将按顺序尝试每个密钥，以生成不同的散列值。如果有匹配的散列值，则解码操作将继续进行。

  由于能够使用多个密钥，因此可以在不中断服务的情况下更改密匙：添加第二个密钥，等待所有以前发出的地址超时，然后删除第一个密钥。
- SRS_MAXAGE。（可选）指定邮件超时前的天数。如果未指定该选项，则默认值为 14 天。

  必须配置为选定 SRS 域处理电子邮件的每个系统，以进行 SRS 处理，并且三个 SRS 选项的设置必须一致。

设置这些选项后，即可启用 SRS 地址解码。编码则有所不同，应仅对您已知与转发活动关联的信封 From: 地址进行编码。SRS 编码由以下六个新的通道关键字控制：addresssrs、noaddresssrs、destinationsrs、nodestinationsrs、sourcesrs 和 nosourcesrs。

要进行 SRS 编码，必须符合以下三个条件：

(1) 当前源通道必须用 sourcesrs 标记（nosourcesrs 是默认设置）。

(2) 当前目标通道必须用 destinationsrs 标记（nodestinationsrs 是默认设置）。

(3) 当前地址在重写时必须匹配标记为 addresssrs 的通道（ noaddress 是默认设置）。

只有在符合以上所有条件时才能进行编码。最简单的设置是纯转发操作的设置，其中所有的邮件都从 tcp_local 通道进入或发出，并且所有的非本地地址都需要进行 SRS 处理。在这样的设置中，tcp_local 将使用 sourcesrs、destinationsrs 和 addresssrs 这三个关键字进行标记。

最后，imsimta test -rewrite 得到了增强，可以显示 SRS 编码和解码的结果，而不管输入的地址是什么。 例如，地址 foo@example.com 可能生成类似以下的输出：

```
SRS encoding = SRS0=dnG=IS=example.com=foo@example.org
```

如果重写此编码的地址，则生成的输出为：

```
SRS decoding = foo@example.com
```

imsimta test -rewrite 还会显示 SRS 解码期间出现的所有错误。

◆ ◆ ◆ 第 16 章

16 LMTP 传送

Sun Java System Messaging Server MTA 可以在使用多层邮件服务器部署的情况下使用 LMTP（Local Mail Transfer Protocol，本地邮件传输协议）（在 RFC 2033 中定义）将邮件传送到消息存储。在这些情况下，您使用入站中继和后端消息存储时，中继将负责地址扩展和传送方法（例如自动回复和转发），还负责邮件列表扩展。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 服务器并非旨在作为一般用途的 LMTP 服务器，而是用作中继和后端消息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 已实现的 LMTP 服务不适用于与其他 LMTP 服务器或其他 LMTP 客户端结合使用。

本章包含以下几个部分：

16.1 LMTP 传送功能

MTA 的 LMTP 服务器能更有效地将邮件传送到后端消息存储，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服务部署中的一个限制因素。

- 减少邮件队列的数目。

  对于邮件服务部署的管理员来说，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。

16.2 不使用 LMTP 的两层部署中的邮件服务处理

图 16–1 以图解形式显示了不使用 LMTP 的两层部署方案中邮件处理的以下说明。

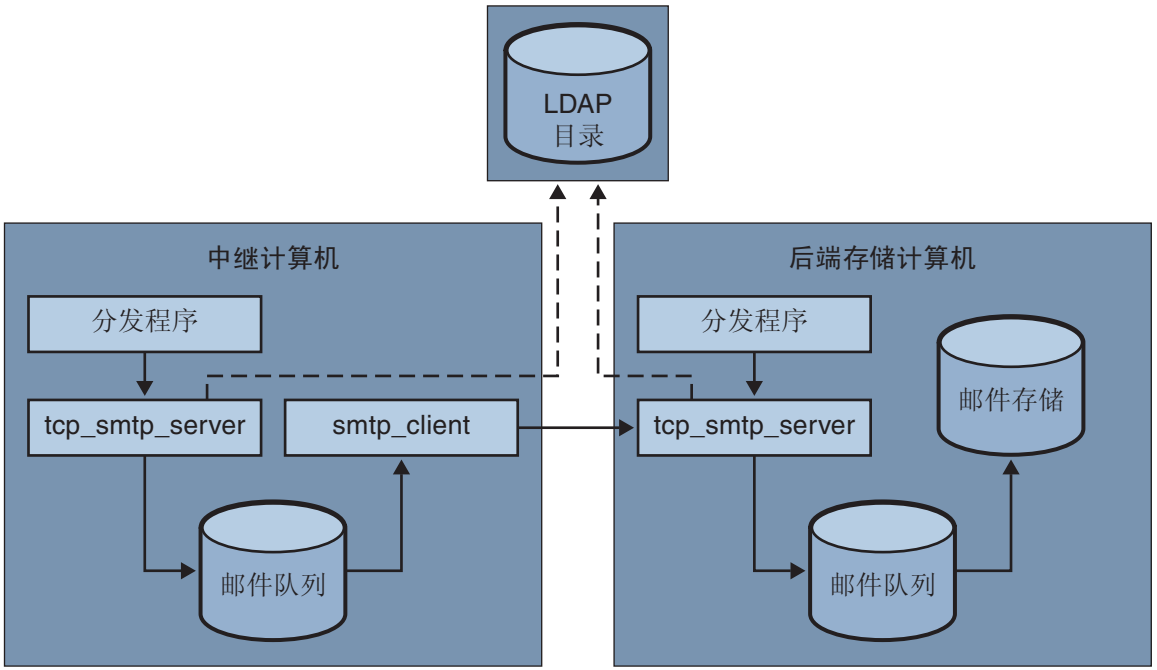


图 16–1 不使用 LMTP 的两层部署

不使用 LMTP 的情况下，在存储系统前面带有中继的两层部署中，入站邮件的处理从 SMTP 端口上的连接开始，该连接由中继计算机上的分发程序选取并传递到 `tcp_smtp_server` 进程。此进程对入站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`
- 将邮件加入队列以传送到邮件主机

`smtp_client` 进程从队列中选取邮件并将其发送至邮件主机。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至 `ims_ms` 通道
- 将邮件加入队列以传送到存储

然后 `ims_ms` 进程选取邮件并尝试将其传送至存储。在此方案中，执行了两次加入队列处理，并且每个 MTA 均执行一次 LDAP 查找。

16.3 使用 LMTP 的两层部署中的邮件服务处理

第 463 页中的 “16.3 使用 LMTP 的两层部署中的邮件服务处理”以图解形式显示了使用 LMTP 的两层部署方案中邮件处理的以下说明。

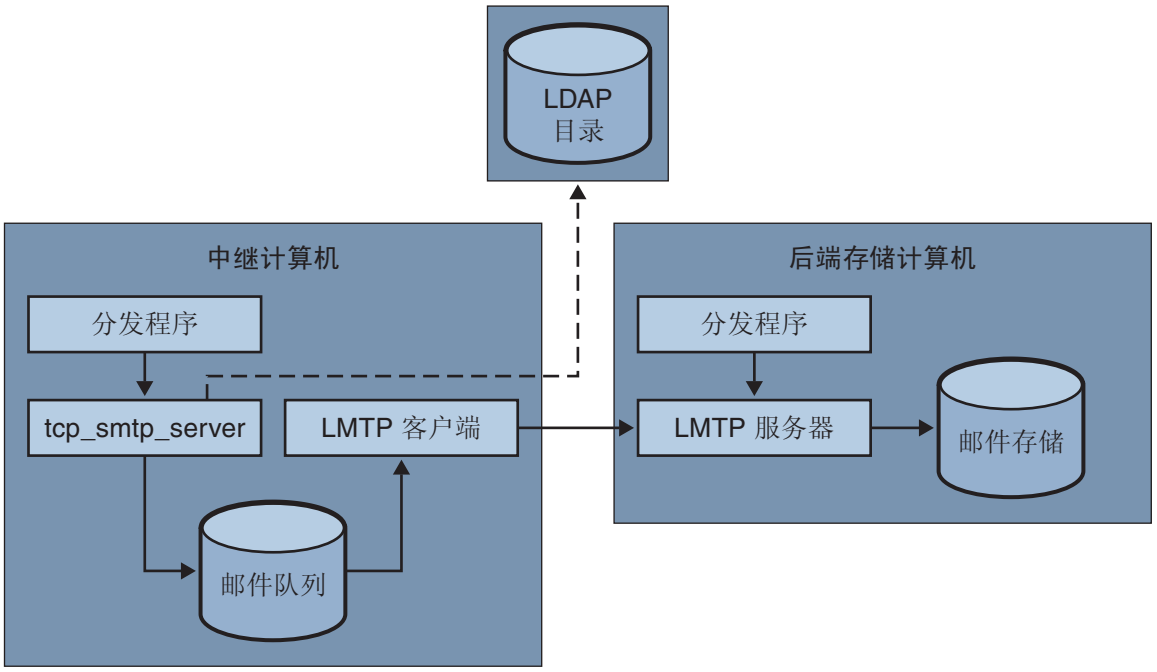


图 16–2 使用 LMTP 的两层部署

在 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。此进程对入站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消息存储计算机
- 将邮件加入队列以传送到邮件主机

在存储计算机上，分发程序将接收与 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，消息存储上的 LMTP 进程不使用任何 MTA 机制以用于处理地址或邮件。

16.4 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 加入队列或取消排队功能、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消息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他收件人信息（例如用户的配额）将与收件人地址一起显示为 LMTP 参数。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。

16.5 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消息存储计算机中。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 传送的消息存储，可以实现此目的。

▼ 配置与 LMTP 配合使用的入站 MTA 中继

要配置入站 MTA 中继以使用 LMTP，请执行以下操作：

1 修改 imta.cnf 文件并更改 LMTP 重写规则，使之如下所示：

```
! lmtp
.lmtp   $E$F$U%$H.lmtp@lmtpcs-daemon
.lmtp   $B$F$U%$H@$H@lmtpcs-daemon
!
```

```
! lmtp native
.lmtpn  $E$F$U%$H.lmtpn@lmtpcn-daemon
.lmtpn  $B$F$U%$H@$H@lmtpcn-daemon
!
```

2 **将邮箱 DELIVERY_OPTIONS 设置为：**

```
#*mailbox=@$X.LMTP:$M%$\$2I$_+$2S@lmtpcs-daemon
```

3 **将本机 DELIVERY_OPTIONS 子句设置为：**

```
#*native=@$X.LMTPN:$M+$2S@native-daemon
```

4 **为每个 tcp_lmtp* 通道块添加通道关键字 multigate connectcanonical 。**

5 **为 tcp_lmtpcs 通道添加以下通道关键字：**

```
fileinto @$4O:$U+$S@$D
```

请注意，以上关键字中的 "O" 为大写字母 O，而不是数字零。

6 **外来 MTA 中继的配置设置应该如下所示：**

DELIVERY_OPTIONS 的 option.dat 条目应该如下所示：

```
!-----------------------------------------
! Modified DELIVERY_OPTIONS to activate LMTP
! delivery from a frontend to the backend store
!-----------------------------------------
!
DELIVERY_OPTIONS=\
    #*mailbox=@$X.LMTP:$M%$\$2I$_+$2S@lmtpcs-daemon,\
    #&members=*,\
    #*native=@$X.LMTPN:$M+$2S@native-daemon,\
    #*unix=@$X.LMTPN:$M,\
    #*file=@$X.LMTPN:+$F,\
    #&@members_offline=*,\
    #/hold=@hold-daemon:$A,\
    #program=$M%$P@pipe-daemon,\
    #forward=**,\
    #*^!autoreply=$M+$D@bitbucket
!
```

完成更改之后，已修改的 imta.cnf 重写规则应该如下所示：

```
! lmtp
.lmtp   $E$F$U%$H.lmtp@lmtpcs-daemon
.lmtp   $B$F$U%$H@$H@lmtpcs-daemon
!
! lmtp native
.lmtpn  $E$F$U%$H.lmtpn@lmtpcn-daemon
```

```
.lmtpn  $B$F$U%$H@$H@lmtpcn-daemon
!
```

更改的通道块应该如下所示：

```
!
! tcp_lmtpcs (LMTP client - store)
tcp_lmtpcs defragment lmtp  multigate connectcanonical \
   fileinto @$4O:$U+$S@$D port 225 nodns single_sys \
   subdirs 20 maxjobs 7 pool SMTP_POOL dequeue_removeroute
lmtpcs-daemon

!
! tcp_lmtpcn (LMTP client - native)
tcp_lmtpcn defragment lmtp multigate connectcanonical port 226 \
   nodns single_sys subdirs 20 maxjobs 7 pool SMTP_POOL \
   dequeue_removeroute
lmtpcn-daemon
```

16.5.1 配置具有 LMTP 和一个最小 MTA 的后端存储

如果后端存储要通过 LMTP 接收邮件，则它们只需要一个最小的 MTA。需要一个分发程序、一个作业控制器和简单的 MTA 配置。特别是需要 `dispatcher.cnf`、`job_controller.cnf` 和 `mappings` 文件，这些文件构成 MAT 配置的唯一重要部分。

`dispatcher.cnf` 文件必须包含以下内容：

```
! VERSION=1.1
! IMTA default dispatcher configuration file
!
! Global defaults
!
MIN_PROCS=1
MAX_PROCS=10
MIN_CONNS=30
MAX_CONNS=50
MAX_SHUTDOWN=2
MAX_LIFE_TIME=86400
MAX_LIFE_CONNS=10000
MAX_IDLE_TIME=600
HISTORICAL_TIME=0
!
! 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
```

请注意，默认情况下，`dispatcher.cnf` 文件中的 LMTP 服务均已被注释。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|192.18.74.206|* $Y
  TCP|*|226|192.18.74.206|* $Y
  TCP|*|225|192.18.74.129|* $Y
  TCP|*|226|192.18.74.129|* $Y
  TCP|*|*|*|*   $N500$ Do$ not$ connect$ to$ this$ machine
```

以上 IP 地址是 LMTP 服务器和客户端的 IP 地址。您应该用连接到后端存储的网络中的中继 IP 地址替换此处在 `PORT_ACCESS` 映射表中指定的示例 IP 地址。

必须有一个 `imta.cnf` 文件，但是它只用于完成配置。最小的 `imta.cnf` 文件由以下通道定义组成：

```
!
! IMTA configuration file
!
! 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 通道定义已被注释掉。如果需要 LMTP 工作，必须取消其注释。

您可以使用安装时创建的默认 `job_controller.cnf` 文件。不需要修改此文件。

16.5.2 配置中继以通过 LMTP 将邮件发送到带有消息存储和完整 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 465 页中的 “配置与 LMTP 配合使用的入站 MTA 中继”中的说明进行配置。

16.5.3 在具有完整 MTA 的后端消息存储系统中配置 LMTP

从后端存储邮件服务系统的配置到使用 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` 文件的结尾：

```
! 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 服务均已被注释。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。

这与上述用于仅为 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，正如 LMTP 需要后端存储一样。

16.5.4 处理响应 LMTP 邮件数据时的 4.2.1 邮箱忙错误

如果 LMTP 通道选项 MAILBOX_BUSY_FAST_RETRY 被设置为 1（默认值），将通过以下方式处理响应 LMTP 邮件数据时的 4.2.1 邮箱忙错误：在很短的随机时间间隔后重试邮件；不应用正常邮件的 backoff 值。将该选项设置为 0 可禁用此行为。

16.6 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 客户端使用标准的 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 中的消息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。此信息用于使消息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。我们不支持使用此扩展的其他客户端与我方服务器结合使用，也不支持将我方客户端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 客户端发送整个邮件（充满点的），类似于 SMTP 执行的操作。完成邮件传送后，每行上将带有一个点 (.)。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 服务器会将每个收件人（在 RCPT TO: 行中给定）的状态发送回 LMTP 客户端。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。

对话可以使用另一个 MAIL FROM: 行重复，或使用以下交互式操作结束：

```
---> quit
<--- 221 OK
```

表 16–1 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 16–1 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

表 16–1 收件人的 LMTP 状态代码 （续）

短代码	长代码	状态文本
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 17 章

17 休假自动邮件回复

对于自动生成的电子邮件回复（自动回复），尤其是休假邮件，MTA 使用邮件处理通知 (Message Disposition Notification, *MDN*) 和 Sieve 脚本语言。MDN 是由 MTA 发送给发件人和/或邮寄主管以报告有关邮件传送处理情况的电子邮件。MDN 也称为已读回执、确认、回执通知或发送收据。Sieve 是用于创建邮件过滤器的简单脚本撰写语言。与 Messaging Server 5.x 不同，Sieve 使用的字符集为 UTF-8，而不是 ISO-2022-JP。

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消息存储上完成休假处理的情况除外。

本章包含以下几个部分：

17.1 休假自动回复概述

休假 Sieve 脚本可通过各种 LDAP 休假属性自动生成（请参见第 477 页中的 “17.4 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。

注 – 休假邮件的字符集已更改为 UTF-8。

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。

17.2 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 option.dat 文件中定义的 MTA 选项 DELIVERY_OPTIONS 所定义。option.dat 文件的 DELIVERY_OPTIONS 中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，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 属性创建休假 Sieve 脚本。自动回复规则可以包含前缀字符 "!"、","、"#"、"^" 和 "*"。

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，这样可以通过单独的传送选项启用自动回复机制，以便可由 "^" 标志进一步限制。检查此阶段的日期比使用 Sieve 逻辑更有效。

表 17–1 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 17–1 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。
@	从各个邮件标题字段以及与信封 From: 地址关联的 LDAP 条目中提取首选语言信息。要该信息在适当的时候可用，进行自动回复时该信息必须经过 reprocess 通道。这通过将 @ 标记添加到 autoreply 传送选项实现。请注意，添加通道中继会增加邮件处理的系统开销。

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。

17.2.1 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可在为用户提供服务的邮件服务器上生成自动回复。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，并在 DELIVERY_OPTIONS 中将字符 # 放置在自动回复规则之前。

1 **使用 an 编辑器打开 option.dat 文件。**

2 **添加或更改 DELIVERY_OPTIONS 选项，以使现有的自动回复规则类似于：**

```
#*^!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。有关以 NFS 形式装入的重要信息，请参见第 359 页中的 “12.8.2.3 将基于 NFS 的文件系统用于片段整理和休假缓存”。

这些文件的位置由选项 VACATION_TEMPLATE 控制。应该将该选项（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的路径。模板必须为 file:URL，并且需使用 $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。

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。

17.3 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 进行检查以确保休假操作是由用户级别而不是系统级别 Sieve 脚本来执行。如果在系统级别的脚本中使用休假，将产生一个错误。
2. 选中“无休假通知”内部 MTA 标志。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 检查 `:addresses` 标记的参数中所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:` 头字段中。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。如果已在 `:days` 变量允许的时间范围内发送了回复，则处理将终止并且将不会发送回复。
6. Messaging Server 将通过 `: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，系统会将 `mailautoreplymode` 自动设置为 `reply`。

默认情况下，系统将清除“无休假通知”MTA 标志。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。`novacation` Sieve 操作只允许在系统级别 Sieve 脚本中使用 。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的限制（例如阻止对包含子字符串 `"MAILER-DAEMON"` 的地址的回复）。

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由 `VACATION_TEMPLATE` MTA 选项的设置指定。该选项应设置为 `file: URL`。

这些文件的维护是自动进行的，并由 `VACATION_CLEANUP` 整数 MTA 选项设置控制。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。

17.4 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 MTA 选项 `LDAP_AUTOREPLY_ADDRESSES` 定义的属性

  此属性可以生成 Sieve 休假的 `:addresses` 参数。默认情况下此选项没有值。该属性可以有多个值，其中每个值都指定一个要传递给 `:addresses` 休假参数的单独的地址。

- 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`—创建一个多部分文本，可回显原始邮件文本和添加的 `mailAutoReplyText` 或 `mailAutoReplyTextInternal` 文本。
  - `reply`—将 `mailAutoReplyText` 或 `mailAutoReplyTextInternal` 指定的单个部分的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)，该通知包含作为返回内容的原始邮件。`reply` 将生成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 变量来传送。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。

- 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 设置为另一个属性的名称，可以指示 MAT 使用此信息的另一个属性。

- 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给休假操作。

- 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）。仅当 mailAutoReplyMode=reply 时使用。如果值为 0，则每次收到邮件时将发回一封回复。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，并且不允许值为 0。）

  如果用户条目中未显示该属性，系统将从 AUTOREPLY_TIMEOUT_DEFAULT MTA 选项获取一个默认超时值。通过设置 LDAP_AUTOREPLY_TIMEOUT MTA 选项，可以指示 MTA 使用此信息的另一个属性。

MAT 可以在多个 LDAP 属性和具有不同语言标记的属性值之间进行选择，并确定要使用的正确值。生效的语言标记和与信封 from 地址关联的首选语言信息进行比较。目前接收该处理的属性仅有 LDAP_AUTOREPLY_SUBJECT（通常为 mailAutoReplySubject ）、LDAP_AUTOREPLY_TEXT（通常为 mailAutoReplyText ）、LDAP_AUTOREPLY_TEXT_INT（通常为 mailAutoReplyTextInternal ）、LDAP_SPARE_4、LDAP_SPARE_5、LDAP_PREFIX_TEXT 和 LDAP_SUFFIX_TEXT。

每个属性值应拥有不同的语言标记值。如果不同的值具有相同的标记值，则实际上将会随机选择这些值。

17.5 其他自动回复任务和问题

本部分介绍配置部分没有介绍的自动回复任务和问题。

17.5.1 收到从非 Sun 邮件服务器自动转发的电子邮件时发送自动回复邮件

MTA 收到从非 Sun 系统自动转发的邮件时可能发生自动回复问题。例如，如果客户在 sesta.com 有一个家庭账户，且客户将该账户设置为自动向其 siroe.com 上的工作账户转发邮件，同时，如果 siroe.com 使用 Messaging Server，且该用户将其账户设置为自动回复休假邮件，则 Messaging Server 在发出休假邮件时将出现问题。

发生该问题是因为 sesta.com 邮件服务器将信封地址从 user@sesta.com 更改为 user@siroe.com，但它不更改标题，标题仍然是 user@sesta.com。当 MTA 收到邮件时，它只查看标题地址。它尝试将此地址与 LDAP 用户目录中的地址匹配。如果它找到用户已设置自动回复的匹配，则将发送休假邮件。由于没有 LDAP 地址与 user@sesta.com 匹配，因此没有发送任何休假邮件。该问题在于实际地址位于信封而不是标题中。

由于执行自动转发的远程系统已知的收件人地址对于本地系统的相应用户而言是未知的，因此需要一种方式使此类地址对于本地系统也是已知的，从而在必要时能够发送休假回复。

可通过 Sieve vacation 操作的 :addresses 参数达到此目的。它可接受对应于收件人的地址列表，以执行此检查。MTA 选项 LDAP_AUTOREPLY_ADDRESSES 定义的属性允许在用户 LDAP 条目中指定此类地址。

要在收到从非 Sun 邮件服务器自动转发的邮件后能够自动回复，用户或管理员应该将电子邮件地址从可能转发这些邮件的地址设置为 LDAP_AUTOREPLY_ADDRESSES 定义的属性。

◆ ◆ ◆ 第 18 章

18 邮件过滤和访问控制

本章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。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 481 页中的 “18.1 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。管理员可以控制通过 Messaging Server 发送和接收邮件的人员。

第 504 页中的 “18.9 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。

18.1 第 1 部分：映射表

第 1 部分包含以下各节：

18.2 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。通过这些映射表，您可以控制能够发送和/或接收邮件的人员。表 18–1 列出了本节中介绍的映射表。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，并以斜杠将其与字符串的其余部分 string（通常为 "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。

18.2.1 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 207 页中的 “10.3 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* 是邮件要排队发送至的通道；*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 – 每当修改 mappings 文件之后，必须重新编译配置（请参见第 203 页中的 “10.1 编译 MTA 配置”）。

表 18–1 访问控制映射表

映射表	说明
SEND_ACCESS（请参见 第 486 页中的 “18.3.1 SEND_ACCESS 和 ORIG_SEND_ACCESS 表” 。）	用于根据信封 From 地址、信封 To 地址、源通道和目标通道来阻止外来连接。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 486 页中的 “18.3.1 SEND_ACCESS 和 ORIG_SEND_ACCESS 表” 。）	用于根据信封 From 地址、信封 To 地址、源通道和目标通道来阻止外来连接。执行重写之后，但在别名扩展之前检查 To 地址。
MAIL_ACCESS（请参见 第 487 页中的 “18.3.2 MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射表” 。）	用于根据在 SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息来阻止外来连接。即，将在 SEND_ACCESS 中找到的通道和地址信息与在 PORT_ACCESS 中找到的 IP 地址和端口号信息结合。
ORIG_MAIL_ACCESS（请参见 第 487 页中的 “18.3.2 MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射表” 。）	用于根据在 ORIG_SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息来阻止外来连接。即，将在 ORIG_SEND_ACCESS 中找到的通道和地址信息与在 PORT_ACCESS 中找到的 IP 地址和端口号信息结合。
FROM_ACCESS（请参见 第 488 页中的 “18.3.3 FROM_ACCESS 映射表” 。）	用于根据信封 From 地址来过滤邮件。To 地址为不相关的地址时使用该表。
PORT_ACCESS（请参见 第 490 页中的 “18.3.4 PORT_ACCESS 映射表” 。）	用于根据 IP 编号阻止外来的连接。
IP_ACCESS	用于根据源通道、远程服务器的 IP 地址和当前尝试的 IP 地址索引来阻止外来连接。请参见 第 492 页中的 “18.3.5 IP_ACCESS 映射表” 。

MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射是最常规的，这些映射不仅包含对 SEND_ACCESS 和 ORIG_SEND_ACCESS 可用的地址和通道信息，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）。

18.3 访问控制映射表标志

本节包含以下几个部分：

- 第 486 页中的 “18.3.1 SEND_ACCESS 和 ORIG_SEND_ACCESS 表”
- 第 487 页中的 “18.3.2 MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射表”
- 第 488 页中的 “18.3.3 FROM_ACCESS 映射表”
- 第 490 页中的 “18.3.4 PORT_ACCESS 映射表”
- 第 492 页中的 “18.3.5 IP_ACCESS 映射表”
- 第 493 页中的 “18.3.6 限制指定 IP 地址到 MTA 的连接”

表 18–2 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 映射表支持一组略有不同的标志（请参见表 18–3）。

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 18–2 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 215 页中的 “检查特殊标志”。
$B	将邮件重定向到 bitbucket。
$D	如果请求获得延迟传送收据，则设置该标志（在 FROM_ACCESS 中不可用）。请参见第 215 页中的 “检查特殊标志”。
$E	如果发出/接受 EHLO 命令，从而导致使用 ESMTP，则设置该标志（在 FROM_ACCESS 中不可用）。请参见第 215 页中的 “检查特殊标志”。
$F	如果请求获得失败传送收据，则设置该标志（在 FROM_ACCESS 中不可用）。请参见第 215 页中的 “检查特殊标志”。
$H	将邮件保存为 .HELD 文件。
$L	如果使用 LMTP，则设置该标志（在 FROM_ACCESS 中不可用）。请参见第 215 页中的 “检查特殊标志”。
$S	如果请求获得成功传送收据，则设置该标志（在 FROM_ACCESS 中不可用）。请参见第 215 页中的 “检查特殊标志”。
$T	如果已使用 TLS，则设置该标志。请参见第 215 页中的 “检查特殊标志”。
$U	如果在 ORIG_SEND_ACCESS、SEND_ACCESS、ORIG_MAIL_ACCESS 和 MAIL_ACCESS 中使用，则从映射开始将获得一个整数变量，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放弃。
$!	仅可用于 FROM_ACCESS。禁用与该邮件有关的休假邮件的发送；即，它设置 novacation 标志。（这样做与在系统/通道 Sieve 中明确设置 novacation 的效果相同。）这将覆盖（阻止应用）后续 vacation 操作，该操作在其他情况下可应用于该邮件。
带有变量的标志，按照变量读取顺序+（请勿按字母顺序排列此表！）	

表 18–2 访问映射标志 （续）

标志	说明
$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。
$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，则将 *string* 发送到系统日志（UNIX user.notice 工具和严重性）或事件日志 (NT)。
$>*string*	+++ 如果访问被拒绝，则将 *string* 发送到系统日志（UNIX user.notice 工具和严重性）或事件日志 (NT)。
$D*delay*	延迟响应的间隔为 *delay*（单位为百分之一秒），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* 添加至邮件。
$G*conversion_tag*	如果在 ORIG_SEND_ACCESS、SEND_ACCESS、ORIG_MAIL_ACCESS 和 MAIL_ACCESS 中使用，此标志将从映射结果中读取值，并将该值视为要应用到当前收件人的一组转换标记。如果与 FROM_ACCESS 一起使用，转换标记将应用于所有收件人。在从映射读取的变量序列中，$G 位于 $A（标题地址）之后。请参见第 386 页中的 “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。请参见第 361 页中的 “12.9.2 指定绝对邮件大小限制”。
$X*error-code*	如果拒绝邮件，则发布指定的 *error-code* 扩展 SMTP 错误代码。
$,*spamadjust_arg*	允许您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 标志防止拒绝服务攻击是一个好方法。特别是，在任何 $> 条目或拒绝访问的 $< 条目中使用 $D 是一个很好的方法。

18.3.1 SEND_ACCESS 和 ORIG_SEND_ACCESS 表

您可以使用 SEND_ACCESS 和 ORIG_SEND_ACCESS 映射表来控制其他人能否发送邮件、接收邮件，或同时控制这两方面。访问检查内容包括邮件的信封 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。

如果存在 SEND_ACCESS 或 ORIG_SEND_ACCESS 映射表，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*

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* 是邮件要排队发送至的通道；*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。

此处的地址为信封地址，即信封 From: 地址和信封 To: 地址。如果是 SEND_ACCESS，则将在执行重写、别名扩展等操作后检查信封 To: 地址；如果是 ORIG_SEND_ACCESS，则将在执行重写之后，但在别名扩展之前检查最初指定的信封 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 483 页中的 “18.3 访问控制映射表标志”。

将 MAT 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）的探测值添加一个以垂直条分隔的其他字段。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：

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）发送的邮件源于本地通道 l，传送至 Internet 的邮件通过某种类型 TCP/IP 通道发出。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。在此映射表中，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）。

示例 18–1 SEND_ACCESS 映射表

```
SEND_ACCESS

   *|postmaster@sesta.com|*|*    $Y
   *|*|*|postmaster@sesta.com    $Y
```

示例 18–1 SEND_ACCESS 映射表 （续）

```
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，系统只能读取 "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”邮件源，例如来自基于 PC 的邮件系统或来自 POP 或 IMAP 客户端的邮件。

注 – 尝试发送邮件的客户端将决定是否把 MTA 拒绝错误文本实际提供给尝试发送邮件的用户。如果使用 SEND_ACCESS 拒绝外来 SMTP 邮件，MTA 将只发出一段包括可选拒绝文本的 SMTP 拒绝代码；SMTP 发送客户端将负责使用该信息构建要发送回原始发件人的退回邮件。

18.3.2 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。同样，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*

同样，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*

此处，如果邮件为外来 SMTP 邮件，则 *port-access-probe-info* 由 PORT_ACCESS 映射表探测中通常包含的所有信息组成；否则为空白。*app-info* 包含 HELO/EHLO SMTP 命令中所声明的系统名称。此名称显示在字符串末尾，并以斜杠将其与字符串的其余部分 string（通常为 "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。*submit-type* 可以为 MAIL、SEND、SAML 或 SOML 的其中之一，这取决于将邮件提交给 Messaging Server 的方式。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。而对于 MAIL_ACCESS 映射，*send-access-probe-info* 由 SEND_ACCESS 映射表探测中通常包含的所有信息组成。同样，对于 ORIG_MAIL_ACCESS 映射，*orig-send-access-probe-info* 由 ORIG_SEND_ACCESS 映射表探测中通常包含的所有信息组成。

将 MAT 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

加一个以垂直条分隔的其他字段。如果邮件不具有 ORCPT 地址，则使用原始、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，可以更方便地实施某些类型的控制，例如强制允许在来自特定 IP 地址的邮件中显示哪些信封 From: 地址。这对限制电子邮件伪造，或鼓励用户正确配置其 POP 和 IMAP 客户端的 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，并且确保来自子网 1.2.0.0 中所有系统的邮件上的信封 From: 地址均来自 siroe.com，则可以使用 MAIL_ACCESS 映射表，如以下示例所示。

示例 18–2 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
```

18.3.3 FROM_ACCESS 映射表

FROM_ACCESS 映射表可控制哪些人员可以发送邮件，和/或使用已经验证的地址覆盖不确定的 From: 地址。

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，但增加了已经验证的发件人信息（如果有）。因此，如果存在 FROM_ACCESS 映射表，则对于每次尝试的邮件提交，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*

此处，如果邮件为外来 SMTP 邮件，则 *port-access-probe-info* 由 PORT_ACCESS 映射表探测中通常包含的所有信息组成；否则为空白。*app-info* 包含 HELO/EHLO SMTP 命令中所声明的系统名称。此名称显示在字符串末尾，并以斜杠将其与字符串的其余部分 string（通常为 "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。*submit-type* 可以为 MAIL、SEND、SAML 或 SOML 的其中之一，这取决于将邮件提交给 MTA 的方式。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* 是邮件的来源通道（即对邮件进行排队）；*from-address* 是不确定的邮件创始者的地址；*auth-from* 是已经验证的创始者地址（如果有此信息）或为空白（如果没有已经验证的信息）。

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 483 页中的 “18.3 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以外，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（在接受的邮件上添加 Sender: 标题地址）。例如，使用此映射表，可以将原始信封 From: 地址简单替换为已验证的地址。

示例 18–3 FROM_ACCESS映射表

```
FROM_ACCESS

  *|SMTP*|*|tcp_auth|*|        $Y
  *|SMTP*|*|tcp_auth|*|*       $Y$J$4
```

使用 FROM_ACCESS 映射表修改某些源通道（将 authrewrite 设置为非零值）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，如果在 tcp_local 通道上设置了 authrewrite 2，则无需使用以下 FROM_ACCESS 映射表，因为仅使用 authrewrite 就足以获得此效果（按原样添加已经验证的地址）：

```
FROM_ACCESS

   *|SMTP*|*|tcp_auth|*|     $Y
   *|SMTP*|*|tcp_auth|*|*    $Y$K$4
```

但是，FROM_ACCESS 的真正目的在于允许进行更加复杂和细微的更改，如下面示例所示。如果要向外来邮件添加 Sender: 标题行（显示已经验证的 SMTP AUTH 提交者地址），则可以仅使用 authrewrite 关键字。但是，假设只有在已经验证的 SMTP AUTH 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: 地址仅仅因为信封 From: 包含可选子地址信息而被视为有所不同。

```
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|*|$3* $Y
! If authenticated address matches envelope From: sans
! subaddress, do nothing
  *|SMTP*|*|tcp_auth|*+*@*|$3*@$5* $Y
! Fall though to...
! ...authenticated address present, but didn?t match, so force
! Sender: header
  *|SMTP*|*|tcp_auth|*|* $Y$K$4
```

FROM_ACCESS 中的 $(元字符指定应该从结果字符串中读取地址，并将其用于替代当前覆盖的邮寄主管地址。$) 的效果相当于添加了一个约束条件，即调用映射前不得设置覆盖的邮寄主管地址。这使特定的邮寄主管地址可以与非本地域中的地址一起使用 - 根据定义，域邮寄主管地址只能与本地定义的域一起使用。覆盖地址（当前）是读取任何 $N/$F 失败结果之前，从 FROM_ACCESS 结果读取的最后一个字符串。

18.3.4 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，则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 连接并且您正在使用 MMP，则必须使用 TCPAccess 选项。请参见第 161 页中的 “7.5.1 用 MMP 配置邮件访问”。要通过映射表来控制 SMTP 连接，请使用 INTERNAL_IP 映射表（请参见第 496 页中的 “18.6.1 允许为外部站点进行 SMTP 中继”）。

如果映射探测匹配，则后跟可选字符串的标志 $< 可使 Messaging Server 将字符串发送至系统日志 (UNIX) 或事件日志 (NT)。如果访问被拒绝，则后跟可选字符串的标志 $> 可使 Messaging Server 将字符串发送至系统日志 (UNIX) 或事件日志 (NT)。如果设置了 LOG_CONNECTION MTA 选项的第 1 位和 $T 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。要指定此类文本，可以在条目的右侧添加两个垂直条字符，后跟所需的文本。表 18–3 列出了可用的标志。

在 Messaging Server 的早期版本中（6.2 或更早版本），当设置了 LOG_CONNECTION MTA 选项的第 4 位（值 16）或/和启用了 SMTP auth 时，PORT_ACCESS 映射仅通过 SMTP 服务器（而不是分发程序）进行重新计算。此外，计算仅在发出 AUTH、EHLO 或 HELO 命令时发生。现在这已发生更改，在发送标题之前，只要 SMTP 服务器线程启动，就会无条件地计算 PORT_ACCESS。PORT_ACCESS 将使用 diff 进行重新计算。

表 18–3 PORT_ACCESS 映射表

标志	说明
$D	导致从模板结果的强制性 SMTP auth rulset 和领域之后再读取一个参数，并添加可选的应用程序信息。此值必须是语义与 BANNER_PURGE_DELAY 值相同的整数。即，它指定清除和发送标题前的延迟时间（以百分之一秒为单位）。值为 0 将禁用延迟和清除。请注意，任何 PORT_ACCESS 映射设置都将覆盖 BANNER_PURGE_DELAY SMTP 通道选项。有关使用此反垃圾邮件功能的详细信息，请参见第 450 页中的 “14.9.1 反垃圾邮件技术：延迟发送 SMTP 标题”。
$Y	允许访问。
$U	选择性地启用通道级别调试。
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 string 拒绝访问

表 18–3 PORT_ACCESS 映射表 （续）

标志	说明
$T text	如果设置了 LOG_CONNECTION MTA 选项的第 1 位（值 2）和 $N 标志（以便拒绝连接），则再设置 $T 标志会将 "T" 条目写入连接日志。T 日志条目将包含完整的映射结果字符串（$N 及其字符串）。
+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 映射表做出任何更改之后，您将需要重新启动分发程序，以便分发程序能够看到这些更改。（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。要在电子邮件地址级别进行更加通用的控制，SEND_ACCESS 或 MAIL_ACCESS 映射表可能更加适用。

18.3.5 IP_ACCESS 映射表

IP_ACCESS 映射表可用来对 MTA 将连接的 IP 地址作最后时刻的检查；此连接尝试可能被中止或重定向。这在某些特定情况下很有用，例如，对不应该连接的目标 IP 地址的安全性考虑、何处要避免连接到众所周知的非法目标 IP 地址（例如，127.0.0.1）、何处尝试失败转移到另一个与 lastresort 关键字作用类似的目标 IP 地址（请参见第 330 页中的 “12.4.3.7 最后可用的主机”）。

在尝试打开到远程服务器的连接之前的 SMTP 客户端操作期间，会查询该访问映射。映射探测的格式如下：

```
source-channel|address-count|address-current|ip-current|hostname
```

source-channel 是邮件出队的通道。address-count 是远程服务器的 IP 地址的总数。address-current 是尝试的当前 IP 地址的索引。ip-current 是当前 IP 地址。hostname 是远程服务器的符号名称。下表显示了该映射表的标志。

表 18–4 IP_ACCESS 映射表标志

标志	说明
$N	立即拒绝带有 "invalid host/domain error" 的邮件。任何提供的文本都会被当作拒绝的原因记录下来，但不会被包含在 DSN 中。
$I	跳过当前 IP，不尝试连接。
$A	用映射结果替换当前 IP 地址。

18.3.6 限制指定 IP 地址到 MTA 的连接

要限制特定 IP 地址可以连接到 MTA 的频率，请参见第 19 章。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很有用。以前，此功能是通过使用 Port Access 映射表中的共享库 `conn_throttle.so` 执行的。尚未计划对 `conn_throttle.so` 进行新的改进，MeterMaid 是一个更有效的替代选择。

`conn_throttle.so` 是在 `PORT_ACCESS` 映射表中使用的共享库，用于限制特定 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* 是将对此 IP 地址强制实施的最大速率（连接次数/分钟）。

对于处罚性例程，可以使用例程名称 `throttle_p` 代替 `throttle`。如果某些连接在过去的连接次数太多，则 `throttle_p` 将在以后拒绝这些连接。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，但不会返回任何内容。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 10 为每分钟连接次数的阈值。

$N421$ Connection$ not$ accepted$ at$ this$ time 将，并返回 421 SMTP 代码（瞬态负完成）以及消息 "Connection not accepted at this time"

$E 将立即终止映射进程。它使用此条目的输出字符串作为映射进程的最终结果。

18.4 应用访问控制后

Messaging Server 将尽早检查访问控制映射。此操作的确切执行时间取决于所使用的电子邮件协议（当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，将发生 FROM_ACCESS 拒绝。在发送端开始发送邮件数据之前，将发生 SEND_ACCESS 或 MAIL_ACCESS 拒绝以响应 RCPT TO: 命令。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 映射表均可能生效。

18.5 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很有用。有关详细信息，请参见 《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimta test”。下面的示例显示了样例 SEND_ACCESS 映射表以及结果探测。

```
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:
```

18.6 添加 SMTP 中继

默认情况下，Messaging Server 被配置为阻止 SMTP 中继尝试，即拒绝从未经验证的外部源（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。

当 IMAP 和 POP 客户端尝试通过 Messaging Server 系统的 SMTP 服务器将邮件提交到外部地址，而该地址尚未使用 SMTP AUTH (SASL) 进行验证时，系统将会拒绝这些提交尝试。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。

至于哪些系统和子网将被识别为内部，这通常由 `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 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，任何匹配 123.45.67.89 所有 32 位的 IP 地址均应为匹配项，并应被视为内部地址。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），在右侧指定 $Y。或者您可以修改现有的 $(.../...) 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端都可以通过此 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 $(.../...) 测试条件时十分有用。`imsimta test -mapping` 实用程序更常用于检查 `INTERNAL_IP` 映射表是否对各种 IP 地址输入均返回了所需的结果。

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）或后跟 `imsimta restart smtp` 的 `imsimta cnbuild`（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更多信息以及 `imsimta` 命令行实用程序的信息，请参见 Messaging Server Reference Manual。

18.6.1 允许为外部站点进行 SMTP 中继

所有内部 IP 地址均应按上述说明添加到 `INTERNAL_IP` 映射表中。如果有允许从其进行 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。

如果不希望将这些系统/站点视为真实的内部系统/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 映射表的最后一个 $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 地址语法与上一节中所述的语法相同。只要地址正确，ORIG_SEND_ACCESS 检查就会成功，因此我们可以继续执行 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。

18.7 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 499 页中的 “18.7.2 区分已验证用户的邮件”
- 第 499 页中的 “18.7.3 阻止邮件中继”

要启用由内部主机和客户端来进行 SMTP 中继，则必须将“内部”IP 地址或子网添加到 INTERNAL_IP 映射表。

18.7.1 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）上使用 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
```

  向通道重写地址时，routelocal 通道关键字会使 MTA 尝试将通过此通道的地址中的所有明确路由“短路”，从而阻止通过明确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。该关键字被应用于 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，则调用该映射表的重写规则会将地址重写到 tcp_intranet 通道。

由于 tcp_intranet 通道标有 allowswitchchannel 关键字，因此邮件将被切换到 tcp_intranet 通道，并从该通道进入。如果邮件从其 IP 地址不在 INTERNAL_IP 映射表

中的某个系统进入，则反向信封重写可能会重写到 tcp_local，也可能会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，其他所有通道均被标记为 noswitchchannel，因此邮件也不会切换到其他通道，而是保留在 tcp_local 通道中。

注 – 请注意，使用字符串 "tcp_local" 的所有映射表或转换文件条目可能都需要根据用法更改为 "tcp_*" 或 "tcp_intranet"。

18.7.2 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”客户端用户。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 验证的邮件客户端，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，则他们提交的邮件会被视为进入指定的切换通道。

▼ 要添加有区别的已验证提交，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，此通道上应具有先前默认行中明确或隐含指定的 noswitchchannel）。此通道上应具有 mustsaslserver。

2. **修改 tcp_local 通道，在其中添加 maysaslserver 和 saslswitchchannel tcp_auth，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，那些可以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。

18.7.3 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。特别是，您要阻止邮件进入 tcp_local 通道和从同一通道返回。您可以使用 ORIG_SEND_ACCESS 映射表实现此目的。

通过 ORIG_SEND_ACCESS 映射表，可根据源通道和目标通道阻止通信。在此例中，将阻止来自 tcp_local 通道和返回该通道的通信。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 通道并从该通道直接返回。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。

使用 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。

18.7.4 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接受的要传送或转发的所有邮件均来自具有有效 DNS 名称的地址。最简单的方法是将 mailfromdnsverify 通道关键字放在 tcp_local 通道上。

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，确保接受的要传送和转发的所有邮件均来自具有有效 DNS 名称的地址：

```
ORIG_MAIL_ACCESS

  TCP|*|*|*|*|SMTP*|MAIL|*|*@*|*|*  \
$[msg-svr-base/lib/dns_verify.so,  \
dns_verify,$7|$$y|$$NInvalid$ host:$ $$7$ -$ %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 映像也可用于根据 RBL（Realtime Blackhole List，实时黑洞名单）、MAPS（Mail Abuse Prevention System，邮件滥用防止系统）、DUL（Dial-up User List，拨号用户列表）或 ORBS（Open Relay Behavior-modification System，开放中继修改系统）列

表检查外来连接，作为保护系统免受 UBE 影响的另一种尝试。使用新的 mailfromdnsverify 关键字，还可以使用一种单独的“更易于配置”的方法进行这样的检查，而不必执行 dns_verify 调用。这种更简单的方法是使用 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=sbl-xbl.spamhaus.org.
DNS_VERIFY_DOMAIN=list.dsbl.org.
...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。另一种方法是从 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，而使较后的条目对其他所有人员执行所需的检查。或者，在 ORIG_MAIL_ACCESS 映射表中，如果只将检查应用于从 tcp_local 通道进入的邮件，则对于来自内部系统/客户端的邮件将跳过检查。使用了指向 dns_verify 的条目的示例，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,$1,sbl-xbl.spamhaus.org.]EXTERNAL$E
ORIG_MAIL_ACCESS

  TCP|*|25|*|*|SMTP*|*|tcp_local|*@*|*|*  \
$C$[msg-svr-base/lib/dns_verify.so,\
dns_verify_domain,$1,sbl-xbl.spamhaus.org.]$E
```

18.7.4.1 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。而是，他们只包含 A 记录。

在典型设置中，DNS 中针对特定 IP 地址找到的 TXT 记录包含一个在拒绝邮件时可返回 SMTP 客户端的错误消息。但是，如果未找到 TXT 记录，而是找到 A 记录，则 Messaging Server 5.2 之前的 dns_verify 版本将返回消息 "*No error text available*"

dns_verify 目前支持在无可用 TXT 记录时指定使用默认文本的选项。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*"

18.8 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，以便可以调用通用文本数据库进行特定查找。针对特定查找，使用若干映射表条目调用通用文本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）存储在通用文本数据库中，同时结构化映射表条目以对通用文本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...
```

与使用单独输入每个用户的映射表相比，下面示例中显示了一种更有效的设置（如果包含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。有关设置信息，请参见第 232 页中的 “10.9.1 MTA 文本数据库”。

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，在常规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常规数据库探测中）提供了一种区分所生成的两类探测的方法。如图所示，使用 $C 和 $E 标志环绕通用文本数据库探测在映射表调用通用文本数据库中非常典型。

以上示例显示了根据通用文本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文本数据库中受益。

18.9 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)。

本部分包含以下几个部分：

18.10 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**。与 discard 类似，它也可以无提示删除邮件，但不同的是，discard 只取消隐含保留而不进行其他任何操作，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 Yes 或 No 字符串值的属性。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 的属性。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 重定向现在可以添加以下三个标题字段：

  ```
  resent-date: date-of-resend-operation
  resent-to: address-specified-in-redirect
  resent-from: addres-of-sieve-owner
  ```

  可以使用新的重定向参数 :resent 和 :noresent 控制是否添加这些字段。如果没有这两个参数，将使用系统默认值。系统默认值由新的 SIEVE_REDIRECT_ADD_RESENT MTA 选项控制。将选项设置为 1 时，只要没有使用 :noresent，就能生成这些字段。设置为 0 时，当且仅当使用 :resent 时才能生成这些字段。选项默认值为 1，表示默认情况下为常规重定向生成字段。

- Sieve 重定向通过以下三个新参数得到了增强：

  :resetmailfrom - 将信封 FROM: 地址重置为当前 Sieve 拥有者的地址。

  :keepmailfrom- 保存原始邮件的信封 FROM: 地址。

  :notify - 为重定向的邮件指定一个新的通知标志集。指定一个通知标志列表只需要一个参数。DSN SMTP 扩展的 NOTIFY 参数能接受的标志集在此处同样能被接受：SUCCESS、FAILURE、DELAY 和 NEVER。请注意，这些标志被指定为一个 Sieve 列表，例如：

  ```
  redirect :notify ["SUCCESS","FAILURE"] "foo@example.com";
  ```

  如果没有将 :notify 指定为常规 SMTP 默认值 FAILURE，则默认值为 DELAY。如果没有指定 :notify，则默认值为 :keepmailfrom；如果指定了 :notify，则默认值将变为 :resetmailfrom。一个例外情况是，如果使用 SUCCESS 标志，将无条件的强制使用 :resetmailfrom。

18.11 Sieve 过滤概述

Sieve 过滤器由一个或多个条件操作组成，这些操作将根据邮件标题中的字符串应用于邮件。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，或者用户的邮箱过滤器没有明确应用到问题邮件，Messaging Server 在下一步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，并在目录同步过程期间由 MTA 进行检索。

18.12 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邮箱的邮件。只能使用 Messenger Express 创建基于用户的邮件过滤器。

18.13 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。

表 18–5 `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，则不插入任何内容
$2S	与 `$S` 相同，但如果没有可用的子地址，则不插入任何内容，并删除前面的字符
$3S	与 `$S` 相同，但如果没有可用的子地址，则不插入内容，并忽略后面的字符
$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

表 18–5 filter 通道关键字 URL-pattern 替换标记（不区分大小写） （续）

标记	含义
$H	在主机中替换
$I	插入托管域（domainUidSeparator 指定的分隔符右侧 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，则不插入任何内容
$2I	与 $I 相同，但如果没有可用的托管域，则不插入任何内容，并删除前面的字符
$3I	与 $I 相同，但如果没有可用的托管域，则不插入任何内容，并忽略后面的字符
$L	在本地部分中替换
$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。子地址是子地址分隔符（通常为 +）后原始地址的用户部分，但可由 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。

▼ 创建通道级别的过滤器

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：**

msg-svr-base/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**应用此关键字的通道的邮件启用邮件过滤。sourcefilter 通道关键字将为**来自**应用此关键字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，指定了到问题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 通道关键字将为应用此关键字的通道启用邮件过滤。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，将使用源自问题收件人地址（local-part@host.domain）的字符串进行替换。表 18–5 中显示了这些替换序列。

fileinto 关键字指定在应用邮箱过滤器 fileinto 运算符后如何更改地址。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
```

18.14 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处。要创建 MTA 范围内的过滤器，请执行以下步骤：

▼ 创建 MTA 范围内的过滤器

1. **使用 Sieve 编写过滤器**
2. **将过滤器存储在以下文件中：**

   msg-svr-base /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。

18.14.1 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。

要将邮箱过滤器放弃的邮件临时保留在系统中以待日后删除，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视为位于用户的个人垃圾箱文件夹的扩展部分中。因此，请注意对于 `filter_discard` 队列区域中的邮件，系统永远不会为其发送警告消息，也不会在用户请求退回或返回时，将此类邮件返回给其发件人。而对此类邮件采取的唯一操作是，在最终通知值过期，或使用诸如 `imsimta return` 之类的实用程序请求手动退回时，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。现在则由选项 `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）。

18.15 调试用户级别的过滤器

如果用户抱怨 Sieve 过滤器未按预期运行，则您可以采取一系列步骤来调试过滤器。下面对这些步骤进行了介绍。

▼ 调试用户级别的过滤器

1. **要使 `fileinto` 过滤能够正常工作，请检查在 `imta.cnf` 文件中的 `ims-ms` 通道是否标记如下：**

   ```
   fileinto $U+$S@$D
   ```

2. **从用户 LDAP 条目中获取用户级别的过滤器。**

   用户级别的过滤器存储在 `MailSieveRuleSource` 属性下的 LDAP 条目中。要使用 `ldapsearch` 命令检索此过滤器，请记住它们是以 base64 编码的，因此您需要使用 `-Bo` 切换对输出进行解码。

   ```
   ./ldapsearch -D "cn=directory manager" -w password -b
   "o=alcatraz.sesta.com,o=isp" -Bo uid=test
   ```

下述 imsimta test -rewrite 命令也将自动对它们进行解码。

3 **验证 MTA 是否可以看到用户过滤器。**

发出命令：

```
# imsimta test -rewrite -filter -debug user@sesta.com
```

此命令应该输出您在前面步骤中检索的用户 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 可看到用户过滤器。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。**

您可以使用用户消息存储区域中的 .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: []
or this:
Sieve Result: [action]
```

其中，*action* 是在此邮件上应用 Sieve 过滤器后要执行的操作。

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 结果将为空白，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。

有关输出的更多信息，请参见第 511 页中的 “18.15.1 imsimta test -exp 输出” 。

9 **如果过滤器在语法上有效并且结果正确，则下一步将检查 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。查看正在接收的内容的唯一方法是：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 367 页中的 “12.11.2 调试关键字”中的 slave_debug 关键字。

18.15.1 imsimta test -exp 输出

完整的 imsimta test -exp 命令如下：

```
# imsimta test -exp -mm -block -input=temp.filter -message=rfc2822.msg
```

下面是一个输出示例：

示例 18–4 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: 输出行显示正在从 tmp.filter 文本文件中读取并解析的过滤器。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 显示了文字 redirect, usr3@sesta.com，这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，您将看到 `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并不总是放弃测试的每个 `.msg` 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。在此特定示例中，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。本示例中的结果操作是 `fileinto` 和 `keep`。

测试过滤器时，应当测试两种结果的各个 `.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` 测试而不是使用 `:contains`。例如，如果要匹配 `from=*@sesta.com`，则必须使用 `:matches`，否则测试会由于不满足测试条件而失败。

18.15.2 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` 将整个输入视为一个 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，该文件包含要针对其测试 Sieve 脚本的 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 19 章

19 使用 MeterMaid 限制外来连接

MeterMaid 是一个服务器，可以对连接和事务进行集中测量和管理，方法包括监视 IP 地址和 SMTP 信封地址。就功能而言，MeterMaid 可用来限制某个特定 IP 地址连接到 MTA 的频率。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很有用。MeterMaid 取代了 `conn_throttle.so`，它提供相似的功能，但通过 Messaging Server 安装扩展了这些功能。尚未计划对 `conn_throttle.so` 进行新的改进，MeterMaid 是一个更有效的替代选择。

本节包含以下几个部分：

19.1 技术概述

`conn_throttle.so` 是作为 MTA 映射表中的调用而使用的共享库，该映射表使用内存中的一个外来连接表来确定最近连接的特定 IP 地址何时太频繁，而应暂时转移出去。虽然有一个内存中的表有助于提高性能，但它最大的开销是每个服务器上的每个单独的进程都要维护自己的表。

在大多数情况下，`conn_throttle.so` 调用是在 `PORT_ACCESS` 映射中完成的，该映射通过分发程序（每个系统上的单个进程）访问。仅有的开销是每个服务器都有一个单独的表。

MeterMaid 的主要改进是，它维护限制信息的单个系统信息库，该限制信息可以被 Messaging Server 环境下的所有系统和进程访问。它继续维护一个内存中的数据库来存储数据，以获取最佳性能。重新启动 MeterMaid 将丢失所有以前存储的信息，但由于数据的生命周期通常很短，因此这样的重新启动（不是经常发生）所带来的损失也比较小。

19.2 操作原理

MeterMaid 的配置存储在 msg.conf 中，并通过 configutil 维护。

通过使用 check_metermaid.so 的映射表调用从 MTA 访问 MeterMaid。可以从任何 *_ACCESS 表中调用 MeterMaid。当从 PORT_ACCESS 表中调用时，MeterMaid 可基于连接的 IP 地址检查限制，这是实现 MeterMaid（替代原来的 conn_throttle.so）的最常用方法。如果从别的 *_ACCESS 表中调用，MeterMaid 也可用于对其他数据（如信封 From 或信封 To 地址，以及 IP 地址）建立限制。

在 check_metermaid.so 中只定义一个入口点。throttle 例程联系提供两个以逗号分隔的后续参数的 MeterMaid。第一个参数是用于检查数据的表的名称，第二个参数是要检查的数据。

如果探测得到的结果是，被检查的特定数据超过了它在该表中的配额，check_metermaid.so 将返回 "success"，以便映射引擎继续处理该条目。该条目的剩余部分则用来处理超出配额的连接。

```
PORT_ACCESS

  *|*|*|*|* $C$|INTERNAL_IP;$3|$Y$E
  *|*|*|*|* $C$:A$[/opt/SUNWmsgsr/lib/check_metermaid.so,throttle,tablename,$3]$N421$ \
Connection$ declined$ at$ this$ time$E
  *          $YEXTERNAL
```

请注意，要在调用 check_metermaid.so. 之前处理映射表条目中的 $:A 标志测试，这确保只有在分发程序检查 PORT_ACCESS 时才执行 MeterMaid 探测，因为分发程序将为探测设置 A 标志。

19.3 为 MeterMaid 配置参数

MeterMaid 的配置存储在 msg.conf 中，并通过 configutil 维护。下面是 MeterMaid 当前支持的设置：括号中是默认值。有关 MeterMaid 参数的完整列表，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“configutil Parameters”。

- local.metermaid.enable 在运行 MeterMaid 守护进程的系统上，该设置必须设置为 yes，以便启动 Watcher 并对 MeterMaid 进行控制。
- logfile.metermaid.* 它与 map、pop 和其他服务使用的设置相同。默认情况下，MeterMaid 将日志文件写入 msg-svr-base/data/log/metermaid。
- metermaid.config.listenaddr (INADDR_ANY) MeterMaid 应绑定的地址。在大多数系统中，不需要更改默认值，但对于多穴或 HA 系统，建议指定相应的地址。
- metermaid.config.maxthreads (20) MeterMaid 服务器是多线程的，用于维护安排任务的线程池。该值设置了 MeterMaid 将使用的最大线程数。在有 4 个以上 CPU 的系统中，增加该值可能会增加总的吞吐量。

- `metermaid.config.port` (63837) 这是 MeterMaid 侦听连接的端口，MeterMaid 客户端将连接到此端口。
- `metermaid.config.secret`（无默认值，必须提供值） 为了验证外来连接，MeterMaid 使用一个共享机密，该机密在客户端连接到 MeterMaid 后立即发送。
- `metermaid.config.serverhost`（无默认值，必须提供值） 这是客户端将要连接的主机名或 IP 地址。它可能与 `metermaid.config.listenaddr` 相同，但更可能具有一个特定值将客户端定向到一个系统，特别是 Messaging Server 环境下的系统。

以下设置供 `check_metermaid` 客户端使用：

- `metermaid.mtaclient.connectfrequency` (15) 每 `connectfrequency` 秒尝试一次连接。当客户端需要连接到 MeterMaid 时，将使用此设置作为内部限制，以防止在 MeterMaid 不可用的情况下持续尝试连接。在客户端无法与 MeterMaid 通信期间，该设置将向 MTA 映射引擎返回 "fail" 状态，表示 MeterMaid 还没有阻塞该连接。

  例如，如果 `check_metermaid.so` 尝试连接到 MeterMaid，但由于某种原因失败了，那么在接下来的 N 秒（由 `metermaid.mtaclient.connectfrequency` 指定）内将不再进行其他连接尝试。该设置将防止 `check_metermaid.so` 在 MeterMaid 无法工作的情况下过于频繁地尝试连接到 MeterMaid。
- `metermaid.mtaclient.connectwait` (5) 当客户端等待 MeterMaid 的连接（初始连接或重用另一个已建立好的连接）时，该设置在返回 "fail" 状态并允许继续连接之前将等待 `connectwait` 秒。
- `metermaid.mtaclient.debug` (no) 如果启用该选项，客户端中的调试信息将被输入到服务器或 SMTP 服务器的特定于线程的日志文件中。
- `metermaid.mtaclient.maxconns` (3) 为了支持多线程的服务器，客户端将维护一个到 MeterMaid 的连接池。这样做可以增加通信期间的并发性。但是，由于 MeterMaid 执行的内部锁定，对特定表的访问被限制为一次一个请求，因此来自单个进程的多个连接可能会提供一些好处，但比较有限。
- `metermaid.mtaclient.readwait` (10) 在与 MeterMaid 通信时，客户端在 "fail" 状态并允许继续连接之前将等待 `readwait` 秒。

最后，也会在 `msg.conf` 中定义限制表，如下所示。 每个配置参数中的 * 是被定义的特定表的名称。例如，对于名为 internal 的表，第一个参数应为 `metermaid.table.internal.data_type`.

- `metermaid.table.*.data_type`（字符串） MeterMaid 在其表中支持两类数据：字符串和 ipv4。字符串数据被限制为每个条目 255 个字节，并可以使用区分大小写或不区分大小写功能进行比较（请参见下面列出的 `metermaid.table.*.options`）。
- `metermaid.table.*.max_entries` (1000) MeterMaid 在初始化每个表时，将预分配此数量的条目。MeterMaid 自动回收旧条目，即使这些条目还没有过期。当收到新连接时，MeterMaid 将重新使用最近访问得最少的条目。站点应指定一个足够大的值以缓存 `quota_time` 期间接收到的连接。
- `metermaid.table.*.options` 是一个以逗号分隔的关键字列表，用于定义表的行为或特征。有效的关键字有：

- nocase — 在使用数据时，使用不区分大小写的比较功能来完成所有比较。（此选项仅对字符串数据有效。）
- penalize — 在 quota_time 秒之后，限制通常会将连接数重置为 0，如果启用了 penalize 选项，限制将根据配额减少连接数（但不会小于 0），以便其他连接尝试减少以后的 quota_time 周期。例如，如果配额是 5，quota_time 为 60，在第一分钟内系统收到 12 次连接尝试，则头 5 次连接将被接受，而接下来的 7 次连接将被拒绝。过了 60 秒之后，根据特定地址计算的连接数将减少到 7，仍然将其保持在配额之上，并拒绝连接尝试。假定没有进行额外的连接尝试，又经过 60 秒的周期之后，连接数将进一步减为 2，MeterMaid 会重新允许连接尝试。

- metermaid.table.*.quota (100) 当收到连接时，它将根据配额计数。如果 quota_time 秒内接收到的连接数超过了该值，MeterMaid 将拒绝连接。（对外来连接的实际影响是由映射表控制的，这可能会导致额外的检查、延迟或拒绝连接。）
- metermaid.table.*.quota_time (60) 它指定了连接将根据 quota 进行计数的时间段（秒数）。经过这么多秒后，将根据该表的 type 减少基于外来地址所计算的连接数。
- metermaid.table.*storage (hash) MeterMaid 可以使用两种不同的存储方法：hash 和 splay。建议使用默认的散列表，但在某些情况下，splay 树可能会提供更快的查找功能。
- metermaid.table.*.type (throttle) 目前，MeterMaid 唯一支持的表类型为 throttle。该类型的表跟踪数据，通常是 IP 地址，并在 quota_time 秒的周期内将外来连接限制为 quota 连接。

19.4 示例 — 使用 Metermaid 限制过多的 IP 地址连接

本示例使用 MeterMaid 将 IP 地址限制为每分钟 10 次连接。下面给出映射文件中等效的 conn_throttle.so 设置供参考：

```
PORT_ACCESS
   *|*|*|*|*  $C$|INTERNAL_IP;$3|$Y$E
   *|*|*|*|*  $C$[/opt/SUNWmsgsr/lib/conn_throttle.so,throttle,$3,10]\
$N421$ Connection$ declined$ at$ this$ time$E
   *          $YEXTERNAL
```

此 PORT_ACCESS 映射表实现了 conn_throttle.so，将非 INTERNAL 连接限制为每分钟不超过 10 次连接的速率。

这两种技术之间的一个基本区别是，MeterMaid 不是直接将速率限制之类的细节配置到映射表中，而是使用 configutil 参数进行设置。下面介绍了此示例。

1. **指定某一系统为 MeterMaid 服务器主机。**

   在此系统中，设置以下 configutil 参数：

   ```
   local.metermaid.enable -v TRUE
   ```

设置一个验证密码，用于验证客户端和 MeterMaid 服务器之间的通信：

```
configutil -o metermaid.config.secret -v password
```

2. **定义一个限制表。**

   MeterMaid 的限制行为由指定限制表的使用决定，这些表定义了操作特性。定义一个将连接速率限制为每分钟 10 次的表，请设置以下参数：

   ```
   configutil -o metermaid.table.ext_throttle.data_type -v ipv4
   configutil -o metermaid.table.ext_throttle.quota -v 10
   ```

   ext_throttle 是限制表的名称。`ipv4` 是数据类型 Internet 协议版本 4 地址的表示形式。10 是配额（连接限制）。

3. **在 MeterMaid 系统上，启动 MeterMaid。**

   ```
   # start-msg metermaid
   ```

4. **在 MTA 将使用 MeterMaid 进行限制的系统上，指定 MeterMaid 主机和密码。**

   需要进行以下设置：

   ```
   configutil -o metermaid.config.secret -v MeterMaid_Password
   configutil -o metermaid.config.serverhost -v name_or_ipaddress_of_MetermaidHost
   ```

5. **设置 MeterMaid `PORT_ACCESS` 表。**

   此表类似于等效的 `conn_throttle.so` 设置：

   ```
   PORT_ACCESS

      *|*|*|*|*  $C$|INTERNAL_IP;$3|$Y$E
      *|*|*|*|*  $C$:A$[/opt/SUNWmsgsr/lib/check_metermaid.so,throttle,\
   ext_throttle,$3] $N421$ Connection$ declined$ at$ this$ time$E
      *          $YEXTERNAL
   ```

   第一行检验尝试连接的 IP 地址是否是内部的。如果是，则允许连接。第二行通过 MeterMaid 执行 IP 地址检查，如果该 IP 地址连接过于频繁则减少连接次数。第三行允许任何其他标记为 `EXTERNAL` 的连接通过。

   请注意，此 `check_metermaid.so` 的调用与 `conn_throttle.so` 的调用非常相似。`check_metermaid.so` 中的函数是相同的。`throttle` 及其参数就是使用 `metermaid.table.`*tablename* 配置的表名称和要检查的 IP 地址 (`$3`)。与 `conn_throttle.so` 一样，在达到限制（在`metermaid.table.ext_throttle.quota` 中指定）时，此函数返回 *success*。这将允许处理映射条目行的剩余部分，向远程 SMTP 客户端发送一则消息（421 SMTP 代码，瞬态负完成，**此时不接受连接**），并通知分发程序关闭连接。

同时要注意，`$:A` 确保仅在从分发程序调用时才处理此行。若没有该项，还将在 `tcp_smtp_server` 进程的上下文中将调用 `check_metermaid.so`，并探测 `PORT_ACCESS` 映射表。这将导致 MeterMaid 对每个外来连接计数 2 次。

这就是将 MeterMaid 设置为 `conn_throttle.so` 的替代方案的基本配置。有关这些主题的信息，请参见第 210 页中的 “10.3.2 映射操作”和第 490 页中的 “18.3.4 PORT_ACCESS 映射表”。

19.4.1 其他有用的 MeterMaid 选项

有两个其他的配置选项在某些环境下可能很有用。`conn_throttle.so` 共享库还有一个 `throttle_p` 函数，它通过推算超出 60 秒（基本值）的延长时间段，阻止超过限制的连接。通过在 MeterMaid 服务器系统上配置以下选项，可以在 MeterMaid 中实现相同的行为：

```
configutil -o metermaid.table.ext_throttle.options -v penalize
```

这将更改 `ext_throttle` 表的行为，以便在连接尝试次数大于为 `metermaid.table.ext_throttle.quota` 设置的值时，可以阻止连接。

另一个选项与接收大量连接的系统有关。由于 MeterMaid 能够跟踪整个分布式 MTA 环境中的连接，因此 MeterMaid 内部的内存数据库中所保留的连接的数量限制对于 MTA 环境的总体容量可能会不足。默认值是每个表 1000 个条目，但如果您希望整个 MTA 环境中每分钟的连接数超过 1000，则可以通过以下配置选项增加连接数：

```
configutil -o metermaid.table.ext_throttle.max_entries -v max_entries
```

请注意，即使在 60 秒内达到了 *max_entries*，MeterMaid 仍会自动丢弃最早的和最少使用的条目。因此，在 MeterMaid 的表中将保留连接较频繁的系统并进行计数，从而保持足够的信息以提供有效的限制。

◆ ◆ ◆ 第 20 章

20 管理消息存储

本章介绍了消息存储和消息存储管理界面。本章包含以下各节：

20.1 概述

消息存储包含特定 Messaging Server 实例的用户邮箱。消息存储的大小随邮箱、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，消息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消息存储分区（请参见第 563 页中的 “20.10 配置消息存储分区”）。

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消息存储。

为了管理消息存储，Messaging Server 提供了一组命令行实用程序，如表 20–1 中所述。有关使用这些实用程序的信息，请参见第 565 页中的 “20.11 执行消息存储维护过程”和《Sun Java System Messaging Server 6.3 Administration Reference》。

表 20–1 消息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 邮件客户端可以访问的消息存储。
`hashdir`	标识包含用于特定用户的消息存储的目录。
`imsconnutil`	监视消息存储的用户访问。
`imexpire`	根据管理员指定的条件（如生存期）自动从消息存储中删除邮件。
`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 Messaging Server 邮箱导出到 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消息存储中的信息同步。
`MoveUser`	将用户的帐户从一个邮件服务器移动到另一个邮件服务器。
`imquotacheck`	计算消息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。

20.2 消息存储目录布局

图 20–1 显示了服务器实例的消息存储目录布局。消息存储用于提供对邮箱内容的快速访问。表 20–2 中介绍了存储目录。

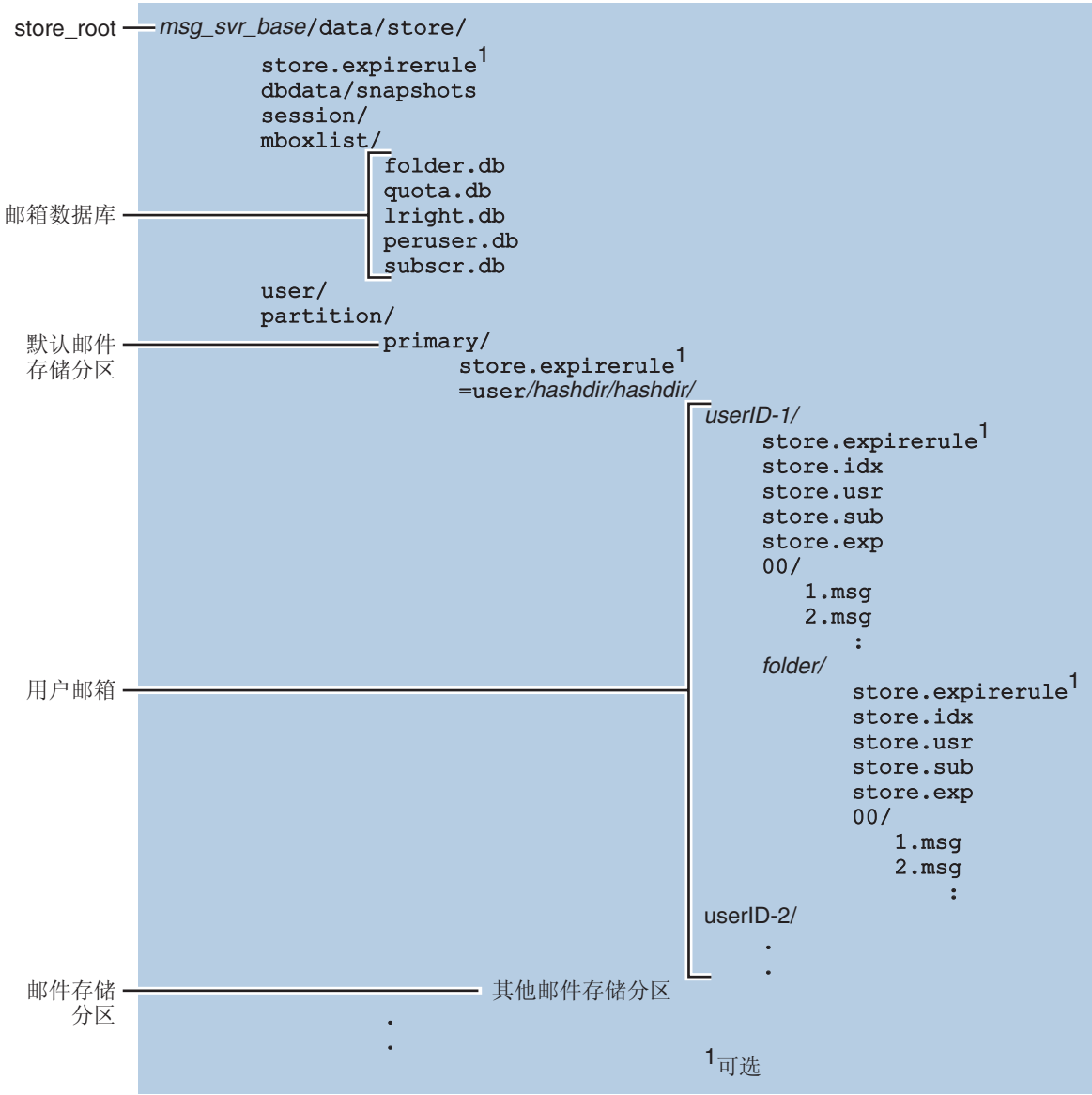


图 20–1 消息存储目录布局

消息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消息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**消息存储分区**，即专门用于存储消息存储的**磁盘**分区上的一个区域。有关详细信息，请参见第 563 页中的 “20.10 配置消息存储分区”。虽然为了易于维护，我们建议每个消息存储分区使用一个磁盘分区，但是消息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
```

下表介绍了消息存储目录。

表 20–2 消息存储目录说明

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` 消息存储的顶层目录。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 554 页中的 “20.9 设置自动删除邮件（过期和清除）功能”。
store_root`/dbdata/snapshots`	`stored` 周期性进行的消息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/`	包含活动消息存储进程的信息。
store_root`/user/`	不使用。
store_root`/partition/`	包含消息存储分区。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。

表 20–2 消息存储目录说明 （续）

位置	内容/说明
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。
.../=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*/ **或** .../*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。

20.2.1 有效和无效的文件夹名称

以下是有效和无效的 IMAP 文件夹字符。

有效的 IMAP 文件夹字符：<space> ! " # $ & ' ( ) + , - . / 0-9 : ; < = > @ A-Z [\ ] ^ _ ‘ a-z { | } ~

无效的 IMAP 文件夹字符：% * ?

请注意，某些字符序列将被拒绝，例如名为 public/ 的文件夹。使用英语语言环境时这些限制同样适用。其他语言（如日语）使用编码字符集。

20.3 消息存储如何删除邮件

从消息存储中删除邮件分三个阶段：

1. **删除**。客户端可以将邮件标志设置为**删除**。此时邮件被标记为删除，但是通过去掉删除标志，客户端仍然可以恢复邮件。如果有第二个客户端，则已删除标志可能不会立即被该客户端识别。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，邮件将从消息存储索引文件 `store.idx` 中删除。邮件本身仍然在磁盘上，但是一旦邮件被擦除，客户端将不能再恢复邮件。

   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 554 页中的 “20.9 设置自动删除邮件（过期和清除）功能”。
3. **清除**。默认情况下，`imexpire` 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 `local.schedule.expire` 和 `store.cleanupage` 配置此实用程序，其中 local.schedule.expire 用于控制邮件过期时间安排，而 store.cleanupage 用于控制清除操作的宽限期（在此宽限期之前不会清除邮件）。请注意，这与 `imsimta purge` 命令和用于清除旧版本 MTA 日志文件的 `configutil` 参数 `local.schedule.purge` 不同。

20.4 指定管理员对存储的访问权限

消息存储管理员可以查看和监视用户邮箱，并指定消息存储的访问控制。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消息存储以进行 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：

- 第 527 页中的 “添加管理员条目”
- 第 527 页中的 “修改管理员条目”
- 第 527 页中的 “删除管理员条目”
- 第 527 页中的 “20.4.1 防止邮箱由管理员之外的其他人员删除或重命名”

▼ 添加管理员条目

- **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

- **命令行。**

  要通过命令行修改“消息存储管理员 UID”列表中的现有条目，请运行以下命令：

  ```
  configutil -o store.admins -v "adminlist"
  ```

  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`）。

▼ 删除管理员条目

- **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"
  ```

  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`）。

20.4.1 防止邮箱由管理员之外的其他人员删除或重命名

您可能希望某些邮箱受到保护以免管理员之外的其他人员删除或修改。下面的过程介绍了如何实现此操作。如果除管理员之外的其他人员试图删除、修改或重命名受保护的邮箱，系统将显示**邮箱已固定**错误消息。

设置 `local.store.pin` `configutil` 变量。使用以下格式：

```
configutil -o local.store.pin -v "mailbox1"%"mailbox2"%"mailbox 3"
```

其中，*mailbox1*、*mailbox2* 和 *mailbox 3* 是要保护的邮箱（请注意，邮箱名中可以使用空格），`%` 是邮箱间的分隔符。

20.5 关于共享文件夹

组或**共享文件夹**与任意其他邮件文件夹类似，不同之处在于，其他用户和组可以根据所具有的权限读取、删除组或共享文件夹中的邮件或向其中添加邮件。将邮件添加到共享文件夹时，可以通过普通的拖放操作、使用 Sieve 过滤器或直接使用以下形式发送邮件来实现：*uid+folder @domain*。

下面的示例显示了向某个**专用共享文件夹**发送电子邮件时所用的地址，该文件夹名为 `crafts_club`，由 carol.fanning@siroe.com 拥有：

```
carol.fanning+crafts_club@siroe.com
```

下面的示例显示了向某个**公用共享文件夹**发送电子邮件时所用的地址，该文件夹名为 `tennis@siroe.com`。

```
public+tennis@siroe.com
```

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电子邮件对话非常有用。例如，一组软件开发者可以创建名为 `mosaic_voices` 的共享文件夹，用于讨论特定项目的开发。将邮件发送或拖至 `mosaic_voices` 文件夹时，任何有权访问该共享文件夹的用户（可以通过单个地址或组地址添加权限）都可以打开此邮箱并阅读邮件。

共享文件夹显示在用户邮箱树中名为 `Shared Folders` 的文件夹下。下面显示了一个示例：

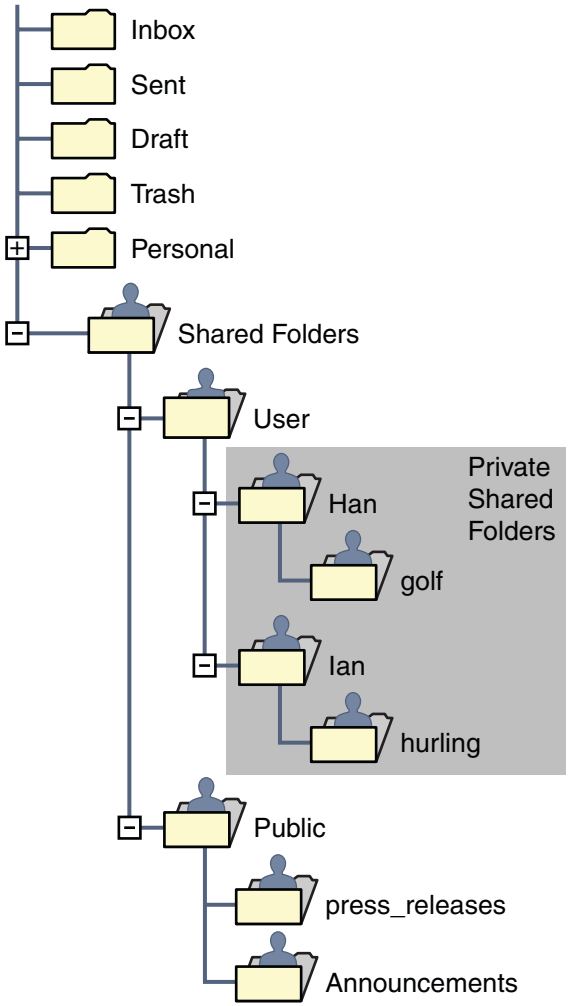


图 20–2 来自邮件客户端的共享邮件文件夹列表示例

有两种共享文件夹：

- **专用共享文件夹**—由特定用户使用 Communications Express 或其他支持创建共享文件夹的邮件客户端创建和拥有的共享文件夹。（有关详细信息，请参见 Communications Express 帮助屏幕。）专用共享文件夹位于 `Shared Folders/User` 邮件文件夹目录中。
- **公用共享文件夹**—公用共享文件夹由邮件管理员创建，但没有拥有者。公用文件夹的电子邮件地址类似如下形式：

  `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。公用共享文件夹位于 Shared Folders/Public 邮件文件夹目录中。

通常，只有特定消息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消息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 534 页中的 “20.6.4 设置分布式共享文件夹” 。

20.6 共享文件夹任务

本节介绍了共享文件夹的管理员任务：

▼ 指定专用共享文件夹的共享属性

1 **专用共享文件夹由用户创建。**

许多邮件客户端支持创建专用共享文件夹。您可以在 Communications Express 上尝试该操作。

2 **设置专用共享文件夹的共享参数。**

支持以下 configutil 参数：

store.privatesharedfolders.restrictanyone - 如果启用 (1)，将禁止一般用户将专用共享文件夹的权限设置为 anyone。默认值：0

store.privatesharedfolders.restrictdomain - 如果启用 (1)，将禁止一般用户与其域之外的用户共享专用文件夹。默认值：0

store.privatesharedfolders.shareflags - 如果为 0，用户之间将不能共享标记。如果为 1，用户之间可以共享标记。默认值：0

store.publicsharedfolders.user - 公用共享文件夹拥有者的 userid。通常只是 public。默认值：NULL（未设置）

▼ 创建公用共享文件夹

由于公用文件夹的创建需要访问 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 **创建一个名为 `public` 的 LDAP 用户条目，用作所有公用文件夹的容器（请参见第 528 页中的“ 20.5 关于共享文件夹 ”）。**

示例：

```
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 `public` 帐户内创建文件夹。**

例如，创建一个名为 gardening 的公用文件夹：

```
mboxutil -c user/public/gardening
```

3 **设置文件夹的名称。**

通常为 `public`。以下是将文件夹名称设置为 `public` 的命令：

```
configutil -o store.publicsharedfolders.user –v public
```

4 **指定用户及其对该共享文件夹的访问权限。**

使用 `readership` 命令指定用户及其访问权限。例如，以下命令将授予 `sesta.com` 上的每个用户对 `gardening` 公用文件夹的查找、读取和邮寄访问权限：

```
readership -s user/public/gardening anyone@sesta.com lrp
```

有关如何使用 readership 的详细说明，请参见第 532 页中的 “20.6.2 设置或更改共享文件夹的访问控制权限”。

20.6.1 使用电子邮件组添加共享文件夹

共享文件夹通常可以通过使用 Communications Express 向共享文件夹列表中添加用户，或通过之前介绍的创建公用共享文件夹来创建。但是，有时用户可能希望向共享文件夹列表中添加电子邮件组（邮件分发列表），以使组中的每个用户均具有访问该共享文件夹的权限。例如，名为 tennis@sesta.com 的组具有 25 名成员，他们决定创建一个共享文件夹以存储所有发送到该组地址的电子邮件。

▼ 向共享文件夹中添加电子邮件组

需要具有系统管理员权限才可以向共享文件夹中添加电子邮件组。

1. **创建一个文件夹。（如果已创建，则跳过该步骤。）**

   通常由组中的某位成员完成此操作。如果该文件夹尚未创建，则可以使用以下命令为他们创建该文件夹：

   ```
   mboxutil -c user/gregk/gardening
   ```

   gregk 是共享文件夹拥有者的 uid。gardening 是共享文件夹的名称。

2. **向每个将拥有组共享文件夹访问权限的成员的用户条目中添加 aclGroupAddr *group_name@domain* 属性-值对。**

   对于上述示例，向每个有权访问共享文件夹的用户条目中添加以下属性-值对：

   ```
   aclGroupAddr: tennis@sesta.com
   ```

   请注意，如果使用组条目中的 memberURL 属性动态创建组，则组成员将已具有该属性。该属性的 URL 值与以下所示类似：

   ```
   memberURL: ldap:///o=sesta.com??sub?(&(aclGroupAddr=tennis@sesta.com)
   (objectclass=inetmailuser))
   ```

   （由于印刷原因，样例条目行已自动换行。实际条目应显示在一行中。）

3. **指定组和对共享文件夹的访问权限。**

   使用 readership 命令执行此操作。对于上述示例，以下命令将授予 tennis@sesta.com 的成员对公用文件夹 gardening 的查找、读取和邮寄访问权限：

   ```
   readership -s user/gregk/tennis tennis@sesta.com lrp
   ```

   有关如何使用 readership 的详细说明，请参见第 532 页中的 “20.6.2 设置或更改共享文件夹的访问控制权限”。

20.6.2 设置或更改共享文件夹的访问控制权限

用户可以使用 Communications Express 界面设置或更改对共享文件夹的访问控制。管理员可以使用 readership 命令行实用程序设置或更改对共享文件夹的访问控制。命令的格式如下：

`readership -s`*foldername identifier rights_chars*

其中，*foldername* 是要为其设置权限的公用文件夹的名称，*identifier* 是要为其指定权限的个人或组，*rights_chars* 是要指定的权限。有关每个字符的含义，请参见表 20–3。

注 – 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。

表 20–3 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：来自文件夹的 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、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）

20.6.2.1 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
```

要为消息存储上的每个用户指定相同的访问权限，请发出以下命令：

```
readership -s User/public/golftournament anyone 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=golf@sesta.com 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@sesta.com 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@sesta.com lwr
```

要拒绝个人或组的访问权限，请为 ACL 权限字符加上前缀短划线。例如，要拒绝对 jsmith 的邮寄权限，请发出以下命令：

```
readership -s User/public/golftournament jsmith@sesta.com -p
```

注 – 使用 *uid+folder@domain* 地址向共享文件夹邮寄邮件需要在具备 p（邮寄）访问权限的前提下使用 readership 命令。请参见第 532 页中的 “20.6.2 设置或更改共享文件夹的访问控制权限”。

20.6.3 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。

20.6.4 设置分布式共享文件夹

通常，只有特定消息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消息存储中访问的**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消息存储组内的所有用户。但是，请注意 Web 邮件客户端（HTTP 访问客户端，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：

- 消息存储 userid 在消息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 20–4 中列出的配置变量，将远程消息存储（即不保留共享文件夹的消息存储）配置为代理服务器。

表 20–4 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`	消息存储服务器列表	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

20.6.4.1 设置分布式共享文件夹—示例

图 20–3 显示了三个名称分别为 StoreServer1、StoreServer2 和 StoreServer3 的消息存储服务器的分布式文件夹示例。

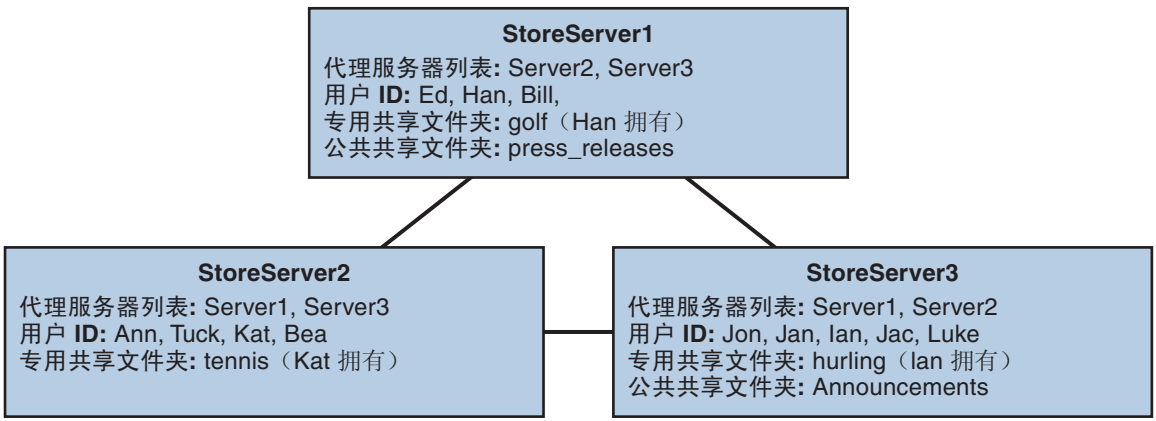


图 20–3 分布式共享文件夹—示例

通过设置表 20–4 中所示的变量，这些服务器被相互连接成对等的代理消息存储。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上的用户均可以访问这三个共享文件夹中的任何一个。图 20–2 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 :> imcheck -d lright.db
Ed: user/Han/golf
Ian: user/Han/golf
anyone: user/public/press_releases
```

```
$ StoreServer2 :> imcheck -d lright.db
Jan: user/Kat/tennis
Ann: user/Kat/tennis
anyone: user/public+Announcements user/public+press_releases



$ StoreServer3 :> imcheck -d lright.db
Tuck: user/Ian/hurling
Ed: user/Ian/hurling
Jac: user/Ian/hurling
anyone: user/public/Announcements
```

20.6.5 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 副本的文件夹的记录。`peruser.db` 包含每个用户和邮箱的条目，其中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 20–5 `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 537 页中的 “20.6.5.1 监视共享文件夹的使用情况”
- 第 537 页中的 “20.6.5.2 列出用户及其共享文件夹”
- 第 537 页中的 “20.6.5.3 删除不活动的用户”
- 第 537 页中的 “20.6.5.4 设置访问权限”

20.6.5.1 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
```

20.6.5.2 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：

```
imcheck -d lright.db
```

输出示例：

```
$ imcheck -d lright.db
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
```

20.6.5.3 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
```

20.6.5.4 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 532 页中的 “20.6.2 设置或更改共享文件夹的访问控制权限”。

20.7 管理邮件类型

本节包含以下主题：

20.7.1 邮件类型概述

统一邮件服务应用程序可以接受、发送、存储和管理多种邮件类型，包括文本邮件、语音邮件、传真邮件、图像数据以及其他数据格式。消息存储允许您定义多达 63 种不同的邮件类型。

有一种利用类型处理邮件的方法，即根据邮件类型将其分组到不同的文件夹中。

引入了邮件类型功能后，无需再使用单个邮箱文件夹维护不同的邮件类型。配置邮件类型后，无论将消息存储在何处，消息存储都能够识别出来。因此，您可以在同一个文件夹中存储不同的邮件类型。您也可以执行以下任务：

- 跟踪邮件类型的使用
- 发送按邮件类型分组的通知
- 对不同的邮件类型设置并管理不同的配额，无论它们是存储在同一个文件夹还是不同的文件夹中
- 根据为每种邮件类型配置的唯一标准将邮件从一个文件夹移动到另一个文件夹
- 根据为每个邮件类型配置的标准处理邮件过期

20.7.1.1 规划邮件类型配置

在统一邮件服务应用程序中，给不同格式的数据分配标准的 Internet 邮件标题，以便 Messaging Server 能够存储和管理这些数据。例如，当语音邮件发送到终端用户的电话时，电话前端系统将邮件标题添加到外来语音邮件，并将其传送到消息存储。

为了识别并管理不同类型的邮件，统一邮件服务系统的所有组件都必须使用相同的邮件类型定义和标题字段来标识邮件。

在配置消息存储支持邮件类型前，您必须

- 计划您希望使用的邮件类型
- 决定每个邮件类型的定义
- 决定要使用的标题字段

例如，如果您的应用程序包括电话邮件，您可以将该邮件类型定义为 "multipart/voice-message" 并使用 Content-Type 标题字段来标识邮件类型。

然后，您可以配置电话前端系统，将以下标题信息添加到每一个将被传送到消息存储的电话邮件：

```
Content-Type: multipart/voice-message
```

接下来，您可以配置消息存储以识别 `multipart/voice-message` 邮件类型，这将在下面几节中介绍。

20.7.1.2 定义和使用邮件类型

定义邮件类型就是给邮件一个唯一的定义，如 `multipart/voice-message`。默认情况下，消息存储读取 Content-Type 标题字段以确定邮件类型。只要您愿意，也可以配置其他标题字段来标识邮件类型。

消息存储读取 Content-Type 标题字段（或其他指定的字段），忽略大小写。也就是说，即使标题的大小写字母组合与规定的不同，消息存储也视其为有效的标题字段。

消息存储只读取标题字段中的邮件类型名称。它忽略其他参数。

要定义邮件类型，可使用 `configutil` 实用程序设置 `store.messagetype` 参数的值。有关说明，请参见第 539 页中的 “配置邮件类型”。

配置邮件类型允许消息存储标识和操作指定类型的邮件。这是统一邮件服务应用程序中管理邮件类型首要的、基本的步骤。

要充分利用消息存储提供的邮件类型功能，还应该执行以下部分或全部任务：

- 配置 JMQ 通知插件并编写 Message Queue 客户端，以检索跟踪邮件类型状态的通知。
- 配置应用到每个邮件类型的配额根
- 根据邮件类型编写过期规则，将 LDAP 属性值设置为过期，并清除邮件。

这些任务在以下小节中汇总：

- 第 542 页中的 “20.7.3 发送邮件类型的通知邮件”
- 第 543 页中的 “20.7.4 按邮件类型管理配额”
- 第 545 页中的 “20.7.5 按邮件类型制定邮件过期规则”

▼ 配置邮件类型

要配置邮件类型，可使用 `configutil` 实用程序设置定义和标识邮件类型的 `store.messagetype` 参数。

1 **通过将 `store.messagetype.enable` 参数设置为 `on` 启用邮件类型。**

`configutil` 参数允许消息存储标识和操作邮件类型。必须先设置该参数才能配置各个邮件类型。

例如，输入以下命令：

```
configutil -o store.messagetype.enable -v 1
```

2 **通过设置 `store.messagetype.`*x* 参数定义和标识邮件类型。**

变量 *x* 标识消息存储中的这一特定邮件类型。变量 *x* 必须是大于 0 小于 64 的整数。您可以将该参数配置为其中任何一个整数，最多能够定义 63 种邮件类型。

使用描述类型的文本字符串定义邮件类型的值。

例如，要定义文本邮件类型，您可以输入以下命令：

```
configutil -o store.messagetype.1 -v text/plain
```

要定义语音邮件类型，您可以输入以下命令：

```
configutil -o store.messagetype.2 -v multipart/voice-message
```

3 **通过设置 `store.messagetype.`*x*`.flagname` 参数为邮件类型提供标志名称。**

该参数创建一个标识邮件类型的唯一标志。在被标识类型的邮件第一次出现在消息存储中时，该标志将自动设置，在该邮件清除前该标志将一直与之关联。标志名称值是一个描述邮件类型的文本字符串。它不必与使用 `store.messagetype.`*x* 参数设置的值相同。

变量 *x* 是使用 `store.messagetype.`*x* 参数定义的邮件类型的整数 ID。

例如，要定义之前的步骤中配置的邮件类型的标志名称，可输入以下命令：

```
configutil -o store.messagetype.1.flagname -v text

configutil -o store.messagetype.2.flagname -v voice_message
```

4 **通过设置 `store.messagetype.`*x*`.quotaroot` 参数配置配额根名称。**

该参数启用配额函数来标识和管理该邮件类型的配额根。参数值是一个名称—一个描述邮件类型的文本字符串。它不必与使用 `store.messagetype.`*x* 参数设置的值相同。

变量 *x* 是使用 `store.messagetype.`*x* 参数定义的邮件类型的整数 ID。

配置该参数时，您可以设置应用到指定邮件类型的配额。有关详细信息，请参见第 543 页中的 “20.7.4 按邮件类型管理配额”。

例如，要对之前的步骤中配置的邮件类型使用配额根，可输入以下命令：

```
configutil -o store.messagetype.1.quotaroot -v text

configutil -o store.messagetype.2.quotaroot -v voice
```

5 **要配置其他标题字段来标识邮件类型，可设置 `store.messagetype.header` 参数。**

默认情况下，消息存储读取 Content-Type 标题字段来确定标题类型。只有希望使用其他标题字段来标识邮件类型时才需要配置 `store.messagetype.header` 参数。该参数的值是一个文本字符串。

例如，要使用名为 `X-Message-Type` 的字段，可输入以下命令：

```
configutil -o store.messagetype.header -v X-Message-Type
```

20.7.2 IMAP 命令中的邮件类型

当您为邮件类型配置 `store.messagetype.`*x*`.flagname` 参数时，您创建了一个标识该邮件类型的唯一标志。最终用户无法修改此标志。

Messaging Server 将邮件类型标志作为用户标志呈现给 IMAP 客户端。将邮件类型映射到用户标志允许邮件客户端使用简单的 IMAP 命令根据邮件类型来操纵邮件。

例如，您可以执行以下操作：

- 使用 IMAP FETCH FLAGS 命令将邮件类型标志名称作为用户定义的标志向客户端显示。

  有关 IMAP FETCH FLAGS 命令的用法示例，请参见示例 20–1，如下所示。
- 使用邮件类型标志作为 IMAP SEARCH 命令中的关键字。

  有关 IMAP SEARCH 命令的用法示例，请参见示例 20–1，如下所示。

邮件类型用户标志是只读的。它不能被 IMAP 命令修改。

下例假定您使用这里显示的值配置邮件类型 `configutil` 参数：

```
store.messagetype.enable = yes

store.messagetype.1 = text/plain
store.messagetype.1.flagname = text
store.messagetype.1.quotaroot = text

store.messagetype.2 = multipart/voice-message
store.messagetype.2.flagname = voice_message
store.messagetype.2.quotaroot = voice
```

示例 20–1 基于邮件类型 `configutil` 配置的 IMAP FETCH 会话

以下 IMAP 会话读取当前选择的邮箱中的邮件：

```
2 fetch 1:2 (flags rfc822)
* 1 FETCH (FLAGS (\Seen text) RFC822 {164}
```

示例 20–1 基于邮件类型 configutil 配置的 IMAP FETCH 会话 （续）

```
Date: Wed, 8 July 2006 03:39:57 -0700 (PDT)
From: bob.smith@siroe.com
To: john.doe@siroe.com
Subject:  Hello
Content-Type: TEXT/plain; charset=us-ascii


* 2 FETCH (FLAGS (\Seen voice_message) RFC822 {164}

Date: Wed, 8 July 2006 04:17:22 -0700 (PDT)
From: sally.lee@siroe.com
To: john.doe@siroe.com
Subject:  Our Meeting
Content-Type: MULTIPART/voice-message; ver=2.0

2 OK COMPLETED
```

在上例中，读取了两个邮件，一个文本邮件和一个语音邮件。

邮件类型标志使用由 `store.messagetype.*.flagname` 参数配置的格式来显示。

Content-Type 标题字段标识邮件类型。邮件类型名称显示为来自外来邮件。它们使用大小写字母的组合，并包括 `charset=us-ascii` 之类的邮件类型参数。

示例 20–2 基于邮件类型 configutil 配置的 IMAP SEARCH 会话

以下 IMAP 会话在当前选择的邮箱中搜索语音邮件：

```
3 search keyword voice_message
* SEARCH 2 4 6
3 OK COMPLETED
```

在上例中，邮件 2、4、6 是语音邮件。用来搜索的关键字是 `voice_message`，即 `store.messagetype.2.flagname` 参数的值。

20.7.3 发送邮件类型的通知邮件

通知可以传送关于各种不同类型的邮件（例如文本邮件、语音邮件和图像数据）的状态信息。Messaging Server 使用 Sun Java System Message Queue 发送邮件类型的通知信息。有关为 Message Queue 配置 JMQ 通知插件的消息，请参见第 22 章。

要启用 JMQ 通知插件识别特定的邮件类型，必须配置 `store.messagetype` 参数，包括 `store.messagetype.`*x*`.flagname` 参数。有关详细信息，请参见第 539 页中的 “配置邮件类型”。

一旦配置了邮件类型，JMQ 通知邮件就能够标识特定邮件类型。您可以编写 Message Queue 客户端，以根据邮件类型解释通知邮件，并将每种类型的状态信息传送到邮件客户端。

JMQ 通知功能可以按邮件类型统计邮箱中的当前邮件数。随通知邮件发送的是指定每种邮件类型计数的数组，而不是一个计数。

例如，`NewMsg` 通知邮件中的数据可以通知用户在其收件箱中有 7 个新的语音邮件和 4 个新的文本邮件。

有关按邮件类型发送通知的详细信息，请参见第 624 页中的 “22.3.3 特定邮件类型的通知”。

20.7.4 按邮件类型管理配额

为邮件类型设置配额时，应包含**配额根**中的值。配额根指定用户的配额。它可以针对特定的邮件类型和邮箱文件夹指定不同的配额，也可以指定应用到所有剩余邮件类型、文件夹和未按类型定义的邮件的默认配额。

有关设置和管理配额的完整信息，请参见第 547 页中的 “20.8.2 配额操作原理”。

20.7.4.1 设置邮件类型配额之前

在为邮件类型设置配额之前，您必须配置以下参数：

- 为每种邮件类型设置 `store.messagetype.`*x*`.quotaroot` 参数。有关详细信息，请参见第 539 页中的 “配置邮件类型”。
- 将 `store.typequota.enable` 参数设置为 `on`。

  例如，输入以下命令：

  ```
  configutil -o store.typequota.enable -v 1
  ```

20.7.4.2 设置邮件类型配额的方法

使用以下方法之一为邮件类型设置配额：

- 使用 LDAP 属性 `mailQuota` 和/或 `mailMsgQuota` 为用户设置邮件类型配额。

  有关如何使用这些属性设置配额根的信息，请参见《Sun Java Communications Suite 5 Schema Reference》中的第 3 章 “Messaging Server and Calendar Server Attributes”中的 `mailQuota` 和 `mailMsgQuota` 条目。
- 设置默认的邮件类型配额，当未设置 `mailQuota` 和 `mailMsgQuota` 属性时，此默认值将应用于所有单个用户。

  要设置默认配额，请使用 `store.defaultmessagequota` 和/或 `store.defaultmailboxquota` 参数。

有关如何使用这些参数设置配额根的信息，请参见第 550 页中的 “20.8.4 配置消息存储配额” 。

使用上述 configutil 参数或 LDAP 属性为邮件类型设置配额时，您必须使用 store.messagetype.*x*.quotaroot 参数指定的配额根。

20.7.4.3 邮件类型配额根示例

本节中说明的示例为用户 joe 设置以下配额：

- 默认的邮箱存储配额为 40 M
- 默认的邮箱邮件配额为 5000
- Archive 文件夹的存储配额为 100 M
- 文本邮件类型的存储配额为 10 M
- 文本邮件类型的邮件配额为 2000
- 语音邮件类型的存储配额为 10 M
- 语音邮件类型的邮件配额为 200

该配额根允许 Archive 文件夹的存储配额 (100 M) 比所有其他文件夹和邮件类型的总存储配额 (60 M) 大。另外，Archive 文件夹没有邮件限制；在本例中，归档只有存储限制。

邮件类型既有存储配额又有邮件数量配额。

邮件类型配额适用于所有这些类型的邮件之和，无论它们是存储在 Archive 文件夹还是任何其他文件夹中。

对于所有非文本或非语音邮件类型且未存储在 Archive 文件夹中的邮件，将应用默认的邮箱配额。也就是说，邮件类型配额和 Archive 配额不记为默认邮箱配额的一部分。

要在本例中设置配额根，应该执行以下步骤：

1. 将 store.messagetype.*x*.quotaroot 参数配置如下：

```
store.messagetype.1.quotaroot = text

store.messagetype.2.quotaroot = voice
```

2. 将用户 joe 的 mailQuota 属性配置如下：

```
mailQuota: 20M;#text%10M;#voice%10M;Archive%100M
```

3. 将用户 joe 的 mailMsgQuota 属性配置如下：

```
mailMsgQuota: 5000;#text%2000;#voice%200
```

当运行 getquotaroot IMAP 命令时，得到的 IMAP 会话显示用户 joe 邮箱的所有配额根，如下所示：

```
1 getquotaroot INBOX
* QUOTAROOT INBOX user/joe user/joe/#text user/joe/#voice
* QUOTA user/joe (STORAGE 12340 20480 MESSAGE 148 5000)
* QUOTA user/joe/#text (STORAGE 1966 10240 MESSAGE 92 2000)
* QUOTA user/joe/#voice (STORAGE 7050 10240 MESSAGE 24 200)

2 getquotaroot Archive
* QUOTAROOT user/joe/Archive user/joe/#text user/joe/#voice
* QUOTA user/joe/Archive (STORAGE 35424 102400)
* QUOTA user/joe/#text (STORAGE 1966 10240 MESSAGE 92 2000)

* QUOTA user/joe/#voice (STORAGE 7050 10240 MESSAGE 24 200)
```

20.7.5 按邮件类型制定邮件过期规则

过期和清除功能允许您根据过期规则中定义的条件，将邮件从一个文件夹移动到另一个文件夹、归档邮件，以及从消息存储中删除邮件。可以使用 `imexpire` 实用程序执行这些任务。

`imexpire` 实用程序由管理员运行，因此不受强制配额的限制。

有关如何编写过期规则和使用 `imexpire` 实用程序的信息，请参见第 554 页中的 “20.9 设置自动删除邮件（过期和清除）功能”。

您可以编写过期规则使不同类型的邮件根据不同的条件过期。

过期功能非常灵活，为设置过期条件提供了许多选择。本节将介绍一个示例，其中文本邮件和语音邮件将根据不同的条件过期。

该示例假设您已经将文本邮件和语音邮件配置如下：

```
store.messagetype.1 = text/plain

store.messagetype.2 = multipart/voice-message
```

同时假设将消息存储配置为读取 Content-Type 标题字段来确定邮件类型。

示例 20–3 不同邮件类型的过期规则示例

```
TextInbox.folderpattern: user/%/INBOX
TextInbox.messageheader.Content-Type: text/plain
TextInbox.messagedays: 365
TextInbox.action: fileinto:Archive


VoiceInbox.folderpattern: user/%/INBOX
VoiceInbox.messageheader.Content-Type: multipart/voice-message
```

示例 20–3 不同邮件类型的过期规则示例 （续）

```
VoiceInbox.savedays: 14
VoiceInbox.action: fileinto:OldMail

VoiceOldMail.folderpattern: user/%/OldMail
VoiceOldMail.messageheader.Content-Type: multipart/voice-message
VoiceOldMail.savedays: 30
VoiceOldMail.action: fileinto:Trash

Trash.folderpattern: user/%/Trash
Trash.savedays: 7
Trash.action: discard
```

在本例中，文本邮件和语音邮件以不同的方式过期，它们遵守不同的时间安排，如下所示：

- 文本邮件在到达消息存储一年后，将从用户收件箱移动到用户的 Archive 文件夹。
- 语音邮件在两周后将从收件箱移动到 OldMail 文件夹。如果用户保存语音邮件，保存的日期将被重置，邮件将在新日期的两周后被移走。
- 语音邮件在 30 天后将从 OldMail 文件夹移动到 Trash 文件夹。用户也可以在 OldMail 文件夹中保存语音邮件，这将使邮件在新的保存日期上再推迟 30 天后才会被移走。
- 所有类型的邮件在移动到 Trash 文件夹 7 天后将被放弃。

  过期规则自动将语音邮件移动到 Trash。当用户删除文本邮件时它们将移动到 Trash。

注意：`savedays` 规则使邮件在保存指定天数之后过期。在典型的语音邮件系统中，用户可以在语音邮件菜单中保存语音邮件。对于文本邮件，当它移动到一个文件夹时被保存。`messagedays` 规则使邮件在第一次到达消息存储指定的天数之后过期，无论它存储在哪个文件夹或被移动了多少次。

20.8 关于消息存储配额

随着电子邮件和语音邮件的发展，IMAP 邮箱可以变得很大。消息存储配额限制（或**配额**）表示一个用户或域可以保留的磁盘空间大小或邮件数，它针对特定的文件夹或者特定的邮件类型。配额用于限制或减少消息存储的使用。本节包含有关以下内容的信息：

有关详细信息，请参见第 569 页中的 “20.11.4 监视配额限制”。

20.8.1 配额概述

可以为特定的用户或域设置配额，也可以根据邮件数或字节数设置配额。还可以为特定文件夹和邮件类型设置配额。邮件类型配额允许您为邮件类型指定限制。例如，语音邮件和电子邮件。文件夹配额设置用户文件夹的大小限制，以字节或邮件数为单位。例如，可以对 Trash 文件夹设置配额。Messaging Server 允许您为域和用户设置默认配额或自定义配额。

设置配额后，即可配置超过或接近配额时系统响应用户或域的方式。一种响应方式是向用户发送一个超过**配额通知**。超过配额时的另一种响应方式是停止向消息存储传送邮件。这叫做**强制配额**，通常发生在指定的**宽限期**之后。宽限期是邮箱在强制发生前可以超出配额的时间。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 554 页中的 “20.8.4.5 设置宽限期”。）
- 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 243 页中的 “10.10.4.3 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。

用户删除或擦除邮件，或者服务器根据已建立的过期策略删除邮件时，磁盘空间将变为可用（请参见第 554 页中的 “20.9 设置自动删除邮件（过期和清除）功能”）。

20.8.1.1 电话学应用程序服务器的异常

为支持统一的邮件服务要求，Messaging Server 提供了覆盖由消息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。这种用法的适用范围很小，但可以用于电话学应用程序。有关配置 TAS 通道的详细信息，请联系 Sun 邮件服务代表。

按邮件类型配额对于使用统一邮件服务的电话学应用程序非常有用。例如，如果在用户的邮箱中存储了一个混合邮件（如文本和语音邮件），那么管理员可以对不同类型的邮件设置不同的配额。用户的电子邮件可以有一个配额，语音邮件可以有一个不同的配额。

20.8.2 配额操作原理

将配额属性添加到 LDAP 用户和域条目可以指定自定义的用户和域配额。配额默认值、通知策略、强制配额和宽限期是在 `configutil` 参数中或通过使用 `imquotacheck` 实用程序指定的。

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。对于用户，配额是指所有用户文件夹中的所有累积字节或邮件数。对于域，配额是指特定域中所有用户的所有累积字节或邮件数。对于邮件类型，配额是指该邮件类型的所有累积字节或邮件数。对于文件夹，配额是指用户文件夹的所有累积字节或邮件数。

您可以为用户邮箱树指定以下配额值：

- 用户邮箱中特定文件夹的配额值。
- 特定邮件类型（如语音邮件或文本邮件）的配额值。（邮件类型配额应用于用户邮箱中所有文件夹中该类型的邮件。）
- 对用户邮箱中所有未明确分配配额的文件夹和邮件类型应用默认的配额值。

为一个用户分配多个配额值时适用以下原则：

- 配额不得重叠。例如，当存在特定邮件类型或文件夹的配额时，该类型的邮件或者该文件夹中的邮件不记入默认配额。每个邮件只能记入一个配额。
- 整个用户邮箱的总配额等于所有默认配额与按照类型和文件夹指定的配额值之和。
- 邮件类型配额优先于文件夹配额。例如，假设为用户的 `memos` 文件夹指定了一个配额，而为语音邮件指定了另一个配额。现在假设用户将 8 个语音邮件存储在 `memos` 文件夹中。这 8 个邮件将记入语音邮件配额，而不记入 `memos` 文件夹配额。

对配额属性和 `configutil` 参数做出的更改将自动生效，但不是立即生效，因为信息存储在缓存中，更改完全生效前需要花一点时间。Messaging Server 提供一个立即更新更改的命令，即《Sun Java System Messaging Server 6.3 Administration Reference》中的“iminitquota”。

`imquotacheck` 实用程序允许您根据分配的配额检查消息存储的使用情况。

20.8.3 消息存储配额属性和参数

本节列出主要的消息存储配额属性和 `configutil` 参数。目的在于提供功能接口的概述。有关这些属性和参数的详细信息，请参阅相应的参考文档。

下表列出了配额属性。请参阅《Sun Java Communications Suite 5 Schema Reference》。

表 20–6 消息存储配额属性

属性	说明
`mailQuota`	允许的用户邮箱磁盘空间的字节数。
`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。
`mailUserStatus`	邮件用户的状态。可能的值有 `active`、`inactive`、`deleted`、`hold` 和 `overquota`。

表 20–6 消息存储配额属性 （续）

属性	说明
`mailDomainDiskQuota`	域中所有邮箱可以使用的磁盘空间字节数。
`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）。
`mailDomainStatus`	邮件域的状态。值和默认值与 `mailUserStatus` 相同。

下表列出了配额参数。有关最新和最详细的信息，请参阅《Sun Java System Messaging Server 6.3 Administration Reference》中的第 3 章 “Messaging Server Configuration”。

表 20–7 消息存储 `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：OFF
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。在向客户端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。（默认值为当消息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`。
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 mailuserstatusLDAP 属性被设置为 overquota，因此 MTA 将不再接受任何邮件。默认值：off

消息存储配额还包括几个实用程序。《Sun Java System Messaging Server 6.3 Administration Reference》中的“iminitquota” 初始化配额设置。换句话说，配额属性和 `configutil` 参数在运行该命令后将自动生效。不运行该命令更改也可以生效，但不是立即生效，因为信息存储在缓存中，更改生效前需要花费一定的时间。

imquotacheck 实用程序允许您根据分配的配额检查消息存储的使用情况。

20.8.4 配置消息存储配额

本节介绍了以下任务：

20.8.4.1 指定默认用户配额

没有在 LDAP 条目中设置个人配额的用户将应用默认配额。该过程分为两个步骤：1) 指定用户默认配额 2) 指定哪些用户受默认配额限制。以下示例显示了如何设置默认用户配额。有关详细的参数信息，请参阅《Sun Java System Messaging Server 6.3 Administration Reference》中的第 3 章 “Messaging Server Configuration”。

要以邮件大小（以字节为单位）的形式指定默认的用户磁盘配额，请运行以下命令：

```
configutil -o store.defaultmailboxquota -v [ -1 | number ]
```

其中 -1 表示无配额（无限制邮件使用量）；*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（无限制邮件）；*number* 表示邮件数。

要为特定用户指定默认配额：

在使用默认消息存储配额的用户条目中将 mailQuota 属性设置为 -2。请注意，如果没有指定 mailQuota，将使用系统默认的配额。

20.8.4.2 指定单个用户配额

每个用户均可以有单独的配额。要设置特定于用户的配额，请在用户 LDAP 条目中设置《Sun Java Communications Suite 5 Schema Reference》中的“mailQuota”或者《Sun Java Communications Suite 5 Schema Reference》中的“mailMsgQuota”属性（有关完整的详细信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“configutil Parameters”）。下例显示了怎样设置用户配额。

要指定系统默认配额，不要向 LDAP 中添加 mailQuota 或将其设置为 –2。

要将配额设置为 1,000 封邮件，请将 mailMsgQuota 设置为 1000。

要将配额设置为 2 兆字节，请将 mailQuota 设置为 2M 或 2000000。

要将配额设置为 2 千兆字节，请将 mailQuota 设置为 2G 或 2000000000 或 2000M。

要指定 2 千兆字节的配额；20 兆字节的语音邮件配额；100 兆字节的 Archive 文件夹配额，请运行以下命令行：

```
mailQuota: 2G;#voice%20M;Archive%100M
```

2 千兆字节配额代表用户邮箱中所有没有明确分配配额的文件夹。在本例中，这不包括 Archive 文件夹中的邮件和**语音**类型的邮件。100 兆字节配额包括 Archive 文件夹所有子文件夹中的邮件。

20.8.4.3 指定域配额

您可以为域设置磁盘空间或邮件配额。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，请在所需的 LDAP 域条目中设置《Sun Java Communications Suite 5 Schema Reference》中的“mailDomainDiskQuota”或者《Sun Java Communications Suite 5 Schema Reference》中的“mailDomainMsgQuota” 属性。

要将配额设置为 1,000 封邮件，请将 mailDomainMsgQuota 设置为 1000。

要将配额设置为 2 兆字节，请将 mailDomainDiskQuota 设置为 2M 或 2000000。

要将配额设置为 2 千兆字节，请将 mailDomainDiskQuota 设置为 2G 或 2000000000 或 2000M。

▼ 设置配额通知

配额通知是指当用户接近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：

1 启用配额通知

运行以下命令行：

```
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。

2 定义配额警告邮件

警告邮件是指当用户快要超过磁盘配额时将向其发送的邮件。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 $$，然后是邮件正文。"$" 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 的转义符。）示例：

```
configutil -o store.quotaexceededmsg -v "Subject: WARNING: User quota
exceeded$$User quota threshold exceeded - reduce space used.'
```

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'
```

3 指定发送警告邮件的频率。

设置以下参数：

```
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。

4 指定配额阈值

配额阈值是指向客户端发出警告前超出配额的百分比。用户的磁盘使用量超出指定的阈值时，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。

对于其客户端支持 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。

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。

20.8.4.4 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。

启用或禁用强制配额：

```
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消息存储。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，也请检查以下参数：

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。

这些消息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。

20.8.4.5 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。宽限期不是邮件将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。（有关更多详细信息，请参见第 521 页中的 “20.1 概述” 。）宽限期从用户已达到配额阈值并被警告时开始。请参见第 551 页中的 “设置配额通知” 。

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。

20.8.4.6 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，不会被传送到消息存储），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。（默认值为当消息存储达到阈值时发送配额警告邮件。）此参数的默认值为 `Off`。

20.9 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消息存储中删除邮件。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、带有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、整个消息存储或特定分区
- 邮箱中的邮件数
- 邮箱总大小
- 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消息存储中保留的天数）
- 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 526 页中的 “20.3 消息存储如何删除邮件” 。

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。

- 第 555 页中的 “20.9.1 imexpire 操作原理”
- 第 555 页中的 “20.9.2 部署自动删除邮件功能”

20.9.1 imexpire 操作原理

可以从命令行调用 `imexpire`，或通过 `imsched` 守护进程安排其自动运行的时间。管理员在名为 `store.expirerule` 的文件中指定一组过期规则。该文件用来指定删除邮件的标准。可以有多个文件，其中属于同一规则范畴的文件将存储在同一目录中。即，普遍适用于整个消息存储的规则、适用于某个分区的规则、适用于用户的规则等等将分别存放在不同的目录中。

注 – 虽然可以使用 `configutil` 命令和 `store.expire.`*attribute* 参数指定全局过期规则，但最好使用 `store.expirerule` 指定这些规则。如果使用 `configutil` 创建的规则太多，可能会产生性能问题。

`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` 的文件中添加指定用户的用户 ID（每行一个），从过期规则中排除这些用户。

20.9.2 部署自动删除邮件功能

自动删除邮件需要三个步骤：

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、文件夹、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。定义要删除邮件的范围。请参见第 556 页中的 “20.9.2.1 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 556 页中的 “20.9.2.2 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 561 页中的 “20.9.2.3 安排自动删除邮件和日志记录级别” 。

20.9.2.1 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指定的所有其他条件一起使用。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。请注意，该属性只使用已修改的 UTF-7 字符集。

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。

20.9.2.2 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。可以通过将规则放入 store.expirerule 文件来设置规则。以下所示为两个全局 store.expirerule 规则的示例：

```
Rule1.regexp: 1
Rule1.folderpattern: user/.*/trash
Rule1.messagedays: 2
Rule2:regexp: 1
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 指定消息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 557 页中的 “过期规则原则”
- 第 560 页中的 “通过文本方式设置 imexpire 规则”
- 第 561 页中的 “设置 imexpire 文件夹模式”

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 6.3 Administration Reference》中的“configutil Parameters”）。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）。无论如何，使用 `store.expirerule` 指定所有过期规则是最佳的。

- 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消息存储（全局规则）、分区、用户或文件夹。
  - 全局规则存储于 *msg-svr-base*`/config/store.expirerule` 中

    注 – 系统将针对每个邮箱检查每种全局规则，这可能会造成一定的系统处理开销（取决于指定的全局规则数）。因此，不应在全局规则文件中指定分区、邮箱或用户规则。总之，除了必要规则外，尽量少把其他过期规则放置到该文件中。

  - 分区规则存储于 *store_root*`/partition/`*partition_name*`/store.expirerule` 中。
  - 用户规则在 *store_root*`/partition/`*partition_name*`/`*userid*`/store.expirerule` 中指定，或通过将 `folderpattern` 规则指定为 `user/`*userid*`/.*` 来指定。
  - 文件夹规则在 *store_root*`/partition/`*partition_name*`/`*userid*`/`*folder*`/store.expirerule` 中指定，或通过将 `folderpattern` 规则指定为 `user/`*userid*`/`*folder* 来指定。
  - 请注意，只在 Messaging Server 6.2p4 发行版及更高版本中实现了使用 *rule_name* 的多个非全局规则（用户、文件夹、分区）。
- 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 20–8）。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 20–8 imexpire 属性

属性	说明（属性值）
action	指定要对过期规则捕获的邮件执行的操作。可能的值有： discard 放弃邮件。该值为默认值。 report 操作向 stdout 打印邮件名称、uid 有效性和 uid。 archive 使用 Sun Compliance and Content Management System 归档邮件，然后放弃邮件。 fileinto:*folder* 操作将邮件放入指定的文件夹。共享的文件夹前缀可以用来将邮件放入属于另一个用户的文件夹。
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。(1/0)
folderpattern	指定此规则影响的文件夹。格式必须以 user/ 开始，表示目录 *store_root*/partition/*/。请参见表 20–9。（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）
messageheader.*header*	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。示例：Rule1.messageheader.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，将采用最早的过期日期。（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。
savedays	邮件被擦除前在文件夹中保存的天数。
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**并且**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)。
sieve	指定邮件选择条件的 Sieve 规则。示例：Rule17.sieve: header :contains "Subject" "Vigara"

表 20–8 imexpire 属性 （续）

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**并且**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**)

本地化的邮箱名称

IMAP 协议指定邮箱名称使用已修改的 UTF-7 编码。Messaging Server 在外部接口上支持本地化的字符集，从而可以本地化邮箱名称。但是，系统在内部将本地化的名称转换为 UTF-7。因此，客户端上具有本地化邮箱名称的文件夹有一个对应的 UTF-7 邮箱文件名称。（请注意，IMAP 错误邮件将以 UTF-7 而不是本地化字符集的形式输出邮箱名称。）

一般来说，尽管消息存储实用程序可能具有允许使用不同字符集的选项标志，但大部分需要邮箱名称的消息存储实用程序通常都希望使用本地化字符集的名称。这些实用程序有 reconstruct、mboxutil、imsbackup、imsrestore 和 hashdir。但是，imexpire 要求使用属性 folderpattern 指定的邮箱名称其字符集为 UTF-7。使用本地化名称将会无效。

要获取 imexpire 相应的 folderpattern，可能需要将本地化邮箱名称转换为等效的 UTF-7 邮箱名称。可以使用 mboxutil -E 命令进行此操作，如下所示：

```
$ mboxutil -l -p user/user1/*
msgs Kbytes last msg       partition quotaroot mailbox
 |
77     27     2006/9/9 3:21 primary   10240   user/kat/INBOX
0       0      -             - primary         -  user/kat/箱

$ mboxutil -l -E MUTF-7 -p user/user1/*
msgs Kbytes last msg       partition quotaroot mailbox

77     27     2006/9/9 3:21 primary   10240   user/kat/INBOX
0       0      -             - primary         -  user/kat/&V4NXPnux-
```

第一个 mboxutil 显示了本地化的文件名。第二个 mboxutil 显示了已修改的 UTF-7 文件名。这也可以使用以下 IMAP list 命令：

```
2 list "" *
* LIST (\NoInferiors) "/" INBOX
* LIST (\HasNoChildren) "/" &V4NXPnux-
```

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*

用户或邮箱规则配置文件的过期规则的格式如下：

attribute: *value*

示例 20–4 显示了 *msg-svr-base*`/config/store.expirerule` 中的一组全局过期规则。

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: 标题中带有 "Vigara Now!" 或 "XXX Porn!" 字符串的邮件。
- 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”

示例 20–4 `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: 1
Rule2.deleted: or
Rule2.messagedays: 14
Rule2.messagecount: 1000
Rule3.folderpattern: user/f.dostoevski/inboxRule3.Subject: *On-line Casino*
```

示例 20–4 imexpire 规则示例 （续）

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 20–9 显示了各种文件夹的文件夹模式。）

表 20–9 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/.*	将规则应用到整个消息存储。
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。

20.9.2.3 安排自动删除邮件和日志记录级别

通过 imsched 时间安排守护进程来激活自动删除邮件。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 20–10 中介绍的 configutil 参数 local.schedule.expire 和 store.cleanupage 自定义此时间安排。

对于大型消息存储，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 imexpire 命令和自动任务时间安排参数（请参见第 107 页中的 “4.6 安排自动任务时间”）安排过期和清除的时间。例如：

```
configutil -o local.schedule.expire -v "0 1 * * 6 /opt/SUNWmsgsr/sbin/imexpire -e"
configutil -o local.schedule.mspurge -v "0 23 * * * /opt/SUNWmsgsr/sbin/imexpire -c"
```

在本例中，邮件在星期六的凌晨 1 点过期，在每天夜里 11 点清除。如果没有设置清除的时间安排，imexpire 将在过期后执行清除操作。

表 20–10 过期和清除 configutil 日志和时间安排参数

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 和 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。
	请注意，您也可以对 imexpire 使用 -e 和 -c 标志分别只添加过期或只添加清除。请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“imexpire”。
	时间间隔示例：
	1) 在 12:30am、8:30am 和 4:30pm 运行 imexpire：
	`30 0,8,16 * * * /opt/SUNWmsgsr/sbin/imexpire`
	2) 在工作日早晨 3:15am 运行 imexpire：
	`15 3 * * 1-5 /opt/SUNWmsgsr/sbin/imexpire`
	3) 仅在星期一运行 imexpire：
	`0 0 * * 1 /opt/SUNWmsgsr/sbin/imexpire`
	默认值：
	`0 23 * * * /opt/SUNWmsgsr/sbin/imexpire`
	要进行禁用：请将 local.schedule.expire.enable 设置为 NO。

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
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

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 -d（调试）选项可以用于指示 imexpire 日志记录 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。或者，在用户邮箱下配置一个伪排外过期规则。

20.10 配置消息存储分区

邮箱存储在消息存储分区，即专门用于存储消息存储的磁盘分区的区域。虽然为了易于维护，我们建议每个消息存储分区使用一个磁盘分区和一个文件系统，但是消息存储分区与磁盘分区并不相同。消息存储分区是专门指定为消息存储的目录。

默认情况下，用户邮箱存储在 *store_root*/partition/ 目录中（请参见第 523 页中的“20.2 消息存储目录布局”）。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。

如果消息存储需要多个磁盘，则可以使用 RAID（Redundant Array of Inexpensive Disks，廉价磁盘冗余阵列）技术简化对多个磁盘的管理。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，消息存储和邮件队列应位于单独的磁盘上。

20.10.1 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，该名称是分区的昵称。

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消息存储时，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。

▼ 添加消息存储分区

- **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`**

20.10.2 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 563 页中的 “20.10.1 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。也可以将邮箱移到其他分区。

▼ 将邮箱移动到其它磁盘分区

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 Communications Suite 5 Schema Reference》中的“mailAllowedServiceAccess”。**

   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 **在已移动用户的 LDAP 条目中将 `mailMessageStore` 属性设置为新分区的名称。**

示例：`mailMessageStore: secondary`

4 **通知用户现在允许消息存储连接。如果可用，则更改 `mailAllowedServiceAccess` 属性以允许 POP、IMAP 和 HTTP 服务。**

20.10.3 更改默认消息存储分区定义

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（该属性指定用户的消息存储分区），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）。

20.11 执行消息存储维护过程

本节提供有关用于执行消息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 25 章。

本节包含以下内容：

20.11.1 给消息存储添加更多的物理磁盘

Messaging Server 消息存储包含特定 Messaging Server 实例的用户邮箱。消息存储的大小随邮箱、文件夹和日志文件的数量的增加而增加。

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，消息存储可能需要一个物理磁盘或多个物理磁盘。Messaging Server 使您可以根据需要添加更多存储。添加更多存储的一种方法是使用存储设备。有关如何使用 Messaging Server 配置 Network Appliance 存储设备的信息，请参见《Using NetApp Filers with Sun Java System Messaging Server Message Store》。

20.11.2 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`。

20.11.2.1 mboxutil 实用程序

使用 `mboxutil` 命令执行典型的邮箱维护任务。`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
- 擦除邮箱
- 恢复已擦除但尚未被清除的邮件
- 列出个人邮箱订阅和不再存在的取消订阅的邮箱
- 您还可以使用 `mboxutil` 命令查看有关配额的信息。有关详细信息，请参见第 569 页中的 “20.11.4 监视配额限制”。

注 – 请注意，不应在执行过程中中止 `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。

有关语法和使用要求的详细信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“mboxutil”。

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
```

20.11.2.2 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
```

20.11.2.3 hashdir 实用程序

消息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消息存储的目录。此实用程序将报告消息存储的相对路径，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
```

20.11.2.4 readership 实用程序

`readership` 实用程序将报告有多少用户（而不是邮箱拥有者）已经阅读了共享 IMAP 文件夹中的邮件。

IMAP 文件夹的拥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（而不是拥有者）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拥有者以外的阅读者。

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
```

20.11.3 邮箱最大大小

一个邮箱的最大大小可以容纳约一百万封邮件。超过此限制将导致邮件无法传送给用户，并且可能会导致消息存储库性能问题。有关详细信息，请参见第 598 页中的“20.14.4.7 由于邮箱溢出而无法传送邮件”。

20.11.4 监视配额限制

通过使用 imquotacheck 监视配额使用情况和限制，此实用程序生成一个报告，其中列出了已定义的配额和限制，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。此功能重复 mboxutil 实用程序中的搜索功能。

在 Messaging Server 6.x 中，此重复功能已从 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
```

要根据指定的 *rulefile*、*myrulefile* 和邮件模板文件 *mytemplate.file* 向所有用户发送通知，请运行以下命令（有关详细信息，请参阅《Sun Java System Messaging Server 6.3 Administration Reference》中的“imquotacheck”）：

```
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
```

20.11.5 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 773 页中的 “27.3.2 监视磁盘空间”。

20.11.6 stored 守护进程

stored 守护进程为消息存储执行以下维护任务：

- 执行检查点数据库事务.
- 死锁检测和死锁数据库事务的回滚。
- 启动时清除临时文件和锁定文件。
- 创建数据库快照归档。
- 根据需要恢复数据库（请参见第 589 页中的 “20.14.2 消息存储启动和恢复”）。

如果任一服务器守护进程崩溃，则必须停止所有守护进程并重新启动所有守护进程，包括 stored。

20.11.7 由于重复存储相同的邮件而减少消息存储大小

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。某些邮件服务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。

在将其他邮件服务系统迁移到 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。消息存储会很大，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，并使用指向单个副本的硬链接替换这些邮件副本。

20.11.7.1 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，它将扫描整个消息存储分区，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消息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 20–1）。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 20–4 中所示。

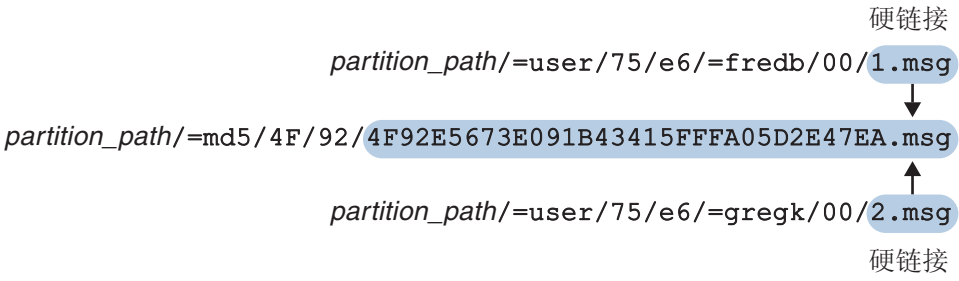


图 20–4 消息存储摘要系统信息库

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 572 页中的 “20.11.7.3 在实时模式下使用 relinker”。

20.11.7.2 在命令行模式中使用 relinker

relinker 将扫描整个消息存储分区，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 572 页中的 “20.11.7.4 配置 relinker”。例如，处理 100 千兆字节的消息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 572 页中的 “20.11.7.3 在实时模式下使用 relinker”。

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。

20.11.7.3 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 572 页中的 “20.11.7.4 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。

20.11.7.4 配置 relinker

表 20–11 显示了用于设置 relinker 条件的参数。

表 20–11 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。即使禁用此选项，relinker 命令行工具也可能运行。但是，由于 stored 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：no
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

20.12 备份并恢复消息存储

消息存储备份和恢复是最常见和最重要的管理任务之一。它由备份消息存储中的所有邮件和文件夹组成。必须实现消息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™）执行消息存储备份和恢复。

Messaging Server 提供了单副本备份过程。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 inode 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。有关详细信息，请参见第 578 页中的 “20.12.5 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消息存储备份和恢复。请参阅第 583 页中的 “20.12.9 消息存储灾难备份和恢复” 。

本节包含以下小节：

20.12.1 创建邮箱备份策略

备份策略取决于若干因素，例如：

20.12.1.1 高峰业务负载

安排系统备份时，需要考虑到高峰业务负载，因为这可以减少高峰时段的系统负载。例如，清晨时段（例如 2:00 AM）可能是安排备份的最佳时段。

20.12.1.2 完全备份和增量备份

增量备份（请参见第 576 页中的 “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消息存储。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。

20.12.1.3 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。

20.12.2 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消息存储目录（图 20–1），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 *msg-svr-base*/config/backup-groups.conf 配置文件中定义的。
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 的格式如下：

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/恢复整个消息存储：

```
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。

20.12.2.1 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
```

20.12.3 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 580 页中的 “20.12.6 使用 Legato Networker”。

20.12.3.1 imsbackup 实用程序

使用 imsbackup，可以将消息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。

以下示例将整个消息存储备份到 /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 575 页中的 “20.12.2 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 -f /dev/rmt/0 -d 20040501:131000 /
```

此命令使用默认块因子 20。有关 imsbackup 命令的完整语法描述，请参见《Sun Java System Messaging Server 6.3 Administration Reference》。

20.12.3.2 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 命令的完整语法描述，请参见《Sun Java System Messaging Server 6.3 Administration Reference》。

20.12.4 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。

20.12.5 部分恢复的注意事项

部分恢复是指仅恢复部分消息存储。完全恢复是指恢复整个消息存储。消息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消息存储的单副本特征。

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，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 inode 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` 将日志记录对象 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。

20.12.5.1 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消息存储服务器上的邮箱中：

- 在恢复操作期间，禁用邮件向用户传送。通过将 LDAP 属性 `mailDeliveryOption` 设置为 `hold` 来实现该操作。
- 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端将必须重新同步邮箱 UID 有效性标志和邮件 UID。客户端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，客户端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。

20.12.6 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。物理消息存储结构和数据格式封装在备份 API 中。备份 API 将直接与消息存储进行交互式操作。它显示了备份服务的消息存储的逻辑视图。备份服务使用消息存储的概念表示法来存储和检索备份对象。

Messaging Server 为备份和恢复消息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 (Application Specific Module, 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 消息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

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` 二进制文件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` 将被自动安装在 `/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 575 页中的 “ 20.12.2 创建备份组 ”中所述的备份组文件。**

   b. **要验证配置，运行 `mkbackupdir.sh`。**

      查看由 `mkbackupdir.sh` 创建的目录结构。该结构应该与表 20–4 中所示的目录结构相似。

      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 20–4。**

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，以下命令将在目录 `/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消息存储所有者（如：`mailsrv`）。

表 20–6 显示了样例备份组目录结构。

```
/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：

5 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”。

6 使用 `savepnpc` 作为备份命令创建备份客户端：

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 575 页中的 “20.12.2 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 580 页中的 “使用 Legato Networker 备份数据” 。

7 **选择“组控制”|“启动”以测试备份配置。**

示例：在 Networker 中创建备份客户端：

要在 Networker 中创建备份客户端，从 nwadmin 选择“客户端”|“客户端设置”|“创建”

```
Name: siroe
Group: IMS
Savesets:/backup/primary/groupA
   /backup/secondary/groupB
   /backup/tertiary/groupC
         .
         .
Backup Command:savepnpc
Parallelism: 4
```

20.12.6.1 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消息存储：

```
recover -a -f -s siroe /backup/siroe
```

20.12.7 使用除 Legato 以外其他的第三方备份软件

Messaging Server 提供了两种消息存储备份解决方案，命令行 imsbackup 和 Solstice Backup (Legato Networker)。运行单个 imbackup 备份整个消息存储的大型消息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。

▼ 使用除 Legato 以外其他的第三方备份软件

1 **将用户分成组（请参见第 575 页中的 “ 20.12.2 创建备份组 ”），并在 *msg-svr-base*/config/ 目录下创建 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，磁盘空间要求将是消息存储大小的两倍。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。**

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
```

20.12.8 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。

20.12.9 消息存储灾难备份和恢复

灾难是指整个消息存储而非一个邮箱或一组邮箱的灾难性故障。即消息存储服务器上的所有数据全部丢失的情况。完整的消息存储灾难恢复将包含恢复以下丢失的数据：

- 所有消息存储数据。可以使用第 573 页中的 “20.12 备份并恢复消息存储”中描述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：

- 所有消息存储分区
- 位于 msg-svr-base/data/store/mboxlist 的消息存储数据库文件。
- 位于 msg-svr-base/data/store/dbdata/snapshots 的消息存储数据库快照（请注意，可以使用 configutil 参数 local.store.snapshotpath 配置消息存储数据库快照文件的位置。）

- 配置数据。包括位于 msg-svr-base/data/config 的本地配置文件

如果您想备份消息存储供灾难恢复时使用，您可以使用文件系统快照工具备份一个文件系统快照。快照**必须**是**快速及时点** (point-in-time) 文件系统快照。否则，将无法使用 mboxlist 备份（mboxlist 数据库必须从完整的数据库快照恢复）。

最好在同一个快速及时点捕获所有数据（消息存储分区、数据库文件等等），但是，如果无法做到这一点，那么您必须按以下顺序备份数据：

1. 数据库快照
2. 数据库文件
3. 消息存储分区
4. 配置数据

如果消息存储分区和数据库文件没有使用同一个快速及时点快照备份，请在恢复文件系统快照后运行 reconstruct -m。这将同步数据库和存储分区。

20.13 监视用户访问

Messaging Server 提供了命令 imsconnutil，允许您通过 IMAP、POP 和 http 监视用户的消息存储访问。您还可以确定用户的上次登录和注销时间。此命令在每个消息存储的基础上运行，不能在多个消息存储之间运行。

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：mailsrv），并且必须将配置变量 local.imap.enableuserlist、local.http.enableuserlist、local.enablelastaccess 设置为 1。

要列出当前通过 IMAP 或任何 Web 邮件客户端登录的用户，请使用以下命令：

```
# imsconnutil -c
```

要列出消息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 连接的客户端登录（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*

请注意，`-k` 选项只有在已配置 IMAP IDLE 的情况下才起作用。有关 `imsconnutil` 语法的完整说明，请参阅《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsconnutil”。

下面是某个示例的输出：

```
$ ./imsconnutil -a -u soroork

UID     IMAP last access    HTTP last access    POP last access
================================================================================
ed   08/Jul/2003:10:49:05   10/Jul/2003:14:55:52  ---NOT-RECORDED---

$ ./imsconnutil -c

IMAP
UID    TIME                AUTH            TO                  FROM
================================================================================
ed   17/Jun/2003:11:24:03  plain     172.58.73.45:193   129.157.12.73:2631
bil  17/Jun/2003:04:28:43  plain     172.58.73.45:193   129.158.16.34:2340
mia  17/Jun/2003:09:36:54  plain     172.58.73.45:193   192.18.184.103:3744
jay  17/Jun/2003:05:38:46  plain     172.58.73.45:193   129.159.18.123:3687
pau  17/Jun/2003:12:23:28  plaintext 172.58.73.45:193   192.18.194.83:2943
ton  17/Jun/2003:05:38:46  plain     172.58.73.45:193   129.152.18.123:3688
ani  17/Jun/2003:12:26:40  plaintext 172.58.73.45:193   192.18.164.17:1767
ani  17/Jun/2003:12:25:17  plaintext 172.58.73.45:193   129.150.17.34:3117
jac  17/Jun/2003:12:26:32  plaintext 172.58.73.45:193   129.150.17.34:3119
ton  17/Jun/2003:12:25:32  plaintext 172.58.73.45:193   192.18.148.17:1764
================================================================================
10 users were logged in to imap.
Feature is not enabled for http.
--------------------------------------------------------------------------------
```

20.14 消息存储故障排除

本节提供主动维护消息存储的原则。此外，本节还介绍了当消息存储被破坏或者意外关闭时，可以使用的其他消息存储恢复过程。注意，有关这些附加消息存储恢复过程的部分是第 591 页中的 “20.14.3 修复邮箱和邮箱数据库”的延伸内容。

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：

20.14.1 标准消息存储监视过程

本节概述了消息存储的标准监视过程。这些过程有助于常规消息存储检查、测试和标准维护。

有关其他信息，请参见第 780 页中的 “27.7 监视消息存储”。

20.14.1.1 检查硬件空间

消息存储应具有足够的附加磁盘空间和硬件资源。消息存储接近磁盘空间和硬件空间的最大限度时，消息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消息存储的空间，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消息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 569 页中的 “20.11.5 监视磁盘空间”和第 780 页中的 “27.7 监视消息存储”。

20.14.1.2 检查日志文件

检查日志文件以确保消息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。您可以在目录 *msg-svr-bas*`/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 25 章。

20.14.1.3 使用自动测量功能检查用户 IMAP/POP/Webmail 会话

Messaging Server 提供了一种称为自动测量的功能，可以将用户的整个 IMAP、POP 或 HTTP 会话捕获到文件中。此功能对调试客户端问题很有用。例如，如果用户抱怨他们的邮件访问客户端未按预期那样工作，则此功能可用于跟踪访问客户端和 Messaging Server 之间的交互作用。

要捕获 POP 会话，请创建以下目录：

msg-svr-base/data/telemetry/ *pop_or_imap_or_http*/*userid*

要捕获 POP 会话，请创建以下目录：

msg-svr-base/data/telemetry/pop/ *userid*

要捕获 IMAP 会话，请创建以下目录：

msg-svr-base/data/telemetry/imap/ *userid*

要捕获 Webmail 会话，请创建以下目录：

msg-svr-base/data/telemetry/http/ *userid*

请注意，目录必须由邮件传送服务器 userid 拥有和重写。

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 flagged draft deleted \Seen $MDNSent Junk)
* OK [PERMANENTFLAGS (\Answered flag draft deleted \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>
```

要禁用自动测量日志记录，请移动或删除您创建的目录。

20.14.1.4 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 进程是否在运行。运行 imcheck
- 检查在 *store_root*/mboxlist 中生成的日志文件。
- 检查默认日志文件 *msg-svr-base*/log/default/default 中的 stored 邮件。
- 检查每当 stored 进程尝试以下功能之一时，以下文件（位于目录 *msg-svr-base*/config/ 中）的时间戳是否已更新：

表 20–12 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《Sun Java System Messaging Server 6.3 Administration Reference》中的第 570 页中的 “20.11.6 stored 守护进程” 一章。

有关监视 stored 功能的其他信息，请参见第 780 页中的 “27.7 监视消息存储”。

20.14.1.5 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。

20.14.1.6 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 591 页中的 “20.14.3 修复邮箱和邮箱数据库”。

20.14.1.7 检查主存文件

仅当进程已经意外终止时才会存在核心转储文件。查阅这些文件很重要，特别是在消息存储中发现问题时。在 Solaris 中，使用 coreadm 配置 core 文件位置。

20.14.2 消息存储启动和恢复

消息存储数据由邮件、索引数据和消息存储数据库组成。虽然此数据相当可靠，在极少时候系统中也可能出现消息存储数据问题。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 573 页中的 “20.12 备份并恢复消息存储”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。

消息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，消息存储守护进程 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 将彻底检查消息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，报告对消息存储完成的修复和使其运行的自动尝试。

20.14.2.1 自动启动和恢复—操作原理

stored 守护进程在其他消息存储进程之前启动。如果有必要，它将初始化并恢复消息存储数据库。消息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。

打开消息存储数据库前，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。请参见第 590 页中的 “表示需要 reconstruct 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 是否已被 “阻塞”。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 以便与消息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。即使消息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 用于调出消息存储，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 的错误消息

本节介绍需要运行 reconstruct 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”

“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”

“正在从快照恢复数据库。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已损坏的数据库。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。

消息存储数据库快照—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，快照将被复制到 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，并且是放入 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。仅当 removed 目录中的数据是一星期以前的数据时，才会替换副本。这将防止有问题的原始数据库由于连续启动而被替换得太快。

指定消息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 20–13 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 20–13 消息存储数据库快照参数

参数	说明
local.store.snapshotpath	消息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

20.14.3 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 590 页中的“表示需要 reconstruct 的错误消息”。

表 20–14 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 6.3 Administration Reference》中的“reconstruct”。

表 20–14 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	仅检查消息存储，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 选项和 -m 选项一起使用，用于限制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 需要对消息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 选项与 -m 选项一起使用，用于限制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。

20.14.3.1 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不一致性并重建。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，因为对于大型消息存储，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 594 页中的 "20.14.3.3 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
```

20.14.3.2 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 – 运行 reconstruct 时同时使用 -P 和 -m 标记将不能修复 lright.db。这是因为修复 lright.db 需要对消息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。

20.14.3.3 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
- 消息存储的总大小
- 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 的消息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` 花费大约 1 小时
- `reconstruct -r -f` 花费大约 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。

20.14.4 常见问题和解决方案

本节列出了常见的消息存储问题和解决方案：

20.14.4.1 Linux - Messaging Server Patch 120230-08 IMAP、POP 和 HTTP 服务器由于每个进程会话过多而未启动

安装该修补程序后，当您尝试启动 Messaging Server 时，IMAP、POP 和 HTTP 服务器无法启动，并可能发送以下示例错误日志：

```
http server - log:
[29/May/2006:17:44:37 +051800] usg197 httpd[6751]: General Critical: Not enough file
descriptors to support 6000 sessions per process; Recommend ulimit -n 12851 or 87
sessions per process.

pop server - log:
[29/May/2006:17:44:37 +051800] usg197 popd[6749]: General Critical: Not enough file
descriptors to support 600 sessions per process; Recommend ulimit -n 2651 or 58
sessions per process.

Once these values setting in /opt/sun/messaging/sbin/configutil then imap server
failed to start

imap server - log:
[29/May/2006:17:44:37 +051800] usg197 imapd[6747]: General Critical: Not enough
file descriptors to support 4000 sessions per process; Recommend ulimit -n 12851
or 58 sessions per process.
```

为所有三个服务器会话设置相应数目的文件描述符。通过向 /etc/sysctl.conf 添加类似以下代码的行并使用 sysctl -p 重读该文件，即可使用附加的文件描述符：

```
fs.file-max = 65536
```

还必须向 /etc/security/limits.conf 添加类似以下代码的行：

```
*   soft  nofile  65536
*   hard  nofile  65536
```

20.14.4.2 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。

20.14.4.3 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，如果未找到任何匹配项，则将失败。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。

20.14.4.4 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。

20.14.4.5 用户邮箱目录问题

当消息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/ 用户目录复制到消息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，则该文件夹可能不在 `folder.db` 中。

   如果使用 `reconstruct -r -n` 命令找不到该文件夹，请使用 `hashdir` 命令确定位置。有关 `hashdir` 的详细信息，请参见第 568 页中的 “20.11.2.3 hashdir 实用程序”，以及《Sun Java System Messaging Server 6.3 Administration Reference》的 "Messaging Server Command-line Utilities" 一章中的 `hashdir` 实用程序部分。
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消息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` 以确保消息存储的一致性。

有关 `reconstruct` 命令的详细信息，请参见第 591 页中的 “20.14.3 修复邮箱和邮箱数据库”。

20.14.4.6 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
```

这表示找不到 `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 `mailsrv` 添加到该组，将 *instance_root* 及其文件的拥有权更改为 `mailsrv` 和该组。

20.14.4.7 由于邮箱溢出而无法传送邮件

消息存储对 `store.idx` 文件设置了 2 千兆字节的硬性限制，这等效于在一个邮箱（文件夹）中可以存放一百万封邮件。当邮箱增长到 `store.idx` 文件将超过 2 千兆字节的那一点时，用户将停止接收任何新的电子邮件。此外，处理该邮箱的其他进程（如 mapd、popd、mshttpd）的性能也会降低。

如果出现该问题，您将在 `mail.log_current` 中看到如下错误：

```
05-Oct-2005 16:09:09.63 ims-ms Q 7 ...System I/O error.Administrator, check
server log for details.System I/O error.
```

此外，MTA 日志文件将出现如下错误：

```
[05/Oct/2005:16:09:09 +0900] jmail ims_master[20745]:Store Error:Unable to
append cache for user/admin:File too large
```

通过查看用户消息存储目录中的文件，或者在 `imta` 查看更详细的信息，您可以准确地确定该问题。

应立即着手减小文件的大小。可以删除一些邮件，或者将一些邮件移动到另一个邮箱。要解决此问题，您也可以使用 `mboxutil -r` 重命名该文件夹，或者使用 `mboxutil -d` 删除该文件夹（请参见第 566 页中的 “20.11.2.1 mboxutil 实用程序”）。

从长远来看，您应该向用户通知邮箱大小限制、实现生存期策略（请参见第 554 页中的 “20.9 设置自动删除邮件（过期和清除）功能”）和配额策略（请参见第 546 页中的 “20.8 关于消息存储配额”）、通过设置 `local.store.maxmessages` 来设置邮箱限制（请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“configutil Parameters”）、建立归档系统，或者执行某些操作来控制邮箱大小。

20.15 将邮箱迁移或移动到新系统

有时必须将现有邮箱从一个 Messaging Server 系统移动到另一个 Messaging Server 系统中。这通常发生于以下情况：

- 从非 Sun Messaging Server 迁移到 Sun Java System Messaging Server
- 将邮箱从一个物理服务器移动到另一个物理服务器

Messaging Server 提供了若干种将邮箱从一个系统移动到另一个系统的方法。每种方法都有它的优点和缺点，这将在以下小节中进行说明。下面的小节介绍了这些方法：

- 第 599 页中的 “20.15.1 在联机状态下将用户邮箱迁移到其他 Messaging Server”
- 第 600 页中的 “在保持联机状态下将用户邮箱从一个 Messaging Server 迁移到另一个 Messaging Server 中”
- 第 604 页中的 “使用 IMAP 客户端移动邮箱”
- 第 605 页中的 “使用 `moveuser` 命令移动邮箱”
- 第 606 页中的 “使用 `imsimport` 命令移动邮箱”

20.15.1 在联机状态下将用户邮箱迁移到其他 Messaging Server

可以使用此过程将消息存储从旧版本的 Messaging Server 迁移到较新版本的 Messaging Server，也可以将邮箱从一个 Sun Messaging Server 消息存储移动到另一个 Sun Messaging Server 消息存储。此过程适用于 iPlanet Messaging Server 5.0 和更高版本。不能使用此过程从早期版本的 Messaging Server 或非 Sun Microsystems 消息存储中移动邮件。

使用此过程移动邮箱的优点如下所示：

- 无需用户参与，系统管理员即可将邮箱从旧的源系统移动到新的目标系统。
- 此过程比任何其他过程都快。
- 如果要移动整个分区，则不需要进行重新链接。
- 两个 Messaging Server 系统都处于活动和联机状态。
- 您可以迁移消息存储上的所有邮箱或这些邮件的某个子集。此过程可以实现增量迁移。

使用此过程移动邮箱的缺点如下所示：

- 此方法不适用于非 Sun 邮件服务器。
- 所迁移的用户在自己的邮箱完成迁移之前，将无法访问这些邮箱。
- 此方法可能很复杂且费时。

20.15.1.1 增量邮箱迁移

增量迁移具有许多优点，可以安全有效地将消息存储移动到其他系统中或升级到新系统；增量迁移允许在保留旧后端消息存储的同时构建新的后端消息存储系统。您可以随后测试新系统，迁移一些友好用户，然后再次测试新系统。在适应了新系统、新配置和迁移过程之后，即可开始迁移实际的商业用户。可以将这些用户分成单独的备份组，这样在迁移过程中，只有此组的成员在短时间内处于脱机状态。

联机增量迁移的另一个优点是，不必在升级失败时规划系统范围的回退。回退是用于恢复对系统所做更改的过程，以便将系统恢复到原始工作状态。进行迁移时，您必须针对故障进行规划，这意味着必须对迁移中的每个步骤进行规划，以便将系统恢复到先前的工作状态。

脱机迁移的问题是，在完成所有迁移步骤并重新启用服务之前，无法确定迁移是否成功。如果系统出现故障且无法立即修复，则需要回退所有已执行的步骤。这可能会给您带来压力，并且需要花费一些时间，而在这段时间内用户仍处于脱机状态。

使用联机增量迁移时，您需要执行以下基本步骤：

1. 构建与旧系统并存的新系统，以使两个系统可以独立运行。

2. 配置旧系统，使之与新系统并存。

3. 迁移一组友好用户，并测试新系统及其与旧系统的并存情况。

4. 对旧系统上的用户进行分组，并根据需要将这些组逐个迁移到新系统中。

5. 对旧系统进行反汇编。

由于两个系统将会并存，因此在迁移到新系统之前，您将有时间来测试和适应新系统。如果必须执行回退过程（这种可能性很小），则只需对步骤 2 和 步骤 4 进行规划。由于未涉及到用户数据，因此步骤 2 很容易恢复。在步骤 4 中，回退过程会将用户状态恢复为活动状态，并将其 mailhost 属性恢复为旧主机。不必执行系统范围的回退。

20.15.1.2 联机迁移概述

在联机状态下迁移邮箱的过程非常简单。但要确保在迁移过程中传输到邮箱的邮件（在 MTA 通道队列中等待传送）不会丢失，则情况会比较复杂。一种解决方案是，以 *held* 状态保留迁移过程中发送的邮件，并等待各个通道队列中的邮件传送出去。但是，邮件可能会由于系统问题或特定用户超过配额而阻塞在队列中。在这种情况下，您必须在迁移邮箱之前解决此问题。

您可以采取各种措施来降低邮件丢失的可能性，并确保邮件不会阻塞在通道队列中，但这些措施会使迁移过程变得更加复杂。

此过程中的步骤的顺序和必要性会有所不同，具体取决于部署以及是否不允许丢失发送到每个邮箱的每封邮件。本节介绍了与这些步骤相关的理论和概念。您必须了解每个步骤，并根据您的特定部署来确定要执行的步骤以及执行顺序。以下是对移动邮箱过程的概述。此过程可能会根据部署的不同而有所不同。

1. 阻止用户访问要移动的邮箱。
2. 暂时保留发送到要移动的邮箱的邮件。
3. 确保邮件未阻塞在通道队列中。
4. 将用户的 mailhost 属性更改为新的邮箱位置。
5. 将邮箱移动到新位置。
6. 释放所保留的邮件，以便将其传送到新邮箱，并使外来邮件能够传送到已迁移的邮箱。
7. 检查旧的消息存储，以查看在迁移后是否将邮件传送到此存储中。
8. 取消阻止用户对邮箱的访问。

▼ 在保持联机状态下将用户邮箱从一个 Messaging Server 迁移到另一个 Messaging Server 中

开始之前 此类型迁移的要求如下所示：

- `stored` 应同时在源（旧）邮件服务器和目标（新）邮件服务器上运行。
- 如果源系统和目标系统并存运行，则这两种系统必须能够互相发送邮件。这一点很有必要，举例来说，如果能够互相发送邮件，即可在目标系统上生成传送状态通知邮件，然后将其传送到源系统。

注 – 某些步骤只有在将邮件服务器从早期版本升级到较高版本时才适用。如果只是将邮箱从一个消息存储迁移到另一个消息存储，则这些步骤可能不适用。适用于迁移整个系统的步骤将会特别指出。

1. **在源系统中，使用 `backup-groups.conf` 文件将要移动的用户条目分为均等的备份组。**

   此步骤是邮箱迁移（将在此过程后面执行的步骤 8）的准备过程。有关详细说明，请参见第 575 页中的 “20.12.2 创建备份组”。

   也可以将用户名置于文件中，然后在 `imsbackup` 命令中使用 `-u` 选项。

2. **通知要移动的用户在移动完成之前无法访问他们的邮箱。**

   确保要移动的用户在数据移动之前已从邮件系统注销。（请参见第 584 页中的 “20.13 监视用户访问”。）

3. **在后端消息存储和 MMP 系统上将验证缓存超时设置为 0，并在 MTA 上将 `ALIAS_ENTRY_CACHE_TIMEOUT` 选项设置为 0。**

   a. **在包含要移动的邮箱的后端消息存储上，将验证缓存超时设置为 0。**

      ```
      configutil -o service.authcachettl -v 0
      ```

      此步骤和步骤 7（将 `mailUserStatus` 更改为 `hold`）将立即阻止用户在迁移期间访问其邮箱。

   b. **在所有 MMP 上，将 LDAP 和验证缓存超时设置为 0。**

      在 `ImapProxyAService.cfg` 和 `PopProxyAService.cfg` 中，将 `LdapCacheTTL` 和 `AuthCacheTTL` 设置为 0。

   c. **在托管 MTA（可将邮件插入到要迁移的邮箱中）的任意 Messaging Server 上，将 `ALIAS_ENTRY_CACHE_TIMEOUT` 选项设置为 0。**

      托管 MTA（可将邮件插入到要迁移的邮箱中）的 Messaging Server 通常是后端消息存储。但是，如果系统使用的是 LMTP，则此系统将是入站 MTA。检查配置以确保正确无误。

      重置 */msg_svr_base* `/config/option.dat` 中的 `ALIAS_ENTRY_CACHE_TIMEOUT` 可以强制 MTA 避开缓存而直接查看 LDAP 条目，从而使中间通道队列（例如，`conversion` 或 `reprocess` 通道）可以查看所移动用户的新 `mailUserStatus (hold)`，而不是过期的缓存信息。`ALIAS_ENTRY_CACHE_TIMEOUT` 位于 `option.dat` 中。

   d. **重新启动重置了缓存的系统。**

      必须重新启动系统以使上述更改生效。有关说明，请参见第 102 页中的 “4.4 启动和停止服务”。

4 **确保源 Messaging Server 和目标 Messaging Server 已启动并且正在运行。**

源 Messaging Server 必须能够将外来邮件路由到新的目标服务器。

5 **将要移动邮箱的所有用户条目的 LDAP 属性 `mailUserStatus` 由 `active` 更改为 `hold`。**

更改此属性可以使外来邮件保留在 `hold` 队列中，并可防止通过 IMAP、POP 和 HTTP 访问邮箱。通常以用户组的形式移动用户。如果移动单个域的所有邮箱，则可以使用 `mailDomainStatus` 属性。

有关 `mailUserStatus` 的更多信息，请参见《Sun Java Communications Suite 5 Schema Reference》中的“mailUserStatus”。

6 **确保发送到迁移邮箱的邮件未阻塞在 `ims-ms` 或 `tcp_lmtp*` 通道队列中（如果已部署 LMTP）。**

使用以下命令查看发送到迁移用户的邮件是否存在于通道队列目录树中，并且处于 *held* 状态（查看 `.HELD` 文件）：

```
imsimta qm directory -to=<user_address_to_be_migrated> -directory_tree

imsimta qm directory -to=<user_address_to_be_migrated> -held -directory_tree
```

如果此队列中有邮件，请在稍后运行相同命令来查看 MTA 是否已将这些邮件移出队列。如果有未移出队列的邮件，则必须在迁移之前解决此问题。这种问题很少发生，但可能的原因有以下几点：收件人邮箱超过配额、邮箱被锁定（可能由于用户已登录并且正在移动邮件）、LMTP 后端服务器未响应、网络或名称服务器问题等等。

7 **更改要移动的用户条目以及任何邮件组条目中的 LDAP 属性 `mailHost*`。**

使用 `ldapmodify` 命令将条目更改为新的邮件服务器。使用 Messaging Server 或目录服务器附带的 `ldapmodify`。不要使用 Solaris 操作系统的 `ldapmodify` 命令。

* 如果关闭了旧邮件主机，则只需更改邮件组条目中的 `mailHost` 属性。可以将此属性更改为新的邮件主机名，也可以干脆删除此属性。对于邮件组而言，`mailHost` 是可选的。具有 `mailHost` 意味着只有该主机可以进行组扩展；而忽略 `mailHost`（此种情况较为常见）则意味着所有 MTA 都可以进行组扩展。请注意，邮件组条目不包含要迁移的邮箱，通常甚至没有 `mailhost` 属性。

有关 `mailhost` 的更多信息，请参见《Sun Java Communications Suite 5 Schema Reference》中的“mailHost”。

8 **将邮箱数据从源 Messaging Server 消息存储移动到目标 Messaging Server 消息存储，并记录开始时间。**

使用 `imsbackup` 实用程序备份邮箱，并使用 `imsrestore` 实用程序将其恢复到新的 Messaging Server 中。例如，要将邮箱从名为 `oldmail.siroe.com` 的 Messaging Server 5.2 系统迁移到 `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- -c y -v 1
```

您可以运行多个并发的备份和恢复会话（每组一个），以使传送到新消息存储的速率达到最大化。有关 imsbackup 和 imsrestore 实用程序以及第 573 页中的 “20.12 备份并恢复消息存储”的更多信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“Command Descriptions”。

注 – 记录 imsbackup 开始运行的时间戳，用于以后的传送验证。

---

9 （系统升级的条件式步骤）如果邮箱迁移是升级（从早期版本的 Messaging Server 升级到当前版本）过程的一部分，请将当前版本的 Messaging Server 设置为新的系统默认 Messaging Server。

将 oldmail.siroe.com 的 DNS A 记录更改为指向 newmail.siroe.com（此服务器负责先前托管在 oldmail.siroe.com 上的域）。

10 启用用户对新消息存储的访问。

如果适用，将 LDAP 属性 mailUserStatus 或 mailDomainStatus 设置为将其更改为 hold 之前的任意值（如 active）。

11 释放所有源 Messaging Server 上处于 *held* 状态的邮件。

任何可能保留外来邮件的系统都需要运行以下命令，以释放所有用户邮件：

```
imsimta qm release -channel=hold -scope
```

其中，*scope* 可以是 all（释放所有邮件）、user（用户 ID）或 domain（用户所在的域）。

12 将验证缓存超时和 ALIAS_ENTRY_CACHE_TIMEOUT 选项重置为默认值或所需值，然后重新启动系统。

此时，您已经迁移了需要迁移的所有用户邮箱。在继续操作之前，请确保 LDAP 中没有使用旧系统作为 mailhost 创建的新条目；如果有，请迁移这些条目。此外，还要确保无法通过修改置备系统来创建此类条目。

还要将 preferredmailhost 属性更改为新邮件主机的名称。

对于后端消息存储，请将验证缓存超时设置为以下值：

```
configutil -o service.authcachettl -v 900
```

对于 MMP，请在 ImapProxyAService.cfg 和 PopProxyAService.cfg 中将 LdapCacheTTL 和 AuthCacheTTL 选项设置为 900。

对于 MTA，请将 ALIAS_ENTRY_CACHE_TIMEOUT 选项设置为 600。ALIAS_ENTRY_CACHE_TIMEOUT 位于 option.dat 中。

必须重新启动系统以使上述更改生效。有关说明，请参见第 102 页中的 “4.4 启动和停止服务”。

13 确保用户客户端将指向新的邮件服务器。

升级完成后，通过用户的邮件客户端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`）。

一种替代方法是使用邮件多路复用器 (MMP)，这样用户可以不必将其客户端直接指向新的邮件服务器。MMP 将从 `mailHost` 属性（存储在 LDAP 用户条目中）获取该信息，并自动将客户端重定向到新服务器。

14 一切正常运行之后，请验证在迁移后没有向旧消息存储中传送任何邮件。

转到旧消息存储并运行 `mboxutil -l` 以列出邮箱。检查最后的邮件传送时间戳。如果在迁移时间戳（运行 `imsbackup` 命令时的日期戳）之后传送了邮件，请使用备份和恢复命令迁移这些邮件。由于提供了准备步骤，因此在迁移后极少会出现传送邮件的情况。

在理论上，邮件可能会在队列中阻塞一段时间，由 `notices` 通道关键字指定天数和小时数（请参见第 243 页中的 “10.10.4.3 设置通知邮件传送间隔”）。

15 删除新消息存储上的重复邮件，然后运行 `relinker` 命令。

此命令可以释放新消息存储上的磁盘空间。请参见第 570 页中的 “20.11.7 由于重复存储相同的邮件而减少消息存储大小”。

16 从迁移的源存储中删除旧邮件，然后从旧存储上的数据库中删除用户。

运行 `mboxutil -d` 命令。（请参见第 566 页中的 “20.11.2.1 mboxutil 实用程序”。）

▼ 使用 IMAP 客户端移动邮箱

无论何时需要将邮件从一个邮件服务器迁移到其他邮件服务器，都可以使用此过程。使用此方法移动邮箱之前，请考虑该方法的优缺点。

使用 IMAP 客户端移动邮箱的优点如下所示：

- 此方法可用于从非 Sun Messaging Server 到 Sun Java System Messaging Server 的迁移。还可以用于将邮箱从一个物理服务器移动到其他物理服务器。
- 系统管理员设置新邮件服务器或消息存储之后，将由用户负责将邮箱移动到新系统。
- 移动邮箱的过程相对简单。
- 不必禁用用户对邮箱的访问。

使用 IMAP 客户端移动邮箱的缺点如下所示：

- 需要新旧系统同时运行，并且可由用户访问。
- 使用此方法移动邮箱所累计花费的时间比使用其他方法长。
- 用户负责将邮箱移动到新系统。
- 执行重新链接操作之前，新消息存储的大小将明显大于旧消息存储。

1. **安装并配置新 Messaging Server。**

2. **将 `local.store.relinker` 设置为启用。**

   这样可以减小重复存储相同的邮件而增加的新系统上的消息存储大小。有关更多信息，请参见第 570 页中的 “20.11.7 由于重复存储相同的邮件而减少消息存储大小”。

3. **在新 Messaging Server 上置备用户。**

   您可以使用 Delegated Administrator 执行此操作。在新系统上置备用户后，新到达的邮件将被立即传送到新的收件箱。

4. **让用户配置其邮件客户端以查看新旧 Messaging Server 邮箱。**

   这可能涉及客户端上新电子邮件帐户的设置。有关详细信息，请参见邮件客户端文档。

5. **指导用户将文件夹从其旧 Messaging Server 拖到其新 Messaging Server。**

6. **验证用户是否已将所有邮箱迁移到新系统，然后关闭旧系统上的用户帐户。**

▼ 使用 `moveuser` 命令移动邮箱

无论何时需要将邮件从一个邮件服务器迁移到其他邮件服务器，都可以使用此过程。将 IMAP 邮箱从非 Sun Messaging Server 迁移到 Sun Java System Messaging Server 时，此过程非常有用。使用此方法移动邮箱之前，请考虑该方法的优缺点。

使用 `moveuser` 命令移动邮箱的优点如下所示：

- 将邮箱从旧系统移动到新系统的工作完全由系统管理员负责。用户不必进行任何操作。
- 适用于所有 IMAP 服务器。

使用 `moveuser` 命令移动邮箱的缺点如下所示：

- 需要新旧系统同时运行，并且可由用户访问。
- 与其他非 IMAP 方法相比，使用此方法移动邮箱花费的时间较多。
- 移动邮箱时必须禁用用户对邮箱的访问。
- 执行重新链接操作之前，新消息存储的大小将明显大于旧消息存储。

1. **安装并配置新 Messaging Server。**

2. **将 `local.store.relinker` 设置为启用。**

   这样可以减小重复存储相同的邮件而增加的新系统上的消息存储大小。有关更多信息，请参见第 570 页中的 “20.11.7 由于重复存储相同的邮件而减少消息存储大小”。

3 **停止向邮件服务器传入邮件。**

将用户属性 `mailUserStatus` 设置为 `hold`。

4 **如果需要，在新 Messaging Server 上置备用户。**

如果从以前版本的邮件服务器迁移，则可以使用同一 LDAP 目录和服务器。`moveuser` 可以更改每个用户条目中的 `mailhost` 属性。

5 **运行 `moveuser` 命令。**

要根据 Directory Server `siroe.com` 中的帐户信息将所有用户从 `host1` 移动到 `host2`，请执行以下命令：

```
MoveUser -l \
"ldap://siroe.com:389/o=siroe.com???(mailhost=host1.domain.com)" \
-D "cn=Directory Manager" -w password -s host1 -x admin \
-p password -d host2 -a admin -v password
```

有关 `moveuser` 命令的详细信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“MoveUser”。

6 **启用用户对新邮件服务存储的访问。**

将 LDAP 属性 `mailUserStatus` 设置为 `active`。

7 **关闭旧系统。**

▼ 使用 `imsimport` 命令移动邮箱

此过程专用于将邮箱从 UNIX `/var/mail` 格式文件夹移动到 Sun Java System Messaging Server 消息存储。但是，如果您正在从中迁移的邮件服务器可以将 IMAP 消息存储转换为 UNIX `/var/mail` 格式，则可以使用 `imsimport` 命令将邮件迁移到 Sun Java System Messaging Server。使用此方法移动邮箱之前，请考虑该方法的优缺点。

使用 `imsimport` 命令移动邮箱的优点如下所示：

- 将邮箱从旧系统移动到新系统的工作完全由系统管理员负责。用户不必进行任何操作。

使用 `imsimport` 命令移动邮箱的缺点如下所示：

- 与其他非 IMAP 方法相比，使用此方法移动邮箱花费的时间较多。
- 移动邮箱时必须禁用用户对邮箱的访问。
- 执行重新链接操作之前，新消息存储的大小将明显大于旧消息存储。

1 **安装并配置新 Messaging Server。**

2 **将 `local.store.relinker` 设置为启用。**

这样可以减小重复存储相同的邮件而增加的新系统上的消息存储大小。有关更多信息，请参见第 570 页中的 “20.11.7 由于重复存储相同的邮件而减少消息存储大小”。

3 **如果需要，在新 Messaging Server 上置备用户。**

您可以使用 Delegated Administrator 执行此操作。现在还不要切换至新系统。

4 **禁用用户对新旧邮件服务存储的访问。**

将 `mailUserStatus` LDAP 属性设置为 `hold`。用户的邮件将被发送到 hold 队列中并且不允许通过 IMAP、POP 和 HTTP 访问邮箱。存储服务器上的 MTA 和 Message Access Server 必须符合此要求。该设置将覆盖所有其他 `mailDeliveryOption` 设置。

5 **如果现有邮件服务器的邮件存储还不是 `/var/mail` 格式，请将其转换为 `/var/mail` 文件。**

请参见第三方邮件服务器文档。

6 **运行 `imsimport` 命令。**

例如：

```
imsimport -s /var/mail/joe -d INBOX -u joe
```

有关 `imsimport` 命令的详细信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimport”。

7 **启用用户对消息存储的访问。**

将 LDAP 属性 `mailUserStatus` 设置为 `active`。

8 **启用用户对新邮件服务存储的访问。**

9 **关闭旧系统。**

◆ ◆ ◆ 第 21 章

21 邮件归档

本章介绍 Messaging Server 的归档概念。这里不提供如何建立归档系统的说明。有关部署说明的详细信息，请参阅《Message Archiving Using the Sun Compliance and Content Management Solution》。将部署信息放在单独的文档中是为了更快的更新配置。

本章包含以下几个部分：

21.1 归档概述

邮件归档系统在与 Messaging Server 分离的系统上保存所有或指定的外来和外发邮件。可以在归档系统中保存和检索发送的邮件、接收的邮件、删除的邮件和移动的邮件。电子邮件用户无法修改或删除归档邮件，因此维护了外来和外发邮件的完整性。邮件归档不仅对于法规遵从性记录的保存很有用，对于消息存储管理也很有用。例如，一些客户可能会使用归档执行邮件备份，或者将旧邮件从花费较大的消息存储器中移动到花费较小的归档存储器中。

可以通过单独的归档软件 GUI 客户端或 Messaging Server 来访问归档邮件。如果从 Messaging Server 中删除了邮件，则可以使用归档客户端来搜索或检索那些被删除的邮件，因为归档邮件是不会被删除的。但请注意，归档邮件并不存储在邮箱文件夹中，因为邮箱文件夹位于 Messaging Server。

也可以设置系统，使其可以从 Messaging Server 中访问归档邮件。例如，您可以设置系统将 2 年以上的邮件归档。邮件正文不是驻留在消息存储中，而是驻留在归档系统中。从用户的角度来看，这些邮件似乎与常规的电子邮件没什么不同。将显示相同的标题和主题信息（这仍然存储在消息存储存储器中），但消息存储可以在需要时从归档服务器下载邮件正文。因此，在从归档服务器下载邮件时，会稍有延迟。此外，无法从电子邮件客户端中搜索归档的邮件。搜索必须通过归档 GUI 完成。

21.1.1 邮件归档系统：法规遵从性归档和操作性归档

有两种归档类型：法规遵从性归档和操作性归档。当您有法定义务维护严格的可检索电子邮件记录保存时，应使用法规遵从性归档。进入 MTA 的选定电子邮件（通过用户、域、通道、外来外发邮件等进行选择）在被传送到消息存储或 Internet 之前，将被复制到归档系统中。可以将归档设置为在过滤垃圾邮件和病毒之前或之后发生。

操作性归档用于邮件管理。例如：

- 通过将较少使用的（旧的）邮件移动到存储开销较低的归档系统中，来减少 Messaging Server 消息存储上的存储使用量。
- 作为数据备份的替代方法。

请注意，法规遵从性归档和操作性归档并不是互相排斥的。也就是说，您可以将系统设置为同时进行法规遵从性归档和操作性归档。

◆ ◆ ◆ 第 22 章

22 配置 JMQ 通知插件为 Message Queue 生成邮件

本章介绍了如何配置 JMQ 通知插件以生成 Message Queue 服务中客户端使用的邮件。

本章包含以下各节：第 22 章

22.1 JMQ 通知概述

Messaging Server 通知插件允许您向邮件传送服务或事件服务传送通知邮件。邮件传送服务将通知发送给使用方（客户端界面），使用方将邮件过滤并传送给指定的用户。

例如，当新电子邮件到达用户的邮箱时，通知插件向邮件传送服务传送一个通知邮件。邮件使用方（即邮件传送服务的一个组件）收到通知并将其发送到用户的电子邮件客户端（如 Communications Express 或 Mozilla Mail）。然后，电子邮件客户端将在用户的计算机屏幕上显示一个弹出消息：“您收到一封新邮件。”

另一个示例：如果用户的邮箱超过了其配额，通知插件将生成超过配额的通知邮件。邮件使用方向用户和需要得知该事件的管理员发送警告。

22.1.1 两种邮件传送服务通知

可以配置 Messaging Server 向两种不同的邮件传送服务传送通知：

- Sun Java System Message Queue 3.6 2005Q4
- Event Notification Service

Message Queue 服务可以实现 Java Messaging Service (JMS) 规范，它提供了邮件代理、用于创建生成或使用邮件的客户端的界面，以及管理服务和控制。在路由和传送功能、协议和邮件格式方面，Message Queue 遵循 JMS 标准。

Event Notification Service 是一个与 Messaging Server 和 Sun Java System Calendar Server 捆绑在一起的组件。它是一个专用服务，使用发布/订阅体系结构来发送和接收事件通知。

您可以为 Message Queue、Event Notification Service 或这两种服务配置通知生成方。

注 – 本章仅介绍如何为 Message Queue 配置通知。

有关 Event Notification Service 的信息，请参见 *Sun Java System Communications Suite Event Notification Service Guide*。

22.1.2 通知插件

要使 Messaging Server 能够为 Message Queue 或 Event Notification Service 生成通知，您必须为该服务配置插件：

- JMQ 通知插件允许您向 Message Queue 代理传送通知邮件。
- iBiff 插件允许您向 Event Notification Service 发布通知事件。

有关如何装入 iBiff 插件和配置 Event Notification Service 的信息，请参见 *Sun Java System Messaging Server* **管理指南**中的“附录 B：在 Messaging Server 中管理 Event Notification Service”。

22.1.3 使用 JMQ 通知的优点

用于 Message Queue 的 JMQ 通知插件具有以下优点：

- Message Queue 实现了 JMS 标准。
- 用于 Message Queue 时，您可以向**主题**或/和**队列**传送方法生成邮件。有关其简短定义，请参见第 613 页中的 “22.1.3.1 发布到主题或队列”。
- Message Queue 在邮件分发期间，尤其在为队列生成邮件时，提供了增强的负载平衡功能。
- JMQ 通知插件允许您最多配置 5 个通知插件。不同的插件可以为主题、队列、Event Notification Service 等生成邮件。有关详细信息，请参见第 613 页中的 “22.1.3.2 使用多个 JMQ 通知插件”。
- Message Queue 提供可靠的通知传送。

  例如，如果您配置 JMQ 通知插件生成邮件时启用了持久性标志，邮件将留在 Message Queue 代理中直到使用方接收到它。邮件被保存起来，如果服务器发生故障，可以重新检索到该邮件并供相应的使用方使用。

22.1.3.1 发布到主题或队列

主题和队列使用不同的邮件传送分发模式；这两种模式都可以在 Message Queue 服务中配置。

主题。邮件生成方将邮件发送到主题时，将使用发布/订阅体系结构。在这种广播模式中，生成方向主题目标发送邮件。任意数量的使用方可以订阅此主题目标。每个订阅此主题的使用方将得到其自身的邮件副本。如果没有使用方订阅此主题，则放弃此邮件。

Event Notification Service 也使用发布/订阅体系结构；它与 Message Queue 中定义的主题模式类似。

队列。当邮件生成方将邮件发送到队列时，使用的是点对点的体系结构。在这种模式中，生成方将邮件发送到队列目的地，只有一个使用方可以从中接收到邮件。如果几个使用方都在等待来自此队列的邮件，则只有一个订户会收到邮件。如果没有使用方在等待，邮件将被保留直到邮件超时或者使用方表示对队列感兴趣。

向队列生成邮件允许您在多个使用方之间分散邮件负载。

22.1.3.2 使用多个 JMQ 通知插件

您可以配置 1 到 5 个通知插件。

Messaging Server 在以下默认位置提供了一个插件库：

```
/opt/SUNWmsgsr/lib/libjmqnotify
```

使用 `configutil` 实用程序为插件指定参数并将插件指向可执行代码的库。

如果您指定了多个插件，则每个插件将独立于其他插件生成通知邮件。例如，如果两个插件配置了 delete-message 参数并且从用户的邮箱删除了邮件，则两个插件都将生成一个通知邮件。

通过配置多个插件，您可以根据不同的目的使用不同的邮件分发模式。例如，您可以配置三个不同的插件生成邮件

- 到队列（使用 Message Queue）
- 到主题（使用 Message Queue）
- 到 Event Notification Service

22.1.3.3 为通知插件配置参数

对于您配置的每一个插件，您都必须定义一组单独的 `configutil` 参数。

这些参数决定两种信息：

- 要生成的通知邮件的种类。例如，启用 `LogUser` 参数导致只要用户登录或注销就会发送通知邮件。

- Message Queue 需要的配置信息。例如，`jmqHost` 参数标识运行 Message Queue 代理的主机的 IP 地址。

有关如何配置插件的说明，请参见第 615 页中的 “配置 JMQ 通知插件”。

22.2 配置 JMQ 通知服务

此节简要介绍了如何使 JMQ 通知插件适合完整的 Message Queue 服务环境。然后，它提供了有关配置 JMQ 通知插件的详细说明。

22.2.1 规划您的 JMQ 通知服务

JMQ 通知插件只是 Message Queue 服务的一部分。邮件传送服务还包括使用邮件的客户端和 Message Queue 基础设施（代理、管理组件等等）。

以下步骤介绍了创建支持 Messaging Server 的 Message Queue 服务应该执行的任务：

1. **设计通知邮件服务。**

   定义 Messaging Server 安装需要的通知邮件。邮件服务开发周期的规划和设计阶段不在本章讨论的范围内。但是，在配置 JMQ 通知插件之前您应回答以下设计问题：

   - 您需要为哪些邮件事件生成通知？有关可用的通知邮件列表，请参见第 622 页中的 “22.3.1 通知邮件”。
   - 您打算为队列、主题，还是这两者生成邮件？
   - 您打算使用专用 Event Notification Service 和 Message Queue 服务吗？

   这些问题的答案将帮助您决定是配置一个还是多个通知插件，以及决定如何配置每个插件。

2. **安装、配置和部署 Message Queue 产品。**

   有关安装 Message Queue 的信息，请参见《*Sun Java System Message Queue Installation Guide*》。

   有关配置和部署 Message Queue 的信息，请参见《*Sun Java System Message Queue* **管理指南**》。

3. **编写一个或多个将要使用 JMQ 通知邮件的 Message Queue 客户端。**

   这些客户端必须符合 Message Queue 客户端 API 的要求。可以从以下路径获得一个客户端源代码的简单示例（用 C 语言编写）：

   ```
   /opt/SUNWmsgsr/examples/jmqsdk/
   ```

   源文件名为 `jmqclient.c`。

   此客户端源代码接收 JMQ 通知邮件（由 `libjmqnotify` 库中的参数定义）中的邮件。然后，它将邮件发送到 `stdout`。

有关用 C 或 Java 编写 Message Queue 客户端的信息，请参见 *Sun Java System Message Queue Developer's Guide for C Clients* 或 *Sun Java System Message Queue Developer's Guide for Java Clients*。

4. **配置并启用 JMQ 通知插件以生成通知邮件。**

   本章的剩余部分介绍如何配置通知插件。

5. **配置并启动运行时 Message Queue 客户端。**

   有关部署运行时 Message Queue 客户端的信息，请参见《 *Sun Java System Message Queue* **管理指南** 》。

▼ 配置 JMQ 通知插件

在这一过程中，您首先配置要生成通知的邮件事件。接下来，指定 Message Queue 需要的信息。最后（步骤 9），通过在插件库名称后指定一个参数来配置插件名称：

```
'/opt/SUNWmsgsr/lib/libjmqnotify$plug-in_name'
```

如果没有指定插件名称，则默认使用 `jmqnotify`。

开始之前 您应该安装、配置和部署以下产品：

- Sun Java System Messaging Server
- Sun Java System Message Queue 3.6 SP3 2005Q4 或更高版本

注 – 以下步骤中将要配置的大部分 `configutil` 参数是可选的。有关参数默认值列表，请参见表 22–2。

---

1 **配置通知邮件参数。**

对于每一种想要包含在插件内的通知邮件，请结合使用 `local.store.notifyplugin` 命令和 `configutil` 实用程序。

例如，要为新邮件启用通知，输入：

```
configutil -o local.store.notifyplugin.jmqnotify.NewMsg.enable -v 1
```

其中 *jmqnotify* 是插件的名称

而 `-v 1` 为此邮件启用通知。值为 `0` 将禁用对此邮件的通知。

有关所有 JMQ 通知邮件的列表，请参见第 622 页中的 “22.3.1 通知邮件” 。

有关启用 JMQ 通知邮件的 `configutil` 参数的定义，请参见 *Sun Java System Messaging Server Administration Reference* 中的第 3 章 "Messaging Server Configuration"。

有些通知邮件使用多个 `configutil` 参数启用具有附加功能的邮件。例如，有些邮件可以在通知文本中包含邮件标题。有关如何配置这些邮件的说明，请参见第 630 页中的 “newflags 和 oldflags 属性的语法” 。

注 – 您必须为每个配置的插件单独配置参数。

因此，如果配置两个插件（名为 `jmq1` 和 `jmq2`），并且希望为两个插件启用新邮件通知，则必须运行 `local.store.notifyplugin` 命令两次：

```
configutil -o local.store.notifyplugin.jmq1.NewMsg.enable -v 1

configutil -o local.store.notifyplugin.jmq2.NewMsg.enable -v 1
```

2. **指定运行 Message Queue 目标（代理）的主机。**
   例如，输入以下命令：
   ```
   configutil -o local.store.notifyplugin.jmqnotify.jmqHost -v "127.0.0.1"
   ```
   其中 *jmqnotify* 是插件的名称
   而 `"127.0.0.1"` 是 Message Queue 代理主机的 IP 地址。

3. **指定 Message Queue 代理的端口。**
   例如，输入以下命令：
   ```
   configutil -o local.store.notifyplugin.jmqnotify.jmqPort -v "7676"
   ```
   其中 *jmqnotify* 是插件的名称
   而 `"7676"` 是为 Message Queue 代理指定的端口。

4. **指定授权为服务生成邮件的 Message Queue 用户的用户 ID 和密码。**
   例如，输入以下命令：
   ```
   configutil -o local.store.notifyplugin.jmqnotify.jmqUser -v "guest"

   configutil -o local.store.notifyplugin.jmqnotify.jmqPwd -v "%$#a62t&"
   ```
   其中 *jmqnotify* 是插件的名称
   而 `"guest"` 和 `"%$#a62t&"` 分别是 Message Queue 用户的用户 ID 和密码。

5. **配置目的地（主题或队列）类型和邮件将要发送到的目的地的名称。**
   按以下步骤操作：

   a. **指定目标是主题还是队列。**
      例如，输入以下命令：
      ```
      configutil -o local.store.notifyplugin.jmqnotify.DestinationType -v "queue"
      ```
      其中 *jmqnotify* 是插件的名称
      而 `"queue"` 指定目标是一个队列。此参数允许的值是 `"queue"` 和 `"topic"`。

b. 指定目标名称。

例如，输入以下命令之一：

```
configutil -o local.store.notifyplugin.jmqnotify.jmqQueue -v "JES-MS"
```

或

```
configutil -o local.store.notifyplugin.jmqnotify.jmqTopic -v "JES-MS"
```

其中 *jmqnotify* 是插件的名称

`jmqQueue` 或 `jmqTopic` 标识目标类型。`jmqQueue` 和 `jmqTopic` 参数是同义的并且相互排斥；在一个插件中只能使用这两个参数中的一个。

`"JES-MS"` 是邮件将要发送到的队列或主题的示例名。

6 指定邮件优先级。

例如，输入以下命令：

```
configutil -o local.store.notifyplugin.jmqnotify.Priority -v 3
```

其中 *jmqnotify* 是插件的名称

而 `-v 3` 是指定给此插件生成的邮件的 Message Queue 优先级。

`Priority` 的默认值为 4。

7 指定 Message Queue 代理保留邮件的时间长度（以毫秒为单位）。

例如，输入以下命令：

```
configutil -o local.store.notifyplugin.jmqnotify.ttl -v 100
```

其中 *jmqnotify* 是插件的名称

而 `-v 100` 指定在发送或放弃某个邮件之前，Message Queue 服务保留邮件 100 毫秒。值为 0 表示邮件永久被保留；不会超时。

8 指定邮件持久性。

例如，输入以下命令：

```
configutil -o local.store.notifyplugin.jmqnotify.Persistent -v 1
```

其中 *jmqnotify* 是插件的名称

而 `-v 1` 指定在 Message Queue 服务中使用持久性邮件。允许的值为 1（持久）和 0（非持久）。

9 配置插件名称。

要配置具有默认名称的单个插件，可以输入插件库的全限定名称或者库名称及其插件参数：

```
configutil -o local.store.notifyplugin -v /opt/SUNWmsgsr/lib/libjmqnotify
```

或

```
configutil -o local.store.notifyplugin -v '/opt/SUNWmsgsr/lib/libjmqnotify$jmqnotify'
```

其中 libjmqnotify 是库名称，

而 jmqnotify 是插件参数的默认名称。

使用美元符号 ($) 分隔库名称和参数。

将整个值用单引号引起来（'**值**'）；否则 shell 将解释美元符号。

默认插件读取的 configutil 参数有以下名称：

```
local.store.notifyplugin.jmqnotify.*
```

要配置其他插件名称（如 jmq42），请输入以下命令：

```
configutil -o local.store.notifyplugin -v '/opt/SUNWmsgsr/lib/libjmqnotify$jmq42'
```

jmq42 插件读取的 configutil 参数有以下名称：

```
local.store.notifyplugin.jmq42.*
```

▼ 配置多个插件

1 **为打算创建的每个插件配置一组单独的 JMQ 通知参数。**

例如，假设您配置了两个插件，名为 jmq1 和 jmq2。假设您想为这两个插件都启用新邮件通知，同时单独为 jmq2 插件启用清除邮件通知。在这种情况下，要运行 local.store.notifyplugin 命令三次，如下所示：

```
configutil -o local.store.notifyplugin.jmq1.NewMsg.enable -v 1

configutil -o local.store.notifyplugin.jmq2.NewMsg.enable -v 1

configutil -o local.store.notifyplugin.jmq2.PurgeMsg.enable -v 1
```

您还必须指定使插件能够与 Message Queue 服务通信的参数。

有关配置所有通知参数的逐步说明，请参见第 615 页中的 “配置 JMQ 通知插件”。

2 **配置插件名称。**

要配置两个名为 jmq1 和 jmq2 的插件，请输入以下命令：

```
configutil -o local.store.notifyplugin
-v '/opt/SUNWmsgsr/lib/libjmqnotify$jmq1$$/opt/SUNWmsgsr/ \
lib/libjmqnotify$jmq2'
```

在本示例中，运行了两个插件库实例。

使用美元符号 ($) 分隔库名称和指定插件名称的参数。

使用两个美元符号 ($$) 分隔第一个插件实例和第二个插件实例。

将整个值用单引号引起来（'**值**'）；否则 shell 将解释美元符号。

在本示例中，第一个实例用名为 `jmq1` 的参数构建其配置：

```
local.store.notify.jmq1.*
```

第二个实例用名为 `jmq2` 的参数构建其配置：

```
local.store.notify.jmq2.*
```

22.2.2 使用多个 configutil 参数指定通知邮件

对于大部分通知邮件，您可以通过运行单个 `local.store.notifyplugin` 命令指定邮件。

但是，以下通知邮件使用（或可以使用）多个 `local.store.notifyplugin` 命令配置：

1. `NewMsg`
2. `UpdateMsg`
3. `DeleteMsg`
4. `MsgFlags`

以下过程介绍了如何设置这些通知邮件。

▼ 配置带有邮件标题和邮件正文的新邮件和更新邮件通知

有新的或更新的电子邮件时，您可以将邮件标题和邮件正文添加到发送的通知邮件文本。

可以选择包括邮件标题还是邮件正文；可以两个功能都包括、仅包括一个功能，或者都不包括。默认情况下发送不带邮件标题和邮件正文的邮件。

1 指定新邮件或更新邮件通知：

```
configutil -o local.store.notifyplugin.jmqnotify.NewMsg.enable -v 1

configutil -o local.store.notifyplugin.jmqnotify.UpdateMsg.enable -v 1
```

其中 *jmqnotify* 是插件的名称

而 `-v 1` 为这些邮件启用通知。值为 `0` 禁用通知。

2 用大于 0 的值指定 `maxHeaderSize` 参数，如下例所示：

```
configutil -o local.store.notifyplugin.jmqnotify.maxHeaderSize -v 1024
```

其中 *jmqnotify* 是插件的名称

而 1024 是要发送的邮件标题的最大大小。maxHeaderSize 的默认值为 0，表示不随邮件发送标题信息。

3 **用大于 0 的值指定 maxBodySize 参数，如下例所示：**

```
configutil -o local.store.notifyplugin.jmqnotify.maxBodySize -v 1024
```

其中 *jmqnotify* 是插件的名称

而 5120 是要发送的邮件正文的最大大小。maxBodySize 的默认值为 0，不随邮件发送正文信息。

▼ 配置带有邮件标题的删除邮件通知

在删除电子邮件消息时，您可以将邮件标题添加到发送的通知邮件文本中。

包含邮件标题是可选的。默认情况下发送不带邮件标题的通知。

1 **在删除电子邮件时发送通知：**

```
configutil -o local.store.notifyplugin.jmqnotify.DeleteMsg.enable -v 1
```

其中 *jmqnotify* 是插件的名称

而 -v 1 为此邮件启用通知。值为 0 禁用通知。

2 **指定 ExpungeHeaders 参数：**

```
configutil -o local.store.notifyplugin.jmqnotify.ExpungeHeaders -v 1
```

其中 *jmqnotify* 是插件的名称

而 -v 1 使删除邮件通知能够包含邮件标题。ExpungeHeaders 的默认值为 0，禁止删除邮件通知包含标题信息。

必须配置 ExpungeHeaders 参数启用 DeleteMsg 邮件包含邮件标题的功能。

3 **用大于 0 的值指定 maxHeaderSize 参数，如下例所示：**

```
configutil -o local.store.notifyplugin.jmqnotify.maxHeaderSize -v 1024
```

其中 *jmqnotify* 是插件的名称

而 1024 是要发送的邮件标题的最大大小。maxHeaderSize 的默认值为 0，表示不随邮件发送标题信息。

22.2.2.1 配置邮件状态更改通知

可以配置一个在电子邮件更改状态的时候发送的通知邮件。

在邮件标志通知中传送的信息

邮件标志通知在状态标志更改时生成，这种更改是因为电子邮件：

- 已回复
- 已标记
- 已删除
- 已读（已阅读）
- 存为草稿

发送邮件标志通知时，通知包含以下属性：

- 在电子邮件状态更改之前为其设置的标志
- 在电子邮件状态更改之后为其设置的标志

此信息包含在两个属性（`oldflags` 和 `newflags`）中，它们是包含 5 个字符的字符串。

有关这两个属性值的说明，请参见第 630 页中的 “newflags 和 oldflags 属性的语法”。

邮件标志通知所需的 configutil 参数

要启用邮件标志通知，必须配置以下 `configutil` 参数：

- `local.store.notifyplugin.MsgFlags`
- `local.store.notifyplugin.*.MsgFlags.enable`

第一个 `MsgFlags` 参数启用 IMAP 服务器和消息存储，以标识和跟踪状态标志更改的值，以便在通知邮件中传送此信息。

此参数应用于所有通知插件。因此，如果**任何**通知插件使用邮件标志通知，您必须启用此参数。如果没有插件使用邮件标志通知，请确保禁用此参数（其默认值）。

第二个参数 `*.MsgFlags.enable` 允许为某个特定的插件库发送邮件标志通知。

注 – 要为邮件标志启用通知，您必须两个参数都配置。

▼ 在邮件状态标志更改时启用通知

1 **跟踪状态标志并使邮件标志通知包含状态信息：**

```
configutil -o local.store.notifyplugin.MsgFlags -v 1
```

其中 `-v 1` 使邮件标志信息能够与邮件标志通知一起发送。值为 `0` 禁用此通知。

2 **使邮件标志通知由特定的插件发送：**

```
configutil -o local.store.notifyplugin.jmqnotify.MsgFlags.enable -v 1
```

其中 *jmqnotify* 是插件的名称

而 `-v 1` 为此插件启用邮件标志通知。值为 `0` 禁用通知。

22.3 JMQ 通知邮件和属性

本节介绍了以下主题：

22.3.1 通知邮件

可以为消息存储中发生的各种事件生成通知邮件。例如，用户登录时，可以生成 `Login` 邮件并发送到 Message Queue 代理。

`configutil` 参数指定每种生成的邮件。通过配置各种 `configutil` 参数，您可以决定哪些事件会生成邮件。`configutil` 参数可以被一个或多个 JMQ 通知插件库引用。

所有邮件都被传送到主题或队列，具体取决于将目标类型设置为 `"topic"` 还是 `"queue"`。有关如何配置 Message Queue 目标的信息，请参见第 615 页中的 “配置 JMQ 通知插件”。

每个邮件由以下邮件标题标识：

`MQ_MESSAGE_TYPE_HEADER_PROPERTY`

JMQ 通知插件支持的邮件如下表所示。

有关启用这些邮件的 `configutil` 参数列表，请参见第 625 页中的 “22.3.4 configutil 参数的默认值”。

表 22–1 JMQ 通知邮件

通知邮件	说明
`DeleteMsg`	从邮箱中删除标记为 “已删除” 的邮件。此操作等效于 IMAP 擦除。
`Login`	用户从 IMAP、HTTP 或 POP 登录。（用 `configutil` 参数 `local.store.notifyplugin.*.LogUser.enable` 启用此邮件。）
`Logout`	用户从 IMAP、HTTP 或 POP 注销。（用 `configutil` 参数 `local.store.notifyplugin.*.LogUser.enable` 启用此邮件。）

表 22–1 JMQ 通知邮件 （续）

通知邮件	说明
MsgFlags	邮件上的邮件标志已更改。新旧标志会包含在此邮件中。
NewMsg	系统收到新邮件并放入用户邮箱中。可以包含邮件标题和邮件正文。
OverQuota	由于用户邮箱超过某个配额（diskquota 或 msgquota）导致操作失败。MTA 通道会保留邮件直到配额更改或用户邮箱计数低于配额。如果邮件在 MTA 保留期间过期，将清除该邮件。
PurgeMsg	邮件被服务器进程 imexpire 从邮箱中清除（由于日期过期）。这是服务器端的清除，而 DeleteMsg 是客户端的清除。这并不是真正意义上的清除。
ReadMsg	邮箱中的邮件已阅读。（在 IMAP 协议中，邮件标记为 Seen。）
TrashMsg	被标记的邮件将被 IMAP 或 HTTP 删除。用户可能仍然会在文件夹中看到此邮件，具体取决于邮件客户端的配置。在执行清除时，邮件将从文件夹中删除。
UnderQuota	配额从 OverQuota 状态恢复到正常状态。
UpdateMsg	通过 IMAP 操作，将邮件附加到邮箱。例如，用户将一个电子邮件复制到邮箱。可以包含邮件标题和邮件正文。

22.3.2 通知邮件的规则和原则

以下规则和原则应用于支持的通知邮件：

- 大部分通知邮件的文本都是一个空白区。（使用空白区是因为 Message Queue 不允许邮件正文为空。）例外情况如下：
  - 在使用 maxHeaderSize 参数配置时，NewMsg、UpdateMsg 和 DeleteMsg 邮件可以包含邮件标题。您必须将 maxHeaderSize 设置为大于 0 的值。

    要使 DeleteMsg 邮件包含邮件标题，还必须将 ExpungeHeaders 参数的值设置为 1。
  - 在使用 maxBodySize 参数配置时，NewMsg 和 UpdateMsg 邮件可以包含邮件正文。您必须将 maxBodySize 设置为大于 0 的值。

    对于 NewMsg 和 UpdateMsg 而言，默认情况下不传送（关闭）邮件正文。这可以防止 Message Queue 过载。其他邮件都不包含邮件正文。
- 可以只为 INBOX 的更改生成通知邮件，也可以为 INBOX 和所有其他文件夹的更改生成通知邮件。以下配置参数允许只为 INBOX 生成（值 = 0），或为 INBOX 和所有其他文件夹生成（值 = 1）：

  ```
  local.store.notifyplugin.jmqnotify.noneInbox.enable
  ```

  默认设置是只从 INBOX 生成邮件（值 = 0）。

没有选择文件夹的机制；当此变量启用时包含所有文件夹（值 = 1）。

- 只有在邮件被置于用户邮箱后（而非“服务器接受它并将其放入邮件队列后”）才发出 NewMsg 通知。
- 不为 POP3 客户端访问生成邮件。
- 可以通过发出 XNOTNOTIFY 抑制所有邮件。例如，仅用于内务处理的 IMAP 脚本（不打算通知用户）可能会发出 XNOTNOTIFY 抑制所有邮件。

22.3.3 特定邮件类型的通知

通知可以传送关于各种不同类型的邮件（例如文本邮件、语音邮件和图像数据）的状态信息。用户经常希望这些不同种类的邮件类型存储在同一个邮件文件夹内。例如，用户可能希望新文本邮件和语音邮件都到达用户的手机收件箱。

要配置这些邮件类型，请使用 configutil 命令，例如 store.messagetype.enable。有关配置和管理邮件类型的信息，请参见“第 18 章：管理消息存储”中的“管理邮件类型”。

一旦配置了邮件类型，JMQ 通知邮件就能够标识特定邮件类型。您可以编写 Message Queue 客户端，使其能够按邮件类型解释通知邮件并向邮件客户端传送关于每个类型的状态信息。

例如，假设不同类型的新邮件到达用户的邮箱。NewMsg 通知邮件可以包含要通知用户的数据（例如，用户收件箱中有七个新语音邮件和四个新文本邮件）。

以下通知邮件可以包含跟踪特定邮件类型的信息：

```
NewMsg
UpdateMsg
ReadMsg
TrashMsg
DeleteMsg
PurgeMsg
OverQuota
UnderQuota
```

JMQ 通知功能可以按邮件类型统计邮箱中的当前邮件数。随通知邮件发送的是指定每种邮件类型计数的数组，而不是一个计数。

特定于邮件的计数包含在 numMsgs 属性中并随通知邮件一起传送。对于 ReadMsg 和 TrashMsg 通知邮件，已读邮件的数量 (numSeen) 和标记为已删除的邮件数量 (numDeleted) 也按邮件类型计数。

注 – Event Notification Service 不支持邮件类型。使用 JMQ 通知插件传送关于邮件类型的信息。

22.3.4 configutil 参数的默认值

用 configutil 参数配置 Message Queue 需要的通知邮件和配置信息。

表 22–2 显示了这些参数及其默认值。

有关 configutil 参数的完整定义，请参见 *Sun Java System Messaging Server Administration Reference* 中的第 3 章 "Messaging Server Configuration"。

表 22–2 configutil 参数及其默认值

configutil 参数	默认值
local.store.notifyplugin.*.maxBodySize	0 — 禁用
local.store.notifyplugin.*.maxHeaderSize	0 — 禁用
local.store.notifyplugin.*.NewMsg.enable	1 — 启用
local.store.notifyplugin.*.UpdateMsg.enable	1 — 启用
local.store.notifyplugin.*.ReadMsg.enable	1 — 启用
local.store.notifyplugin.*.DeleteMsg.enable	1 — 启用
local.store.notifyplugin.*.PurgeMsg.enable	1 — 启用
local.store.notifyplugin.*.LogUser.enable	1 — 启用
local.store.notifyplugin.*.MsgFlags.enable	0 — 禁用
local.store.notifyplugin.*.noneInBox.enable	0 — 禁用
local.store.notifyplugin.*.jmqHost	"127.0.0.1"
local.store.notifyplugin.*.jmqPort	7676
local.store.notifyplugin.*.jmqTopic	"JES-MS"
local.store.notifyplugin.*.jmqQueue	"JES-MS"
local.store.notifyplugin.*.jmqUser	"guest"
local.store.notifyplugin.*.jmqPwd	"guest"
local.store.notifyplugin.*.destinationtype	"topic"
local.store.notifyplugin.*.Priority	4

表 22–2 configutil 参数及其默认值 （续）

configutil 参数	默认值
local.store.notifyplugin.*.ttl	0 — 表示此邮件永不超时。
local.store.notifyplugin.*.Persistent	1 — 启用

22.3.5 通知邮件属性

每个邮件都包含属性中定义的附加信息。不同的属性出现在不同的邮件中。例如，NewMsg 表示新邮件的 IMAP uid。

22.3.5.1 标准通知邮件属性

表 22–3 介绍了标准通知邮件属性。这些属性出现在所有 JMS 邮件中。

表 22–3 标准通知邮件属性

属性	数据类型	说明
hostname	ConstMQString	生成此邮件的计算机的主机名。
pid	MQInt32	生成此邮件的进程的 ID。
process	ConstMQString	指定生成此邮件的进程的名称。
timestamp	MQFloat64	指定从 epoch（GMT 时间 1970 年 1 月 1 日午夜）开始的毫秒数。

22.3.5.2 特定于特定通知邮件的属性

表 22–4 描述了特定通知邮件包含的属性。

每个邮件包含下表中属性的一个子集。有关与每个邮件相关的属性列表，请参见表 22–5。

表 22–4 特定于特定通知邮件的属性

属性	数据类型	说明
client	ConstMQString	与邮件相关的 Message Queue 客户端 IP 地址。
diskquota	MQInt32	与邮件相关的用户磁盘空间配额，以千字节为单位。值设置为 -1 表示没有配额。
diskquotaused	MQInt32	与邮件相关的用户磁盘空间使用量，以千字节为单位。

表 22–4 特定于特定通知邮件的属性 （续）

属性	数据类型	说明
hdrLen	MQInt32	邮件标题大小。请注意，这可能不是邮件正文中标题的大小，因为此标题可能已经被截断。
imapUid	MQInt32	与邮件相关的 IMAP uid 属性。
lastUid	MQInt32	邮箱中使用的最后一个 IMAP uid 值。
mailboxName	ConstMQstring	与事件相关的消息存储邮箱名称。mailboxName 可以使用以下几种格式之一（其中 uid 是用户的唯一标识符）： uid — 标识默认（主）域中用户的收件箱。 uid@domain — 标识托管域中用户的收件箱。 uid/mailboxname — 标识默认域中用户的顶层邮箱。 uid@domain/mailboxname — 标识托管域中用户的顶层邮箱。 uid/foldername/mailboxname — 标识默认域中用户文件夹中的邮箱。 uid@domain/foldername/mailboxname — 标识托管域中用户文件夹中的邮箱。
msgquota	MQInt32	用户的最大邮件数配额。值设置为 -1 表示没有配额。
newflags	ConstMQString	用户的邮箱邮件被当前操作改变后设置的标志。在生成 MsgFlags 通知邮件时，此属性总是与 oldflags 一起出现。 有关 newflags 的语法和值，请参见此表下面的第 630 页中的 “newflags 和 oldflags 属性的语法”。
numDeleted	MQInt32	邮箱中标记为已删除的邮件数量。 此数值统计被邮箱所有者删除的邮件。如果其他用户访问此邮箱，他们在邮箱中的操作不包括在此计数内。（但是，其他用户的操作能够触发通知，如 DeleteMsg）。

表 22–4 特定于特定通知邮件的属性 （续）

属性	数据类型	说明
numDeleted*nn*	MQInt32	邮箱中为每种邮件类型指定的标记为已删除的邮件总数。如果配置了邮件类型， numDeleted*nn* 属性将包含每种邮件类型 *nn* 的计数。 始终发送 numDeleted 属性；它统计所有标记为已删除的邮件的总数，包括所有类型。 例如，如果 20 个邮件被标记为已删除，其中 10 个是类型 3，7 个是类型 16，而其余的不属于任何已识别的类型，则通知中包含以下属性和计数： numDeleted=20 numDeleted3=10 numDeleted16=7
numMsgs	MQInt32	邮箱中当前邮件总数。
numMsgs*nn*	MQInt32	邮箱中为每种邮件类型指定的当前邮件总数。如果配置了邮件类型， numMsgs*nn* 属性将包含每种邮件类型 *nn* 的计数。 始终发送 numMsgs 属性，它统计邮箱中所有邮件的总数，包括所有类型。 例如，如果邮箱中当前有 20 个邮件，其中 10 个是类型 3，7 个是类型 16，而其余的不属于任何已识别类型，则通知中包含以下属性和计数： numMsgs=20 numMsgs3=10 numMsgs16=7
numSeen	MQInt32	邮箱中标记为已读（已阅读）的邮件数。 此数值统计已被邮箱所有者阅读的邮件。如果其他用户访问此邮箱，他们在邮箱中的操作不包括在此计数内。（但是，其他用户的操作能够触发通知，如 ReadMsg）。

表 22–4 特定于特定通知邮件的属性 （续）

属性	数据类型	说明
numSeen*nn*	MQInt32	邮箱中为每种邮件类型指定的标记为已读（已阅读）的邮件总数。如果配置了邮件类型，numSeen *nn* 属性将包含每种邮件类型 *nn* 的计数。 始终发送 numSeen 属性；它统计邮箱中所有标记为已读的邮件的总数，包括所有类型。 例如，如果邮箱中有 20 个标记为已读的邮件，其中 10 个是类型 3，7 个是类型 16，而其余的不属于任何已识别类型，则通知中包含以下属性和计数： numSeen=20 numSeen3=10 numSeen16=7
numSeenDeleted	MQInt32	邮箱中标记为已读（已阅读）和已删除的邮件数。 此数值统计已被邮箱所有者标记为已阅读和已删除的邮件。如果其他用户访问此邮箱，他们在邮箱中的操作不包括在此计数内。（但是，其他用户的操作能够触发通知，如 ReadMsg 和 DeleteMsg）。
numSeenDeleted*nn*	MQInt32	邮箱中为每种邮件类型指定的标记为已读（已阅读）和已删除的邮件总数。如果配置了邮件类型，numSeenDeleted*nn* 属性将包含每种邮件类型 *nn* 的计数。 始终发送 numSeenDeleted 属性；它统计邮箱中所有标记为已读和已删除的邮件的总数，包括所有类型。 例如，如果邮箱中有 20 个标记为已读和已删除的邮件，其中 10 个是类型 3，7 个是类型 16，而其余的不属于任何已识别类型，则通知中包含以下属性和计数： numSeenDeleted=20 numSeenDeleted3=10 numSeenDeleted16=7
oldflags	ConstMQString	用户的邮箱邮件被当前操作改变前设置的标志。在生成 MsgFlags 通知邮件时，此属性总是与 newflags 一起出现。 有关 oldflags 的语法和值，请参见此表下面的第 630 页中的 “newflags 和 oldflags 属性的语法”。
quotaRoot	ConstMQString	此属性可以是用户名、文件名或邮件类型。

表 22–4 特定于特定通知邮件的属性 （续）

属性	数据类型	说明
size	MQInt32	邮件大小。请注意，此属性可能不是邮件正文的大小，因为正文通常是邮件被截断的版本。
uidValidity	MQInt32	IMAP uid 有效性属性。
userid	ConstMQString	与邮件相关的 userid。

注 – 在解析邮件引用时，订户应该允许没有记录的属性。这考虑未来添加新属性时的兼容性。

newflags 和 oldflags 属性的语法

newflags 和 oldflags 属性是 5–字符字符串。此字符串必须有以下值：

- 如果设置了 /answered 标志，则第一个字符为 "A"。否则，为空白 (" ")。
- 如果设置了 /flagged 标志，则第二个字符为 "F"。否则，为空白 (" ")。
- 如果设置了 /deleted 标志，则第三个字符为 "D"。否则，为空白 (" ")。
- 如果设置了 /seen 标志，则第四个字符为 "S"。否则，为空白 (" ")。
- 如果设置了 /draft 标志，则第五个字符为 "R"。否则，为空白 (" ")。

22.3.5.3 每个通知邮件包含的属性

表 22–5 显示了与每个通知邮件相关的属性。

例如，要查看哪些属性可以应用于 TrashMsg 邮件，请在列标题中查找 "ReadMsg, TrashMsg"。除了标准属性之外，TrashMsg 邮件还可以使用 mailboxName、 numMsgs、uidValidity、numSeen 和 numDeleted。

表 22–5 每个通知邮件包含的属性

属性	NewMsg, UpdateMsg	ReadMsg, TrashMsg	DeleteMsg, PurgeMsg	MsgFlags	Login, Logout	OverQuota, UnderQuota
client	否	否	否	否	是	否
diskquota	否	否	否	否	否	是
diskquotaused	否	否	否	否	否	是
hdrLen	是	否	否	是	否	否
hostname	是	是	是	是	是	是
imapUid	是	否	是	是	否	否

表 22–5 每个通知邮件包含的属性 （续）

属性	NewMsg, UpdateMsg	ReadMsg, TrashMsg	DeleteMsg, PurgeMsg	MsgFlags	Login, Logout	OverQuota, UnderQuota
lastUid	否	否	是	否	否	否
mailboxName	是	是	是	是	否	否
msgquota	否	否	否	否	否	是
newflags	否	否	否	是	否	否
numDeleted	是	是	是	否	否	否
numDeleted*n*	是*	是*	是*	否	否	否
numMsgs	是	是	是	否	否	是
numMsgs*n*	是*	是*	是*	否	否	否
numSeen	是	是	是	否	否	否
numSeen*n*	是*	是*	是*	否	否	否
numSeenDeleted	是	是	是	否	否	否
numSeenDeleted*n*	是*	是*	是*	否	否	否
oldflags	否	否	否	是	否	否
Owner	否	是	否	否	否	否
pid	是	是	是	是	是	是
process	是	是	是	是	是	是
quotaRoot	否	否	否	否	否	是
size	是	否	否	否	否	否
timestamp	是	是	是	是	是	是
uidValidity	是	是	是	是	否	否
userid	否	是	否	否	是	是

注 – * 只有在消息存储中定义了邮件类型，通知才会包含 numDeleted*n*、numMsgs *n*、numSeen*n* 和 numSeenDeleted*n* 属性。

◆ ◆ ◆ 第 23 章

23 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服务系统的特定部分。

Messaging Server 安全体系结构作为整体的 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。

本章包含以下各节：

23.1 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服务系统的重要要求。

危及服务器通信安全性的原因很多，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端。
- **管理员访问控制**：使用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 客户端访问控制**：使用过滤技术来控制哪些客户端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。
- **消息存储访问**：您可以定义一系列 Messaging Server 的消息存储管理员。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 20 章
- **最终用户帐户配置**：最终用户帐户信息可以主要通过使用 Delegated Administrator 产品进行维护。
- **过滤不请自来的批量电子邮件 (Unsolicited Bulk Email, UBE)**：请参见第 18 章
- 第 24 章对安全/通用 Internet 邮件扩展服务 (Secure/Multipurpose Internet Mail Extensions, S/MIME) 进行了介绍。

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。

23.2 关于 HTTP 安全性

Messaging Server 支持用户 ID/密码验证、客户端证书验证和 Access Manager。但是，在协议如何处理客户端和服务器之间的网络连接方面有些区别。

POP、IMAP 或 SMTP 客户端登录到 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，客户端必须到服务器上重新验证。

HTTP 客户端登陆到 Messaging Server 后，该服务器将为客户端提供唯一的会话 ID。在会话过程中，客户端使用此会话 ID 可以建立多个连接。HTTP 客户端无需对每个连接都重新验证；如果会话被终止并且客户端想要建立新会话，客户端就需要重新验证。（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，并注销客户端；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，因此客户端无法冒充某个 ID。

- 会话 ID 被存储在 URL 中而并非任何 Cookie 文件中。

有关指定配置参数以改进连接性能的信息，请参见第 5 章。

有关 Access Manager 的信息，请参见第 6 章。

23.3 配置验证机制

验证机制是客户端向服务器证明其身份的特殊方法。Messaging Server 支持由简单验证和安全层 (Simple Authentication and Security Layer, 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更多信息，请参见第 640 页中的 “23.5 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，这在网络上是很容易被窃听到的。

  请注意，SSL 可用于缓解窃听问题。有关更多信息，请参见第 640 页中的 “23.5 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。）

注 – 此功能已弃用并将从未来的发行版中删除。

- **CRAM-MD5**—一种询问/响应验证机制，类似于 APOP，但也可用于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，只是为了与 SMTP 验证的预标准实现兼容。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端。客户端则以该询问的散列和用户密码响应。如果客户端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 23–1 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 6.3 Administration Reference》中的“configutil Parameters”。

表 23–1 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
service.{imap|pop|http}.plaintextmincipher	如果此参数大于 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端上启用 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。提供此参数是为了与传统的单域模式兼容，但建议不要在新部署中使用此参数，因为即使是小公司也可能会进行合并或更名，这些都需要支持多个域。

23.3.1 配置访问纯文本密码

要使CRAM-MD5、DIGEST-MD5 或APOP SASL 验证方法起作用，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 以存储明文密码

要启用 CRAM-MD5、DIGEST-MD5 或 APOP 机制，则必须将 Directory Server 配置为以明文存储密码。如果您使用版本 6 之前的 Directory Server，则需要应用以下说明。对于版本 6 或更高版本，请参阅最新的 Directory Server 文档（《Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide》）：

1 **在 Directory Server 控制台上，打开您要配置的 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。

23.3.1.1 针对明文密码配置 Messaging Server

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”）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。

23.3.2 转换用户

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端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：

▼ 转换用户

. 如果您使用版本 6 之前的 Directory Server，则需要应用以下说明。对于版本 6 或更高版本，请参阅最新的 Directory Server 文档（《Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide》）

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 可用于启用一系列 SASL 机制。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）。

23.4 用户密码登录

用户登录到 Messaging Server 时，需要提交密码才能发送或接收邮件，这是对未授权访问的第一步防范措施。Messaging Server 支持对其 IMAP、POP、HTTP 和 SMTP 服务的基于密码的登录。

23.4.1 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更多信息，请参见第 118 页中的 “5.2.2 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端软件传送到服务器上。如果将客户端和服务器都配置为启用 SSL 并且都支持所需级别的加密（如第 650 页中的 “23.5.2 启用 SSL 并选择加密算法”中所说明的），则将进行加密。

用户 ID 和密码都存储在 LDAP 用户安装目录中。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。本章讨论该主题以及 SSL 的其余部分；请参见第 652 页中的 “23.5.3 设置基于证书的登录”。

询问/响应 SASL 机制是纯文本密码登录的另一个备用登录。

23.4.2 SMTP 密码登录

默认情况下，用户连接到 Messaging Server 的 SMTP 服务时无需提交密码即可发送邮件。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，它允许客户端验证服务器。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）。客户端使用 "AUTH" 命令来验证服务器。

有关启用 SMTP 密码登录（和经过验证的 SMTP）的说明，请参见第 332 页中的 “12.4.4 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。

23.5 配置加密和基于证书的验证

本节包含以下小节：

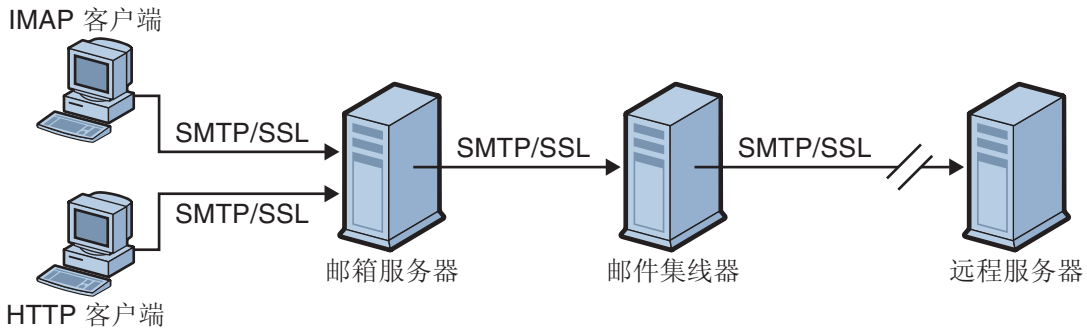
Messaging Server 使用传输层安全性 (Transport Layer Security, TLS) 协议（或称为安全套接字层 [Secure Sockets Layer, SSL] 协议）来进行加密通信以及客户端和服务器的基于证书的验证。Messaging Server 支持 SSL 版本 3.0 和 3.1。TLS 与 SSL 完全兼容并包含所有必需的 SSL 功能。

有关 SSL 的背景信息，请参见《Managing Servers With iPlanet Console 5.0》中的 *Introduction to SSL*。SSL 基于公匙密码学的概念，这在《Managing Servers With iPlanet Console 5.0》的 *Introduction to Public-Key Cryptography* 中已作了说明）。

如果对 Messaging Server 及其客户端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端已经过验证，则盗窃信息者几乎没有机会冒充（欺骗）这些客户端。

SSL 作为 IMAP4、HTTP、POP3 和 SMTP 应用层下面的协议层发挥作用。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发挥作用，如图 23–1 所示。

A. 传出邮件



B. 传入邮件

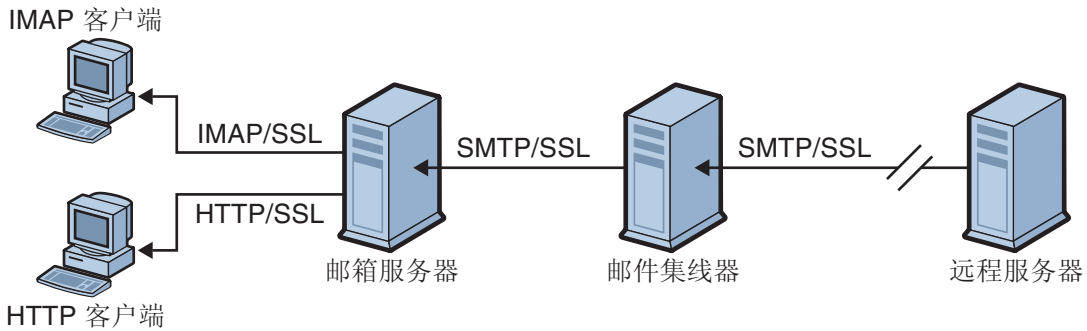


图 23–1 与 Messaging Server 的加密通信

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 – 要能够对外发邮件进行加密，必须修改通道定义以使其包含 `tls` 通道关键字，例如 `maytls`、`musttls` 等。有关更多信息，请参见第 334 页中的 “12.4.8 传输层安全性”手册。

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。设计邮件服务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。

23.5.1 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端和其他服务器。获得证书最有效的方式是使用 `msgcert` 命令（在本节后面部分作了说明）。请注意，以前的 `certutil` 命令仍然起作

用，但它更加复杂，而且没有被国际化。有关 certutil 的更多信息，请参见第 640 页中的 “23.5 配置加密和基于证书的验证”和 http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html。

本节包含以下几个部分：

23.5.1.1 管理内部模块和外部模块

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 服务器使用遵循公钥密码学系统 (Public-Key Cryptography System, 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”支持单个内部软件标记（使用服务器的内部证书数据库）。

对证书设置服务器包括为证书及其密钥创建数据库以及安装 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。

注 – 下列各节将涉及控制台或 Directory Server 控制台。这里指的是版本 6 之前的 Directory Server，对于版本 6 或更高版本，图形用户界面称为 Directory Server 控制中心。有关更多信息，请参阅最新的 Directory Server 文档（《Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide》）。

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. 使用位于 msg-svr-base/sbin 中的 modutil 为安装的驱动程序安装 PKCS #11 模块。

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加密和解密邮件时的性能。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 模块完成加速器的安装（同时使用硬件证书标记）。

23.5.1.2 创建密码文件

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。密码本身在使用 `msgcert generate_certdb` 命令创建它们的证书数据库时生成。

此密码文件的名称为 `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。此密码以明文（不加密的）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。

23.5.1.3 获得和管理证书

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端和其他服务器。用于获得和管理证书的主要机制是使用 `msgcert`。但是，如果安装了 Administration Server，您也可以使用管理控制台。

本节其余部分介绍如何使用 `msgcert`。

23.5.1.4 关于 `msgcert`

`msgcert` 允许您生成证书请求、将证书添加到证书数据库、列出数据库中的证书，等等。要获取详细信息，请在命令行中输入以下内容：

msg-svr-base`/sbin/msgcert --help`

如下所示。

```
# ./msgcert --help

Usage: msgcert SUBCMD [GLOBAL_OPTS] [SUBCMD_OPTS] [SUBCMD_OPERANDS]
Manages the Messaging Servers Certificate Database
The accepted values for SUBCMD are:

add-cert              Adds a certificate to the certificate database
add-selfsign-cert     Creates and adds a selfsign certificate to the
                      certificate database
export-cert           Exports a certificate and its keys from the database
generate-certDB       Creates Messaging Server Databases cert8.db key3.db
                      secmod.db and sslPassword
import-cert           Adds a new certificate and its keys to the cert database
import-selfsign-cert  Adds a new selfsign certificate and its keys to the
                      cert database
list-certs            Lists all certificates in the Certificate database
remove-cert           Removes a certificate from the database
renew-cert            Renews a certificate
renew-selfsign-cert   Renews a selfsign certificate
request-cert          Generates a certificate request
show-cert             Displays a certificate

The accepted value for GLOBAL_OPTS is:-?, --help
               Displays SUBCMD help

NOTE: You must stop all the TLS or SSL-enabled servers before making any
changes to the Certificate Database.
```

以上显示的每个子命令都执行一个特定的证书管理功能。有关这些子命令及其功能的详细信息，可以通过输入以下命令获得：

```
msgcert SUBCMD –help
```

本节剩余部分将介绍一些常见的证书管理过程。

23.5.1.5 管理证书

本节介绍如何在 Messaging Server 中管理 SSL 证书。要在 Messaging Server 上运行 SSL，您必须使用自签名证书，也可以使用包含外部证书授权机构 (Certificate Authority, CA) 的公钥基础设施 (Public Key Infrastructure, PKI) 解决方案。要使用 PKI 解决方案，您需要包含公匙和私匙的 CA 签名服务器证书。此证书特定于一个 Messaging Server。此外还需要一个包含公钥的可信 CA 证书。可信 CA 证书可确保来自 CA 的所有服务器证书都是可信的。此证书有时称为 CA 根密钥或根证书。

配置证书数据库密码

在管理证书时，您无需键入证书密码或指定密码文件。只需将密码作为 -W 参数传递即可。示例：

```
echo "password22" > /tmp/certdbpwd
echo "password22" > /tmp/certdbpwd
# ./msgcert list-certs -W /tmp/certdbpwd
```

▼ 使用默认的自签名证书创建 Messaging Server 证书数据库

1 **要创建 Messaging Server 证书数据库，请运行以下命令：**

```
msgcert generate-certDB
```

此命令将从 CERT_PW_FILE 中读取证书数据库密码（默认值：提示输入密码）

2 **您可以使用以下命令查看该证书：**

```
msgcert show-cert Server-Cert
```

▼ 管理自签名证书

如果将证书用于测试，则您可以使用自签名证书。在部署配置中，您可能希望使用可信的证书授权机构 (Certificate Authority, CA) 证书。您也可以使用 Directory Server 管理控制台执行该任务。

1 **在创建证书数据库时，会自动提供一个默认的自签名证书。如果您要使用不带默认设置的自签名证书，则使用 msgcert add-selfsign-cert 命令。示例：**

```
msgcert add-selfsign-cert --name siroe --org comms --org-unit Messaging
--city SantaClara --state ca --country us MySelfSigned-Cert
```

自签名证书的有效期为 3 个月。

2 **当自签名证书过期时，请使用以下命令续订该证书：**

```
msgcert renew-selfsign-cert cert_alias
```

23.5.1.6 安装可信 CA 证书

使用 ./msgcert add-cert 安装证书授权机构的证书。CA 证书可验证 CA 自身的标识。服务器在验证客户端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，您还将您的企业设置为基于证书的客户端验证（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（可以信任这些 CA 颁发将在客户端显示的证书）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 5.0》。）

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制定（使用 Sun Java System Certificate Server）自己的 CA 以在内部使用，则需要获得并安装其他 CA 证书。

注 – 随 Messaging Server 自动提供的 CA 证书对客户端证书并未初始标记为信任。如果您想要信任由这些 CA 颁发的客户端证书，则需要编辑信任设置。有关说明，请参见第 641 页中的 “23.5.1 获得证书” 。

以下步骤介绍请求和安装 CA 签名服务器证书和可信 CA 证书（用于 Messaging Server）的过程。

▼ 请求 CA 签名服务器证书

您也可以使用 Directory Server 管理控制台执行该任务。

1 生成 CA 签名服务器证书请求。

```
msgcert request-cert [-W CERT_PW_FILE] {-S DN|--name NAME [--org ORG] [--org-unit ORG-UNIT]
   [--city CITY] [--state STATE] [--country COUNTRY] } [-F FORMAT] [-o OUTPUT_FILE]
```

以下是一个请求 CA 签名服务器证书的示例。它以二进制格式返回证书：

```
./msgcert request-cert --name aqua --org siroe --org-unit Messaging -o my_ca_signed_request_cert
```

要以 ASCII 格式返回证书，请使用以下命令：

```
./msgcert request-cert --name aqua --org siroe --org-unit Messaging -F ascii -o my_casigned_request_cert
```

证书授权机构通常需要该示例中显示的所有属性，以便完整地标识服务器。要查看每个属性的说明，请输入 `./msgcert request-cert --help`。使用 `msgcert request-cert` 请求证书时，得到的证书请求是二进制证书请求，除非您指定输出格式为 ASCII。如果指定 ASCII，得到的证书请求是 PEM 格式的 PKCS #10 证书请求。PEM 由是 RFC 1421 至 1424 指定的保密性增强的电子邮件格式，用于以 US-ASCII 字符表示 base64 编码的证书请求。该请求的内容与以下示例类似：

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBdTCB3wIBADA2MRIwEAYDVQQLEwlNZXNzYWdpbmcxDjAMBgNVBAoTBXNpcm9l
MRAwDgYDVQQDEwdhcXVhdGljMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDt
KEh5Fnj/h9GEu18Da6DkJpcNShkwxanjnKs2883ZoUV5Sp4pN7U6Vfbh0414WXZh
D26m3t81q9b9h47Klkf0pW1X3BB6LOjGOHSt2VoNBI8n3hJ6XiN2zYbrlLTgdKuo
y0YrSG/kHFnqKghikag9O/Ox+cwD+mpjl2QnsPZgswIDAQABoAAwDQYJKoZIhvcN
AQEEBQADgYEArqgWQIwNZDC2d3EZawI23Wj9o6Pyvu9J1rkb+NYgIEnNp9jugxqX
F326N0ABLdHXXNX/2ZvC5TKOgS4RidTBM89N9xJvokmvRGfc+1x80uxy474YdNlZ
s+nP8AYo9dW9mrLOammozx9HLPSVYNFp4FxekgV2n8QG7WC5rkN5bCE=
-----END NEW CERTIFICATE REQUEST-----
```

2 按照程序将证书请求传送给证书授权机构。

获得证书授权机构证书的过程取决于所使用的证书授权机构。一些商业 CA 提供了允许您自动下载证书的 Web 站点。其他 CA 将在您请求证书后以电子邮件形式向您发送证书。

发送请求之后，您必须等待 CA 对请求做出响应，即提供您的证书。请求的响应时间各不相同。例如，如果您的 CA 在公司内部，则 CA 可能只需一两天即可响应您的请求。如果您选择的 CA 在公司外部，则 CA 可能需要几个星期才能响应您的请求。

3 保存从证书授权机构收到的证书。

您应该将证书备份在安全的地方。如果您丢失了证书，则可以使用备份文件重新安装它们。您可以将证书保存在文本文件中。PEM 格式的 PKCS #11 证书与以下示例类似。

```
-----BEGIN CERTIFICATE-----
MIICjCCAZugAwIBAgICCEEwDQYJKoZIhKqvcNAQFBQAwfDELMAkGA1UEBhMCVVMx
IzAhBgNVBAoGlBhbG9a2FWaWxsZGwSBXaWRnZXRzLCBJbmMuMR0wGwYDVQQLExRX
aWRnZXQgTW3FrZXJzICdSJyBVczEpMCcGAx1UEAxgVGVzdCBUXN0IFRlc3QgVGVz
dCBUZXN0IFlc3QgQ0EswHhcNOTgwMzEyMDIzMzUWhcNOTgwMzI2MDIzMpzU3WjBP
MQswCYDDVQQGEwJVUzEoMCYGA1UEChMfTmV0c2NhcGUgRGlyZN0b3J5VIFB1Ymxp
Y2F0aW9uczEWMB4QGA1UEAxMNZHVgh49dq2tLNvbjTBaMA0GCSqGSIb3DQEBAQUA
A0kAMEYkCQCksMR/aLGdfp4m0OiGgijG5KgOsyRNvwGYW7kfW+8mmijDtZaRjYNj
jcgpF3VnlbxbclX9LVjjNLC5737XZdAgEDozYwpNDARBglghkgBhvhCEAQEEBAMC
APAwHkwYDVR0jBBgwFAU67URjwCaGqZHUpSpdLxlzwJKiMwDQYJKoZIhQvcNAQEF
BQADgYEAJ+BfVem3vBOPBveNdLGfjlb9hucgmaMcQa9FA/db8qimKT/ue9UGOJqL
bwbMKBBopsDn56p2yV3PLIsBgrcuSoBCuFFnxBnqSiTS7YiYgCWqWaUA0ExJFmD6
6hBLseqkSWulk+hXHN7L/NrViO+7zNtKcaZLlFPf7d7j2MgX4Bo=
-----END CERTIFICATE-----
```

▼ 添加 CA 签名服务器证书和可信 CA 证书

您也可以使用 Directory Server 管理控制台执行该任务。

1 使用以下命令添加 CA 签名服务器证书：

```
msgcert add-cert cert_alias cert_file
```

其中 *cert_alias* 是您提供的用于标识证书的名称，*cert_file* 是包含 PEM 格式的 PKCS #11 证书的文本文件。

例如，要安装 CA 签名服务器证书，可以使用类似以下形式的命令：

```
msgcert add-cert /my_cert/server-cert-file
```

现在证书已经安装，但还不是可信的。要信任 CA 签名的服务器证书，您必须安装证书授权机构证书。

2 使用以下命令添加可信证书授权机构证书：

```
msgcert add-cert -C cert_alias cert_file
```

-C 选项表示证书是可信证书授权机构证书。

例如，要安装来自证书授权机构的可信证书，可以使用以下命令：

```
msgcert add-cert -C CA-cert /my_cert/ca-cert-file
```

3 **可以选择使用以下命令验证安装的证书：**

列出所有服务器证书，并显示别名和有效日期等信息：

```
msgcert list-certs
```

在使用 ./msgcert generate-CertDB 生成证书时，Messaging Server 将具有一个名为 Server-Cert 的默认证书。文本 "Same as issuer" 表示默认证书是自签名的服务器证书。例如：

```
# ./msgcert list-certs
Enter the certificate database password:
Alias          Valid from       Expires on       Self-   Issued by             Issued to
                                                 signed
------------   ---------------  --------------- ------  -------------------- ------------------------  ------------
SelfSignedCrt 2006/07/28 12:58  2006/10/28 12:58   y     CN=SFO,L=SC,ST=ca,C=us  Same as issuer
Server-Cert   2006/07/28 07:47  2006/10/28 07:47   y     CN=perseids             Same as issuer
2 certificates found
```

列出可信的 CA 证书：

```
msgcert list-certs -C
```

查看证书的详细信息（包括证书过期日期）：

```
msgcert show-cert cert_alias
```

例如，要显示一个自签名证书：

```
# ./msgcert show-cert MySelfSigned-Cert
Enter the certificate database password:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            00:83:35:37:94
        Signature Algorithm: PKCS #1 MD5 With RSA Encryption
        Issuer:
            "CN=siroe,O=comms,OU=Messaging,L=SantaClara,ST=ca,C=us"
        Validity:
            Not Before: Fri Jul 28 19:58:31 2006
            Not After : Sat Oct 28 19:58:31 2006
        Subject:
            "CN=siroe,O=comms,OU=Messaging,L=SantaClara,ST=ca,C=us"
        Subject Public Key Info:
```

```
            Public Key Algorithm: PKCS #1 RSA Encryption
            RSA Public Key:
                Modulus:
                    aa:9d:3d:23:b2:59:39:f3:77:c8:69:7f:b0:d1:ac:d2:
                    4e:81:c8:51:0f:27:6f:a1:21:4b:a9:27:46:d7:0f:b4:
                    c8:44:86:32:5e:4f:2f:1c:2f:a9:b8:a3:49:b5:b8:ab:
                    51:a8:a5:ba:1c:e8:90:7d:46:67:f9:a7:44:c5:1d:24:
                    e6:bd:e8:8f:07:b4:5a:68:41:b1:19:f2:ea:98:ba:25:
                    55:b8:ba:9c:af:bb:43:c3:c0:8f:14:a7:4c:2b:50:b4:
                    ac:df:b5:cd:68:de:a6:14:9d:68:77:d3:8b:7f:de:c0:
                    5d:35:d7:55:8d:b5:c3:14:2a:60:a9:bf:de:96:90:a9
                Exponent: 65537 (0x10001)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
        15:86:f1:cc:85:c9:08:0f:ff:d3:56:d8:e2:c8:ea:3c:
        8e:45:36:be:8b:b0:7d:2f:e9:cd:e3:b4:ad:8c:70:59:
        c8:a5:14:da:9c:fa:7f:70:86:64:34:0b:21:ae:c4:28:
        d2:f5:94:5c:a6:78:0f:d9:fd:fc:c5:5e:37:49:25:a9:
        bc:12:59:cb:fb:4e:e9:d4:8a:8d:3d:41:12:ae:f1:7f:
        8d:d3:10:ac:fb:33:51:5d:0c:1b:dc:23:5f:95:d5:6d:
        c6:1d:e5:ed:13:8b:16:41:89:5b:4d:de:c0:c7:56:a2:
        48:82:38:32:5a:99:d5:21:20:c5:0d:5c:ea:0c:84:aa
    Fingerprint (MD5):
        EF:76:A3:6C:09:4E:BC:6B:87:76:A3:35:70:1F:B2:C4
    Fingerprint (SHA1):
        BB:1C:20:4B:79:3A:F1:49:F0:83:FB:CC:9C:56:10:D3:06:97:AA:07

    Certificate Trust Flags:
        SSL Flags:
            Valid CA
            Trusted CA
            User
            Trusted Client CA
        Email Flags:
            User
        Object Signing Flags:
            User
```

▼ 续订过期的 CA 签名服务器证书

当 CA 签名服务器证书（公匙和私匙）过期时，您可以通过以下步骤续订。您也可以使用 Directory Server 管理控制台执行该任务。

1 从证书授权机构获得更新的 CA 签名服务器证书。

2 接收到更新证书后，安装该证书。

```
msgcert renew-cert cert_alias cert_file
```

▼ 导出和导入 CA 签名服务器证书

在某些情况下，您可能需要导出证书，以便以后可以导入该证书（例如将其导入另一个主机）。您也可以使用 Directory Server 管理控制台执行该任务。

1 **导出证书。**

```
msgcert export-cert [-o OUTPUT_FILE] CERT_ALIAS
```

例如：

```
$ ./msgcert export-cert -o /tmp/first-certificate "First Certificate"
$./msgcert export-cert -o /tmp/first-server-certificate Server-Cert
Choose the PKCS#12 file password:
Confirm the PKCS#12 file password:
$ls /tmp
first-server-certificate
/tmp/first-certificate
```

2 **导入证书。**

```
$ msgcert import-cert  CERT_FILE
```

例如，导入证书

```
$ msgcert import-cert /tmp/first-server-certificate
Enter the PKCS#12 file password:
$
```

23.5.2 启用 SSL 并选择加密算法

您可以使用控制台启用 SSL 并选择 Messaging Server 可以在其与客户端的加密通信中使用的加密算法集。您也可以使用 msgcert 实用程序安装 SSL 证书，并运行相应的 configutil 或编辑启用此特定服务的 SSL 所需的相应配置文件。

23.5.2.1 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）应用到数据中来对数据进行操作。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。

客户端用 Messaging Server 启动 SSL 连接时，客户端会让服务器了解客户端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 23–2 列出了 Messaging Server 支持的可与 SSL 3.0 配合使用的加密算法。有关此表中汇总的信息，可在 Managing Servers with iPlanet Console 中的 *Introduction to SSL* 一章中获得的更详细的介绍。

表 23–2 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 位加密和 SHA 邮件验证的 DES	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 位加密和 MD5 邮件验证的 RC4	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 位加密和 MD5 邮件验证的 RC2	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，所生产的某些客户端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，因此将不会阻止蓄意攻击。

要启用 SSL 并选择加密算法，请遵循以下命令行步骤：

要指定一个证书：

```
configutil -o encryption.rsa.nssslpersonalityssl -v certname
```

还有基于服务的配置设置，用于设置 SSL 服务器证书昵称。新的 configutil 设置如下所示：

`local.imta.sslnicknames` 用于 SMTP 和 Submit 服务器；`local.imap.sslnicknames` 用于 IMAP 服务器；`local.pop.sslnicknames` 用于 POP 服务器；`local.http.sslnicknames` 用于 web 邮件服务器。

这些设置与 `encryption.rsa.nssslpersonalityssl` 设置具有相同的含义，并将覆盖该设置。具体地说，该设置是一个以逗号分隔的 NSS 证书昵称列表。尽管在列表中允许多个昵称，但每个昵称必须表示不同的证书类型（例如，RSA 证书和 DSS 证书），这样，该设置几乎总是只有一个昵称。昵称可以是非限定的（此时将搜索 NSS 软件标记

或默认标记），也可以是 *security-module*:*nickname*" 格式（此时将在指定的安全模块中搜索该昵称）。这对存储在硬件标记中或默认 NSS 数据库以外的位置的证书来说是必要的。

这并不允许在产品中使用多个 NSS 软件标记。尤其是，对于 IMAP、POP、SMTP 和 HTTP，只存在一个 `cert8.db`、`key3.db` 和 `secmod.db`。NSS 不允许发生这种情况。

注 – 要能够对外发邮件进行 SSL 加密，则必须修改通道定义以使其包含 `tls` 通道关键字，例如 `maytls`、`musttls` 等。有关更多信息，请参见第 334 页中的 “12.4.8 传输层安全性” 手册。

23.5.3 设置基于证书的登录

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进行的验证。在基于证书的验证中，客户端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：

▼ 设置基于证书的登录

1. **为您的服务器获取服务器证书。（有关详细信息，请参见第 641 页中的 “23.5.1 获得证书”）**

2. **运行“证书设置向导”以安装所有可信的证书授权机构证书，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 645 页中的 “23.5.1.6 安装可信 CA 证书”）**

   请注意，只要服务器的数据库中至少有一个可信的 CA，服务器就会要求每个连接的客户端提供客户端证书。

3. **打开 SSL。**

   （有关详细信息，请参见第 650 页中的 “23.5.2 启用 SSL 并选择加密算法”）

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来搜索相应的 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，当客户端建立一个 SSL 会话以便用户可以登录到 IMAP 或 HTTP 时，Messaging Server 会要求客户端提供用户证书。如果客户端所提交的证书由服务器建立为可信的 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，如果客户端建立 SSL 会话并提供证书，则使用基于证书的登录。如果客户端未使用 SSL 或未提供证书，则服务器会要求提供密码。

23.5.4 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《Sun Java Communications Suite 5 Deployment Planning Guide》中的“Using the MMP SMTP Proxy”和第 664 页中的 “23.8 启用 POP Before SMTP”。

23.6 配置管理员对 Messaging Server 的访问

本节大部分内容与 Sun Java System LDAP Schema v. 1 相关。本节包含以下各小节：

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 服务器的功能；它是指管理员可以使其他管理员有选择地访问单个服务器和服务器功能。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。

23.6.1 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，可以创建邮件服务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]）。
- 限定对特定 Messaging Server 中的特定任务的访问（如第 654 页中的 “23.6.2 限制对特定任务的访问权限”中所述）。

▼ 提供对服务器的整体访问

本节介绍如何授予用户或组访问 Messaging Server 给定实例的权限。

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。

23.6.2 限制对特定任务的访问权限

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。

▼ 限制用户或组对任务的访问

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，通过单击服务器的任务表中的任务文本来选择任务。**
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* 的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。

23.7 配置客户端对 POP、IMAP 和 HTTP 服务的访问

本节包含以下小节：

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，您可以对客户端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。有关对未经许可的海量电子邮件的特殊控制，请参见第 18 章。

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 661 页中的 “23.7.3.2 通常允许”。

23.7.1 客户端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端标识，并可授予客户端对此守护程序的访问权限（如果客户端通过过滤进程）。

作为过滤进程的一部分，Messaging Server TCP 客户端访问控制系统执行（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（以检查客户端主机是否知道客户端上的用户）

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。

客户端请求访问某项服务时，访问控制系统将通过以下标准按顺序将客户端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。
- 如果客户端信息与此项服务的允许过滤器相匹配，则允许访问。
- 如果客户端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 662 页中的 “23.7.4 为服务创建访问过滤器”一节介绍了创建访问过滤器的过程。

23.7.2 过滤器语法

过滤器语句包含了服务信息和客户端信息。服务信息可包含服务的名称、主机名和主机地址。客户端信息可包含主机名、主机地址和用户名。服务器信息和客户端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* 则是代表客户端请求访问的主机名、IP 地址或者通配符名称或模式。处理过滤器后，如果客户端查找访问与 *client* 相匹配，则会允许或拒绝（取决于此过滤器的类型）对 *service* 所指定的服务的访问。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端对 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端对那些服务的访问。（有关通配符名称 [例如 `ALL`] 的说明，请参见第 658 页中的 “23.7.2.1 通配符名称”。）

过滤器中的服务器信息或客户端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* 是与客户端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端访问 `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端规范的更多信息，请参见第 660 页中的 “23.7.2.4 服务器主机规范”和第 660 页中的 “23.7.2.5 客户端用户名规范”）。

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，如果客户端查找访问与 *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 *serviceList* 中指定的所有服务的访问。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 域的任一域中的所有客户端对 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 659 页中的 “23.7.2.2 通配符模式”。

您还可以使用以下语法：

"+" 或 "-" *serviceList*:*$*next_rule*

+（允许过滤器）意味着允许客户端列表中的客户端访问守护程序列表服务。

-（拒绝过滤器）意味着拒绝客户端列表中的客户端访问这些服务。

*（通配符过滤器）允许所有客户端使用这些服务。

$ 分隔规则。

以下示例在所有客户端上启用了多项服务。

```
+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端列表。（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:*
```

23.7.2.1 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 23–3 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。

表 23–3 服务过滤器的通配符名称 （续）

通配符名称	解释
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端主机都匹配。 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端主机都匹配。
KNOWN	匹配用户名称已知的所有用户，或匹配名称**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端主机。 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端主机。
DNSSPOOFER	与其 DNS 名称不匹配自身 IP 地址的所有主机相匹配。

23.7.2.2 通配符模式

可以在服务或客户端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，则该主机地址是匹配的。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。

23.7.2.3 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，**除非**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 主机上的客户端之外，将拒绝所有客户端对所有服务的访问。

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)
```

23.7.2.4 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。

23.7.2.5 客户端用户名规范

对于支持 RFC 1413 中所述的 identd 服务的客户端主机，您可以通过在过滤器的 *clientSpec* 条目中包含客户端的用户名来进一步标识请求服务的特定客户端。在这种情况下，此条目的格式为：

```
user@hostSpec
```

其中 *user* 是由客户端的 identd 服务返回的用户名（或通配符名称）。

在过滤器中指定客户端用户名会很有用，但请记住以下警告：

- identd 服务未经验证；如果客户端系统已损坏，则不能信任此服务返回的客户端用户名。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。
- 大多数现代客户端计算机都不支持 identd，因此它在现代部署中提供的附加值不大。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会减慢不支持 identd 的客户端的访问。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有助于您防止来自客户端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，对于使用 rsh（远程 Shell 服务）来冒充信任的客户端主机的盗窃信息者来说，如果客户端主机支持 ident 服务，则可以使用用户名查找来检测这样的攻击。

23.7.3 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。

23.7.3.1 通常拒绝

在这种情况下，访问被拒绝（默认）。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端访问所有服务。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。

23.7.3.2 通常允许

在这种情况下，访问被授权（默认）。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端的示例如下：

```
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。

23.7.3.3 拒绝对被欺骗的域的访问

可以在过滤器中使用 DNSSPOOFER 通配符名称来检测主机名欺骗。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端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
```

对主机的 IP 地址与其 DNS 主机名不匹配的所有远程主机，此过滤器拒绝提供任何服务。

23.7.3.4 控制对虚拟域的访问

如果邮件服务安装使用虚拟域，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* 中的主机连接到服务（IP 地址对应于 msgServer.siroe*N*.com）。所有其他连接都被拒绝。

23.7.3.5 在允许访问 Webmai 时控制 IMAP 访问

如果想允许用户访问 Webmail，但不访问 IMAP，可以创建类似以下的过滤器：

+imap:*access_server_host*, *access_server_host*

这只允许来自访问服务器主机的 IMAP。您可以在 IMAP 服务器级别使用 service.imap.domainallowed，或在域/用户级别使用 LDAP 属性来设置过滤器。

23.7.4 为服务创建访问过滤器

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。请参见第 18 章

▼ 创建过滤器

- **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 656 页中的 “23.7.2 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 656 页中的 “23.7.2 过滤器语法”中所述的语法规则。有关各种示例，请参见第 661 页中的 “23.7.3 过滤器示例”。

23.7.5 为 HTTP 代理验证创建访问过滤器

任何存储管理员都可以代理验证任何服务。（有关存储管理员的更多信息，请参见第 526 页中的 “20.4 指定管理员对存储的访问权限”。）如果已授权服务的客户端主机通过代理验证访问过滤器访问服务，则可以对这样的服务进行代理验证。

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端和服务之间界面的登录服务器。为有助于配置登录服务器来验证 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 的更多信息，请与您的 Sun Java System 代表联系。

▼ 为 HTTP 代理验证创建访问过滤器

- **命令行。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 656 页中的 “23.7.2 过滤器语法”中所述的语法规则。

23.8 启用 POP Before SMTP

SMTP 验证或 *SMTP* **验证** (RFC 2554) 是提供 SMTP 中继服务器安全性的首选方法。SMTP 验证仅允许已验证的用户通过 MTA 发送邮件。但是，某些传统客户端仅提供对 *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 客户端而不是使用 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 安全标准的客户端，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。

POP before SMTP 的 Messaging Server 实现与 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 客户端连接到 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端 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

有关使用 SMTP 代理的指导，请参见《Sun Java Communications Suite 5 Deployment Planning Guide》中的“Using the MMP SMTP Proxy”。

1 **安装 Messaging Multiplexor (MMP)。**

有关说明，请参见《Sun Java Communications Suite 5 Installation Guide》。

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。这些新文件为：

`AService-def.cfg`、`ImapProxyAService-def.cfg`、`PopProxyAService-def.cfg` 和 `SmtpProxyAService-def.cfg`

这些文件是由安装过程创建的，文档中说明的四个配置文件并非由安装过程创建，也会不受其影响。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 服务器真实的客户端 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 18 章中的第 495 页中的 “18.6 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 7 章以及 《Sun Java System Messaging Server 6.3 Administration Reference》中的“Encryption (SSL) Option”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` 是以空格分隔的 SMTP 中继服务器主机名（带有可选端口）列表，将用于循环中继。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。此选项是不带默认值的强制选项并且必须与 SMTP 服务器上的 `PROXY_PASSWORD` 选项相匹配。

示例： `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端的 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 通道的名称以用于经 POP before SMTP 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 653 页中的“23.5.4 如何使用 SMTP 代理服务器优化 SSL 性能”）。

示例： `default:PopBeforeSmtpKludgeChannel tcp_intranet`

`ClientLookup` 选项的默认值为 `no`。如果设置为 `yes`，则系统将无条件地对客户端 IP 地址的 DNS 执行反向查找，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。

示例： `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 653 页中的“23.5.4 如何使用 SMTP 代理服务器优化 SSL 性能”）

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）。如果连接 SMTP 中继失败，则在故障转移超时时间内 MMP 不会对此中继进行再次尝试（即，如果故障转移超时时间是 10 秒，并且中继失败，则在 10 秒之内 MMP 不会对此中继进行再次尝试）。

示例：`default:FailoverTimeout 10`

23.9 配置客户端对 SMTP 服务的访问

有关配置客户端对 SMTP 服务的访问的信息，请参见第 18 章。

23.10 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：将 `local.service.pab.ldapport` 设置为 `636`、`local.ugldapport` 设置为 `636`、`local.ugldapusessl` 设置为 `1`。

◆ ◆ ◆ 第 24 章

24 管理 Communications Express Mail 的 S/MIME

可在 Sun Java System Communications Express Mail 上使用安全/通用 Internet 邮件扩展 (Secure/Multipurpose Internet Mail Extension, S/MIME) 3.1。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。本章包含以下几个部分：

24.1 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、更改或邮件内容以任何方式被使用
- 使用包含证书撤销列表 (CRL) 的进程来验证外来的签名邮件的数字签名

- 自动对外来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 兼容客户端（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

24.1.1 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
  - 私钥-公钥对及其证书
  - 证书授权机构 (CA)
  - 验证密钥及其证书
  - 证书撤销列表 (CRL)。
    （请参见第 690 页中的 “24.9.2 何时根据 CRL 检查证书？”）

24.2 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端上安装了所有正确版本的软件。

表 24–1 列出了要在客户机中访问 Communications Express Mail 所需的软件和硬件。

表 24–1 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

表 24–1 客户机必需的硬件和软件 （续）

组件	说明
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
具有证书的私钥-公钥	一个或多个具有证书的私钥-公钥对。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 690 页中的 “24.9.2 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（现在重命名为 ActiveIdentity），版本 2.1 或 3.0，或者 ■ 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 24–2 列出了服务器所需的 Sun Microsystems 软件。

表 24–2 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 5 或更高版本
LDAP 服务器	Sun Java System Directory Server 5 2004Q2
Java	Java 2 Runtime Environment，Standard Edition，版本 1.4.2 或更高版本
Access Manager	（如果是在 Schema 2 下进行部署）—Sun Java System Access Manager 6 2005Q1 和 Communications Express（Sun Java System Communications Express 6 2005Q1 或更高版本）。

24.3 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。

24.3.1 私钥和公钥

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 格式证书的私钥和公钥对。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：

- 存储在智能卡中

  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来使用和保护智能卡。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私钥信息。

  有关更多信息，请参见第 670 页中的 “24.3.2 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 670 页中的 “24.3.3 存储在客户机中的密钥”。

24.3.2 存储在智能卡中的密钥

如果私钥-公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。

带有读卡功能的系统实际上分为两部分。一部分是硬件读卡器及其驱动程序。另一部分是实际的卡，通常由不同的供应商提供，并需要驱动程序才能阅读卡。并非所有的卡都受支持。请参阅表 24–1，查看受支持的 SmartCard（ActiveCard，现在称为 ActiveIdentity 和 NetSign）列表。

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 就可以使用私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 668 页中的 “24.2 必需的软件和硬件组件”。

用户计算机上应具有智能卡供应商提供的库。有关更多信息，请参见第 687 页中的 “24.8 客户机的密钥访问库”。

24.3.3 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浏览器供应商提供的库以支持本地密钥库。有关更多信息，请参见第 687 页中的 “24.8 客户机的密钥访问库” 。

24.3.4 在 LDAP 目录中发布公钥

还必须将所有公钥和证书存储到 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钥。

发件人和收件人的公钥用于加密邮件的加密-解密过程。公钥证书用于验证数字签名所使用的私钥。

有关使用 `ldapmodify` 来发布公钥和证书的更多信息，请参见第 695 页中的 “24.11 管理证书” 。

24.3.5 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。这涉及在用户的 LDAP 条目中使用 `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 694 页中的 “24.10 授予使用 S/MIME 功能的权限” 。

24.3.6 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。

24.4 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。

24.4.1 S/MIME Applet

对邮件进行签名、加密或解密的过程以及验证私钥和公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 24–1 显示了 S/MIME Applet 与其他系统组件的关系。

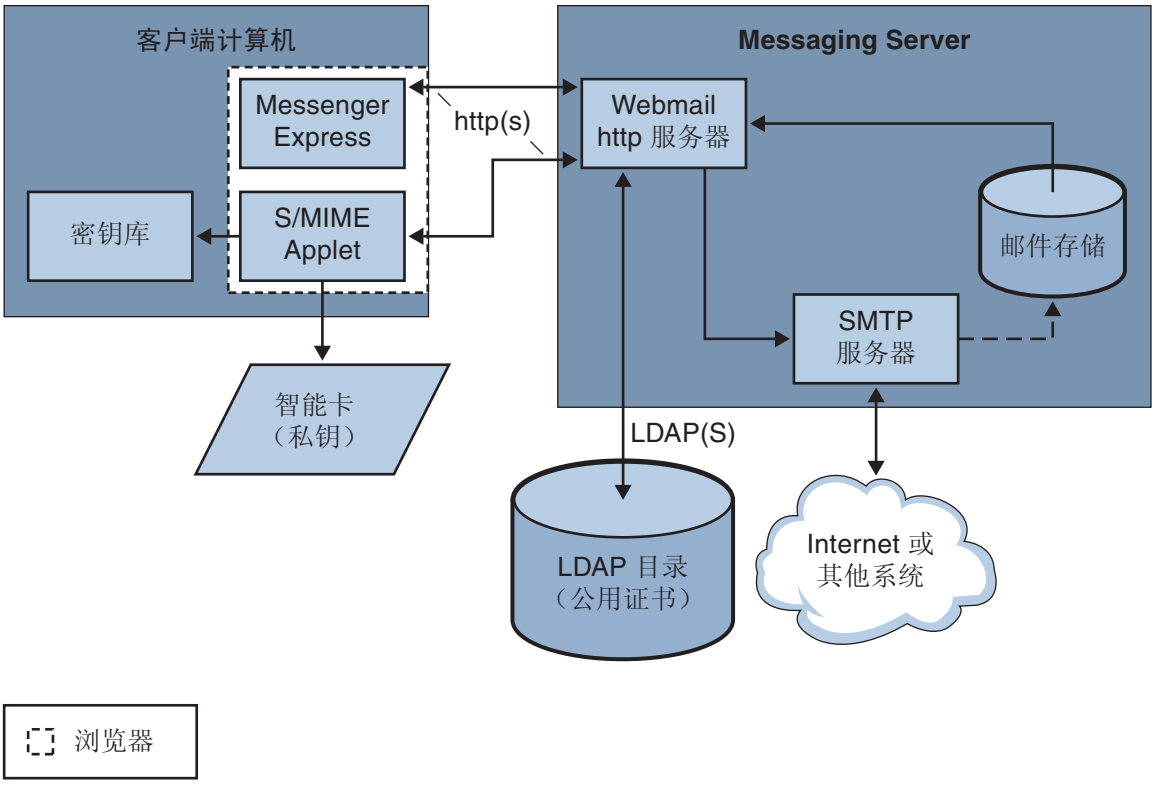


图 24–1 S/MIME Applet

24.4.1.1 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 "Yes" 或 "Always" 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 695 页中的 “24.11 管理证书” 。

24.4.1.2 下载 S/MIME Applet

用户每次登录 Communications Express Mail 时都将下载 S/MIME Applet，除非在用户计算机上针对 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，用户就不必每次登录时都下载此 Applet。

高速缓存可以提高性能，您可以指导用户执行以下步骤来针对 Java 2 Runtime Environment 版本 1.4.*x* 启用高速缓存：

▼ **针对 Java 2 Runtime Environment 版本 1.4 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，则用户也感觉不到验证私钥或公钥的过程。有关更多信息，请参阅第 688 页中的 “24.9 验证私钥和公钥” 。

24.4.2 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：

▼ 配置 S/MIME

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，请为有权使用 S/MIME 功能的所有邮件用户创建或获取私钥-公钥对和标准 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。请参见第 687 页中的 “24.8 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，请参见表 24–3 中的 `trustedurl`；有关搜索 LDAP 目录的信息，请参见第 695 页中的 “24.11 管理证书”。

   b. 在 Directory Server 可以访问的 LDAP 目录中存储公钥和证书。公钥和证书的 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，请参见表 24–3 中的 `certurl`；有关搜索 LDAP 目录的信息，请参见第 695 页中的 “24.11 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。

      注释：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 694 页中的 “24.10 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`（请参见表 24–3）—设置为 LDAP 目录信息，以查找 CA 的证书。使用在步骤 a 中保存的信息。

b. `certurl`（表 24–3）—设置为 LDAP 目录信息，以查找公钥和证书。使用在步骤 b 中保存的信息。

c. `usersertfilter`（请参见表 24–3）—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，以确保在将用户的私钥-公钥对分配给其他邮件地址时可以找到这些密钥对。

d. `sslrootcacertsurl`（请参见表 24–3）—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 685 页中的“24.7 使用 SSL 确保 Internet 链路的安全”。

`checkoverssl`（请参见表 24–3）—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`（请参见表 24–3）—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`（表 24–3）—如果需要进行验证才能访问包含公钥和 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。

注释：每次使用由 `crlmappingurl`、`sslrootcacertsurl` 或 `trustedurl` 参数指定的 LDAP 信息访问 LDAP 目录，都应使用 `logindn` 和 `loginpw` 的值。有关详细信息，请参见第 679 页中的“24.5 smime.conf 文件的参数”和第 677 页中的“24.4.3 使用证书访问 LDAP 中的公钥、CA 证书和 CRL”。

如果访问 LDAP 目录时不需要进行验证，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 684 页中的 “24.6 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 "Yes" 或 "Always" 回答 S/MIME applet 的特定提示问题。请参见第 695 页中的 “ 24.11 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 目录信息的值上和/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。

下表中总结的其他 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 679 页中的 “24.5 smime.conf 文件的参数”。

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

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。

24.4.3 使用证书访问 LDAP 中的公钥、CA 证书和 CRL

S/MIME 所需的公钥、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 包含所需的 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/密码凭证都是可选的；如果未指定任何一个证书，则将首先尝试使用 HTTP 服务器证书访问 LDAP；如果失败，将尝试以 `anonymous` 访问 LDAP。

要访问所需的 URL，需要设置两对 `smime.conf` 凭证参数：`logindn` 和 `loginpw`，以及 `crlurllogindn` 和 `crlurlloginpw`。

在 `smime.conf` 中，`logindn` 和 `loginpw` 是用于所有 URL 的凭证。它们指定对公钥、公钥的证书和 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 690 页中的 “24.9.3 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。

24.4.3.1 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、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
```

24.4.3.2 LDAP 证书用法总结

本节总结了 LDAP 证书的用法。

- 所有 LDAP 凭证都是可选的；如果未指定任何一个凭证，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 凭证对。
- 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使用 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。

24.5 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 (`#`)。

您可以将保存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 24–3 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 24–3 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 24–5 中所述的复选框来覆盖用于他们邮件的这一参数值。 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 24–5 中所述的复选框来覆盖用于他们邮件的这一参数值。 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`

表 24–3 smime.conf 文件中的 S/MIME 配置参数 （续）

参数	用途
certurl	指定 LDAP 目录信息，以查找 Communications Express Mail 用户的公钥和证书（公钥的 LDAP 属性为 `usercertificate;binary`）。有关证书的更多信息，请参见第 695 页中的 “24.11 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`
checkoverssl	根据 CRL 检查密钥的证书时，控制是否使用 SSL 通信链路。有关更多信息，请参见第 685 页中的 “24.7 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。请参见第 692 页中的 “24.9.4 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 对访问 CRL 的尝试的失败进行计数的时间段。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。请参见第 693 页中的 “24.9.7 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 692 页中的 “24.9.5 使用过时 CRL”。

表 24–3 smime.conf 文件中的 S/MIME 配置参数 （续）

参数	用途
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 688 页中的 “24.9 验证私钥和公钥”。 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。
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。有关详细信息，请参见第 690 页中的 “24.9.3 访问 CRL”。您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，则不需要指定。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	针对 `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 692 页中的 “24.9.5 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。

表 24–3 smime.conf 文件中的 S/MIME 配置参数 （续）

参数	用途
logindn	指定对 LDAP 目录中的公钥、公钥的证书和 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`
loginpw	针对 `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 687 页中的 “24.8 客户机的密钥访问库”。
readsigncert	控制在阅读邮件时是否根据 CRL 检查公钥的证书以验证 S/MIME 数字签名。（私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 检查与私钥相关联的公钥的证书。）请参见第 688 页中的 “24.9 验证私钥和公钥”。 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 688 页中的 “24.9 验证私钥和公钥”。 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钥的证书在使用之前是否根据 CRL 进行检查。请参见第 688 页中的 “24.9 验证私钥和公钥”。 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。

表 24–3 smime.conf 文件中的 S/MIME 配置参数 （续）

参数	用途
sendencryptcertrevoked	确定当用于加密外发邮件的公钥证书已撤销时应采取的措施。有关更多信息，请参见第 688 页中的 “24.9 验证私钥和公钥”。 选择以下值之一： `allow`—使用公钥。 `disallow`—不使用公钥。该值为默认值。
sendsigncert	控制是否根据 CRL 来检查公钥证书，从而确定是否可以将私钥用于为外发邮件创建数字签名。（私钥用于数字签名，但是不能根据 CRL 对其进行检查，因而要根据 CRL 检查与私钥相关联的公钥的证书。）有关更多信息，请参见第 688 页中的 “24.9 验证私钥和公钥”。 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	确定私钥已撤销时应采取的措施。（私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 检查与私钥相关联的公钥的证书。如果公钥证书已撤销，则其对应的私钥也将撤销。）有关更多信息，请参见第 688 页中的 “24.9 验证私钥和公钥”。 选择以下值之一： `allow`—使用撤销的私钥。 `disallow`—不使用撤销的私钥。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 685 页中的 “24.7 使用 SSL 确保 Internet 链路的安全”。 如果具有接收来自客户端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`

表 24–3 smime.conf 文件中的 S/MIME 配置参数 （续）

参数	用途
timestampdelta	以秒为单位指定时间间隔，该时间间隔用于确定根据 CRL 检查公钥的证书时是使用邮件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 693 页中的 “24.9.6 确定要使用的邮件发送时间” 。 示例： `timestampdelta==360`
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，以确保将用户的私钥-公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。

24.6 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。

▼ 设置适用于 S/MIME 的 Messaging Server 选项

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` 实用程序来设置这些选项。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。
`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`

24.7 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。 请参见第 686 页中的 “24.7.1 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。 请参见第 686 页中的 “24.7.2 确保 Messaging Server 和 S/MIME Applet 之间的链路的安全”

24.7.1 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)。在设置 Messaging Server 以使用 SSL 之后，请配置 Communications Express 以使用 SSL。请参见《Sun Java System Communications Express 6.3 管理指南》。Communications Express Mail 用户在其浏览器中使用 HTTPS 协议指定 Communications Express URL :

`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 640 页中的 “23.5 配置加密和基于证书的验证”。

24.7.2 确保 Messaging Server 和 S/MIME Applet 之间的链路的安全

根据 CRL 检查公钥的证书时，S/MIME applet 必须直接与 Messaging Server 进行通信。

▼ 使用 SSL 确保通信链路的安全

1. **执行管理任务来为 Messaging Server 配置 SSL。请参见第 640 页中的 “23.5 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 和客户端应用程序（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详细信息，请参见第 692 页中的 “24.9.4 代理服务器和 CRL 检查” 。

24.8 客户机的密钥访问库

无论邮件用户将私钥-公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` 文件中正确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。选择以下名称之一：

`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 24–4。

表 24–4 客户机中的特殊库

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`

表 24–4 客户机中的特殊库 （续）

智能卡或浏览器供应商	操作系统	库文件名
	Windows	`softokn3.dll`
	Windows	core32.dll

24.8.1 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;
```

24.9 验证私钥和公钥

在 Communications Express Mail 使用私钥或公钥之前，必须先通过图 24–2 所示的验证测试。本节其余部分将介绍根据 CRL 检查公钥的证书的详细信息。

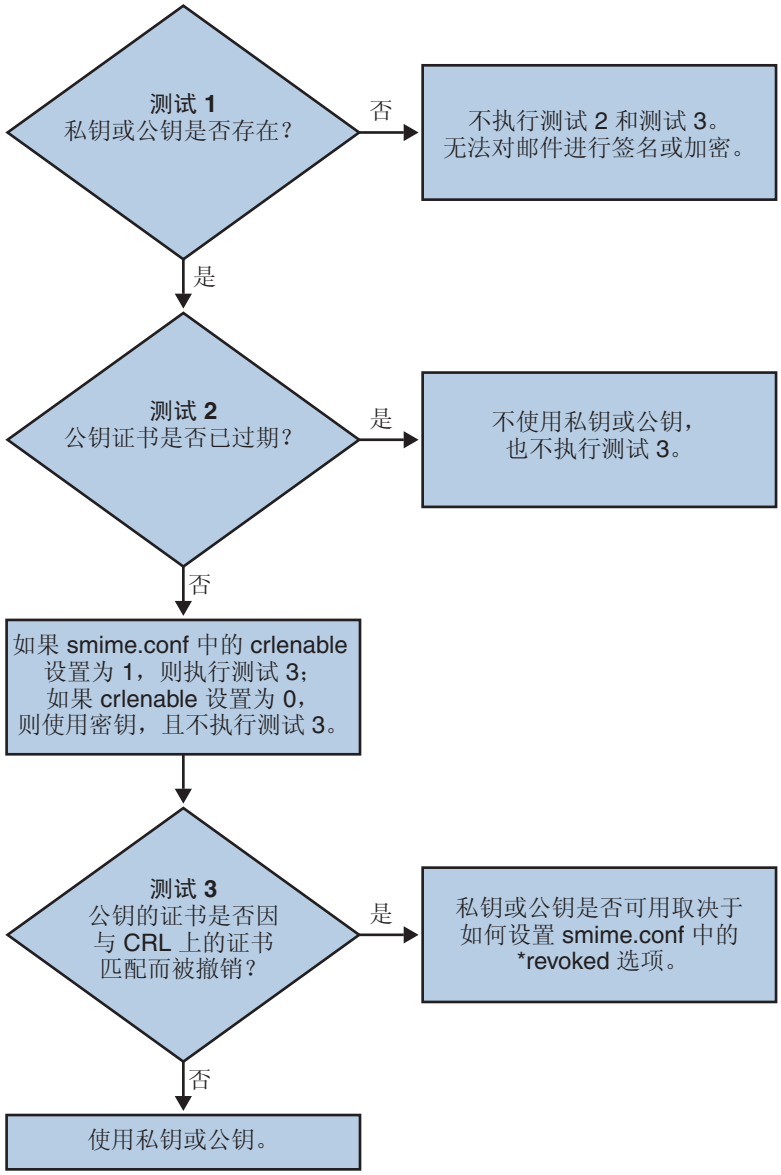


图 24–2 验证私钥和公钥。

24.9.1 查找用户的私钥或公钥

当 Communications Express Mail 用户具有多个私钥-公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 679 页中的 “24.5 smime.conf 文件的参数”中的 usercerfilter。

24.9.2 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。公钥证书用于验证公钥。由于私钥是保密的，只能由拥有该密钥的人员使用，因此不能根据 CRL 直接检查私钥。要确定私钥是否有效，需要使用密钥对的公钥证书。当公钥的证书通过 CRL 测试时，关联的私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。
- 阅读外来的签名邮件时

  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。

24.9.3 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私钥或公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私钥或公钥。

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，因而用户的公钥证书对应多个 URL。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（请参见表 24–3 中的 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 是证书中包含旧信息的 URL，这些信息用来查找 CRL。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` 中的 `crlurllogindn` 和 `crlurlloginpw`，则无需在映射记录中指定登录 DN 和密码。请参见第 677 页中的 “24.4.3 使用证书访问 LDAP 中的公钥、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` 指定查找这些映射定义的目录信息。请参见第 679 页中的 “24.5 smime.conf 文件的参数”。

24.9.4 代理服务器和 CRL 检查

如果您的系统在客户端应用程序和 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，系统仍将阻止进行 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：
  - 将 `smime.conf` 文件中的 `crlenable` 参数设置为 `1`
  - 将 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 685 页中的 “24.7 使用 SSL 确保 Internet 链路的安全” 。

24.9.5 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待决状态。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，并将使用私钥或公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，且不使用私钥或公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。

24.9.6 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 参数来选择进行 CRL 检查时所使用的时间。请将此参数设置为表示秒数的正整数。如果接收时间减去 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，使用接收时间的频率就越高。如果未设置 timestampdelta，将始终使用接收时间。请参见表 24–3 中的 timestampdelta。

24.9.7 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，请参见表 24–3 中的 `crlaccessfail`。

24.9.8 当证书撤销时

当公钥的证书与 CRL 上的任何条目都不匹配时，将使用该私钥或公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，该私钥或公钥将被视为已撤销。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私钥已撤销，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私钥（因为其公钥的证书已撤销）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；将使用该私钥或公钥对外发邮件进行签名或加密

24.10 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 所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。

24.10.1 S/MIME 权限示例

1. 在以下示例中，将阻止一个 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. 在以下示例中，将阻止某个域中的所有 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 656 页中的 “23.7.2 过滤器语法”。

24.11 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》。

24.11.1 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。例 1，按以下方式设置 `trustedurl`：

```
trustedurl==ldap://demo.siroe.com:389/cn=SMIME Admin, ou=people,
o=demo.siroe.com,o=demo?cacertificate;binary?sub?
(objectclass=certificationAuthority)
```

24.11.2 LDAP 目录中的公钥和证书

以下示例展示了如何将邮件用户的公钥和证书添加到 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 参数的值指定了公钥及其证书在 LDAP 目录中的位置。对于示例 2，按如下方式设置 certurl：

```
certurl==ldap://demo.siroe.com:389/ou=people, o=demo.siroe.com,
o=demo?userCertificate;binary?sub?
```

24.11.3 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 证书和公钥及其证书。

24.11.3.1 搜索一个 CA 证书

在以下示例中，由 -b 选项定义的基 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==
```

搜索多个公钥

在以下示例中，由 `-b` 选项定义的基 DN `o=demo.siroe.com,o=demo` `objectclass=*` 将把在 LDAP 目录中找到的、位于此基 DN 上以及此基 DN 下面的所有公钥和证书返回到 `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
```

搜索一个公钥

在以下示例中，由 `-b` 选项定义的基 DN `uid=JohnDoe, ou=people,o=demo.siroe.com,o=demo` `objectclass=*` 描述了 LDAP 目录中的一个公钥及其证书：

```
# 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==
.
.
```

24.11.4 网络安全服务证书

用于网络安全服务 (Network Security Services, 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`）将证书及相关的 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 Administration Guide (http://docs.sun.com/doc/817-7613)。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）。

24.12 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：

24.12.1 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。

24.12.1.1 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 "Yes"，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。

   为确保将 `charsets.jar` 文件安装到 `/lib` 目录中，请通过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 671 页中的 “24.3.6 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：

   - "Yes"，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。
     - "No"，拒绝 S/MIME applet。您将不能使用 S/MIME 功能。

- "Always"，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：

   - "Yes"，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。
   - "No"，拒绝 S/MIME applet。您将不能使用 S/MIME 功能。
   - "Always"，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。

24.12.2 签名和加密设置

您可以设置初始签名和加密设置，以控制是否对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。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 24–5 概括了各个复选框的用法。

表 24–5 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。

表 24–5 Communications Express Mail 的签名和加密复选框 （续）

复选框文本	位置	Communications Express Mail 用户执行的操作
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：可以对每个邮件使用“在邮件中签名”复选框来进行处理，从而覆盖“为所有外发邮件签名”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：可以对每个邮件使用“对邮件进行加密”复选框来进行处理，从而覆盖“对所有外发邮件加密”的设置。

24.12.3 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 25 章

25 管理日志记录

本章提供了用于 Messaging Server MTA、消息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：

25.1 日志记录概述

日志记录是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服务模式情况。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垃圾邮件文件夹中。

25.1.1 日志记录数据的类型

一般情况下，日志记录提供两种类型信息：

- 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。

25.1.2 Messaging Server 日志文件的类型

Messaging Server 日志记录包含三种类型日志文件：

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. **消息存储和服务日志**。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 25–1 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、入队列和出队列信息等等。	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
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

表 25–1 Messaging Server 日志文件 （续）

日志文件的类型	日志文件说明	默认名称
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*）
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	包含消息存储的跟踪信息。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），并记录错误消息，指明具体故障。	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。序列号无法回滚，而只能在服务器的生命期（从安装服务器开始）内单向增加。

timeStamp—指定一个较大整数，该整数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` 的日志文件是指在 IMAP 日志文件目录中创建的第 63 个日志文件，创建时间为 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 733 页中的 “25.4.3 定义和设置服务日志记录选项”。

25.1.3 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。请参见图 8–2 以帮助您理解。

1. 远程主机与邮件服务主机上的 TCP 插槽建立连接，请求 SMTP 服务。
2. MTA 分发程序将响应该请求，并将连接传送至邮件服务主机的 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，它派生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，记录当远程主机与其建立连接并向其发送邮件时所发生的通讯情况。分发程序根据主机 IP 传送至 SMTP 服务器时创建此日志文件。
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。要获得详细信息，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列的日期和时间、发件人和收件人等信息。有关详细信息，请参见第 716 页中的 “25.3.4 MTA 邮件日志记录示例”。对跟踪邮件最有用的文件是 `mail.log_current` 文件。

25.2 管理日志记录的工具

通过使用 `configutil` 命令，您可以自定义创建和管理 Messaging Server 日志文件的策略。

对于消息存储，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。

MTA 使用一个单独的日志记录工具，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 日志条目中但未在 `syslog` 条目中出现的两个附加组件（*facility* 和 *logLevel*）。

25.3 管理 MTA 邮件和连接日志

MTA 提供了记录每个入队列和出队列的邮件的功能。还提供了分发程序错误和调试输出。

本节包含以下几个部分：

- 第 708 页中的 “25.3.1 了解 MTA 日志条目格式”
- 第 711 页中的 “25.3.2 启用 MTA 日志记录”
- 第 711 页中的 “25.3.3 指定附加 MTA 日志记录选项”
- 第 716 页中的 “25.3.4 MTA 邮件日志记录示例”
- 第 728 页中的 “25.3.5 启用分发程序调试”

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。

有关详细信息，请参见第 711 页中的 “25.3.2 启用 MTA 日志记录”。

启用日志记录会使 MTA 在每次邮件通过 MTA 通道时，都将一个条目写入 *msg-svr-base*`/data/log/mail*` 文件中。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。邮件返回作业对所有 `connection.log*` 文件也执行相似的操作。

MTA 执行自动轮转以维护当前文件时，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（或每月）重命名一次旧的 `mail.log` 文件等。

注 – 启用日志记录后，`mail.log` 文件将稳定地增长，如果不对其进行限制，则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。

25.3.1 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。

```
16-Feb-2007 14:54:13.72 tcp_local ims-ms EE 1 adam@sesta.com
rfc822;marlowe@siroe.com marlowe@ims-ms-daemon
```

日志条目显示：

1. 创建条目的日期和时间（在此示例中为 16-Feb-2007 14:54:13.72）。
2. 源通道的通道名称（在此示例中为 `tcp_local`）。
3. 目标通道的通道名称（在此示例中为 `ims-ms`）。（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 客户端出站。）
4. 条目的类型（在此示例中为 `EE`）。条目可以由单个操作代码（请参见表 25–2）组成，也可以由一个操作代码和一个或多个修饰符代码（请参见表 25–3）组成。条目的格式如下所示：

   <action_code> <zero or more optional modifiers>

   例如，EEC 的日志记录条目代码表示邮件使用 ESMTP（修饰符为 `E`）和 SMTP Chunking（修饰符为 `C`）入队列（操作代码为 `E`）。有关当前使用的操作和修饰符代码的详细信息，请参阅下表。
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）。在该字段中，SMS 通道可以被配置为记录页面数，而不是文件大小。请参见 第 872 页中的 “LOG_PAGE_COUNT”。
6. 信封 `From:` 地址（在此示例中为 `adam@sesta.com`）。请注意对于信封 `From:` 地址 为空的邮件（如通知邮件），此字段为空白。
7. 信封 `To:` 地址的原始格式（在此示例中为 `marlowe@siroe.com`）。
8. 信封 `To:` 地址的活动（当前）格式（在此示例中为 `marlowe@ims-ms-daemon`）。
9. 传送状态（仅适用于 SMTP 通道）。

以下三个表说明了日志记录条目代码。

表 25–2 日志记录条目操作代码

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。
D	成功出队列
E	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、邮件超时，或者手动返回邮件（例如，`imsimta qm` "delete" 命令始终为每个收件人生成 "K" 记录，而 qm "return" 命令则生成 "K" 记录而非 "R" 记录）。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" 中系统会根据失败邮件生成一封新的通知邮件（返回给原发件人）。
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/退回邮件
V	事务被异常中止时显示的警告消息。每个加入队列的收件人地址都有一个 "V" 记录。
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。
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；所有收件人的原始邮件文件已出队列，并在该位置将此收件人和其他未成功发送的收件人的新邮件文件加入队列

下表说明了日志记录条目修饰符代码。

表 25–3 日志记录条目修饰符代码

条目	说明
A	使用了 SASL 验证。
C	使用了 Chunking。请注意，必须使用 ESMTP，chunking 才能起作用，因此您通常会看到类似 `EEC` 或 `DEC` 的字段值。
E	发出/接受 EHLO 命令，因此使用了 ESMTP。
L	使用了 LMTP。
S	使用了 TLS/SSL。S 事务日志条目现在增加了各种与通道关联的提交邮件计数器。

如果启用了 `LOG_CONNECTION`（请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“Option File Format and Available Options”），则会使用另一组操作代码。下面对这些条目进行了介绍。

表 25–4 SMTP 通道的 LOG_CONNECTION 操作代码 + 或 - 条目

条目	说明
C	已关闭连接。将出现诊断字段。写入 connection.log_current（或者 mail.log_current，如果使用了单个日志文件）。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。）

```
16-Feb-2007 15:04:01.14 2bbe.5.3 tcp_local ims-ms
EE 1 service@siroe.com rfc822;adam@sesta.com
adam@ims-ms-daemon 20 /opt/SUNWmsgsr/data/queue/ims-ms/000/ZZf0r2i0HIaY1.01
<0JDJ00803FAON200@mailstore.siroe.com> mailsrv
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. 进程 ID（以十六进制表示），其后是句号（点）字符和计数。如果此为多线程通道条目（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 2bbe.5.3。
2. 邮件的 NOTARY（发送收据请求）标志，表示为整数（在本示例中为 20）。
3. MTA 队列区中的文件名（在本示例中为 /opt/SUNWmsgsr/data/queue/ims-ms/000/ZZf0r2i0HIaY1.01）。
4. 邮件 ID（在本示例中为 <0JDJ00803FAON200@mailstore.siroe.com>）。
5. 正在执行的进程的名称（在本示例中为 mailsrv）。在 UNIX 上，对于分发程序进程（例如 SMTP 服务器），此名称通常为 mailsrv（除非已使用 SASL，在这种情况下，此名称将是经过验证的用户名，例如 *service@siroe.com）。
6. 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），或加入通道队列的官方主机名（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）也可在 ident* 通道关键字的控制下报告在括号内；有关默认 identnone 关键字的示例，请参见第 328 页中的 “12.4.3.4 IDENT 查找”，该关键字选择显示在 DNS 中的名称和 IP 地址。

25.3.2 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 730 页中的 “25.4 管理消息存储、Admin 和 Default 服务的日志”

▼ 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 defaults 通道配置文件中（请参见第 277 页中的 “12.1 配置通道默认值”）。例如：**

```
defaults logging notices 1 2 4 7 copywarnpost copysendpost postheadonly
noswitchchannel immnonurgent maxjobs 7 defaulthost siroe.com siroe.com

!
! delivery channel to local /var/mail store
l subdirs 20 viaaliasrequired maxjobs 7 pool LOCAL_POOL
mailhost.siroe.com
```

25.3.3 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其他可选信息字段。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，该文件为 *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《Sun Java System Messaging Server 6.3 Administration Reference》中的“Option File”。

本节包含以下几个部分：

▼ 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 值将禁用系统日志通知的生成。非 0 值将启用系统日志通知的生成，其绝对值控制系统日志优先级和工具掩码。（正值表示系统日志通知和常规 mail.log* 条目；负值（不推荐使用）只表示系统日志通知，而禁用常规 mail.log* 条目。）0 值为默认值并表示未执行系统日志（事件日志）记录。

▼ 控制日志条目格式

1 **编辑 MTA option.dat 文件。**

2 **设置 LOG_FORMAT 选项。**

- 1（默认值）为标准格式。
- 2 要求为非空格式：空地址字段转换为字符串 "<>"
- 3 要求为计数格式：所有变量长度字段都以 N 开头，其中 N 是字段中字符数的计数。
- 4 导致以 XML 兼容的格式写入日志条目。入口日志条目显示为包含多个属性且没有子元素的单个 XML 元素。这三个元素当前被定义为：en 用于入队/出队条目、co 用于连接条目、he 用于标题条目。

  入队/出队 (en) 元素可以具有以下属性：

```
ts - time stamp (always present)
no - node name (present if LOG_NODE=1)
pi - process id (present if LOG_PROCESS=1)
sc - source channel (always present)
dc - destination channel (always present)
ac - action (always present)
sz - size (always present)
so - source address (always present)
od - original destination address (always present)
de - destination address (always present)
rf - recipient flags (present if LOG_NOTARY=1)
fi - filename (present if LOG_FILENAME=1)
ei - envelope id (present if LOG_ENVELOPE_ID=1)
mi - message id (present if LOG_MESSAGE_ID=1)
us - username (present if LOG_USERNAME=1)
ss - source system (present if bit 0 of LOG_CONNECTION
     is set and source system information is available)
se - sensitivity (present if LOG_SENSITIVITY=1)
pr - priority (present if LOG_PRIORITY=1)
in - intermediate address (present if LOG_INTERMEDIATE=1)
ia - initial address (present if bit 0 of LOG_INTERMEDIATE
     is set and intermediate address information is available)
fl - filter (present if LOG_FILTER=1 and filter information
     is available)
re - reason (present if LOG_REASON=1 and reason string is set)
di - diagnostic (present if diagnostic info available)
tr - transport information (present if bit 5 of LOG_CONNECTION
     is set and transport information is available)
ap - application information (present if bit 6 of LOG_CONNECTION
     is set and application information is available)
qt - the amount of time a message has spent in the queue (LOG_QUEUE_TIME=1)
```

下面是一个样例 en 条目：

```
<en ts="2004-12-08T00:40:26.70" pi="0d3730.10.43" sc="tcp_local"
dc="l" ac="E" sz="12" so="info-E8944AE8D033CB92C2241E@whittlesong.com"
od="rfc822;ned+2Bcharsets@mauve.sun.com"
de="ned+charsets@mauve.sun.com" rf="22"
fi="/path/ZZ01LI4XPX0DTM00IKA8.00" ei="01LI4XPQR2EU00IKA8@mauve.sun.com"
mi="<11a3b401c4dd01$7c1c1ee0$1906fad0@elara>" us=""
ss="elara.whittlesong.com ([208.250.6.25])"
in="ned+charsets@mauve.sun.com" ia="ietf-charsets@innosoft.com"
fl="spamfilter1:rvLiXh158xWdQKa9iJ0d7Q==, addheader, keep"/>
```

请注意，为了清晰起见，该条目进行了换行，实际日志文件条目总是以单行显示的。

连接 (co) 条目可以具有以下属性：

```
ts - time stamp (always present, also used in en entries)
no - node name (present if LOG_NODE=1, also used in en entries)
pi - process id (present if LOG_PROCESS=1, also used in en entries)
sc - source channel (always present, also used in en entries)
dr - direction (always present)
ac - action (always present, also used in en entries)
tr - transport information (always present, also used in en entries)
ap - application information (always present, also used in en entries)
mi - message id (present only if message id info available,
     also used in en entries)
us - username (present only if username information available, also
     used in en entries)
di - diagnostic (present only if diagnostic information available,
     also used in en entries)
ct - the amount of time a message has spent in the queue (LOG_QUEUE_TIME=1,
also used in en entries)
```

下面是一个 co 条目示例：

```
<co ts="2004-12-08T00:38:28.41" pi="1074b3.61.281" sc="tcp_local" dr="+"
ac="O" tr="TCP|209.55.107.55|25|209.55.107.104|33469" ap="SMTP"/>
```

标题 (he) 条目具有以下属性：

```
ts - time stamp (always present, also used in en entries)
no - node name (present if LOG_NODE=1, also used in en entries)
pi - process id (present if LOG_PROCESS=1, also used in en entries)
va - header line value (always present)
```

下面是一个 he 条目示例：

```
<he ts="2004-12-08T00:38:31.41" pi="1074b3.61.281" va="Subject: foo"/>
```

▼ 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。**
   默认值为 0，表示邮件 ID 未保存在 `mail.log` 文件中。

▼ 记录邮件在队列中花费的时间

1 **编辑 MTA 选项文件。**

2 **将 LOG_QUEUE_TIME 选项设置为 1。**

该选项记录邮件在队列中花费的时间。队列时间记录为一个整数值（以秒为单位）。在非 XML 格式日志中，该值紧接应用程序信息字符串之后显示。在 XML 格式日志中，该值的属性名为 qt。

▼ 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。也可以将连接日志条目写入 connection.log* 文件。有关详细信息，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改写入 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，此选项通过进程 ID 启用连接条目与对应的邮件条目的关联关系。

▼ 将与使邮件加入队列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相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）。

25.3.4 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。本节包含以下几个部分：

- 第 717 页中的 “25.3.4.1 MTA 日志记录示例：用户发送外发邮件”
- 第 717 页中的 “25.3.4.2 MTA 日志记录示例：包括可选日志记录字段”
- 第 718 页中的 “25.3.4.3 MTA 日志记录示例：发送到列表”
- 第 719 页中的 “25.3.4.4 MTA 日志记录：发送到不存在的域”
- 第 721 页中的 “25.3.4.5 MTA 日志记录示例：发送至不存在的远程用户”
- 第 722 页中的 “25.3.4.6 MTA 日志记录示例：拒绝远程端提交邮件的尝试”
- 第 723 页中的 “25.3.4.7 MTA 日志记录示例：多次传送尝试”
- 第 724 页中的 “25.3.4.8 MTA 日志记录：通过转换通道路由外来 SMTP 邮件”
- 第 725 页中的 “25.3.4.9 MTA 日志记录示例：出站连接日志记录”
- 第 727 页中的 “25.3.4.10 MTA 日志记录示例：入站连接日志记录”

有关其他可选字段的说明，请参见第 711 页中的 “25.3.3 指定附加 MTA 日志记录选项”。

注 – 由于印刷版式原因，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。

如果您希望有关至同一收件人的同一邮件的特定条目相关联，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），如果希望将远程系统的 TCP 连接与已发送的邮件相关联，则启用 `LOG_PROCESS` 和 `LOG_CONNECTION` 的某一级别。

25.3.4.1 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。

示例 25–1 MTA 日志记录：本地用户发送外发邮件

```
16-Feb-2007 15:41:32.36 tcp_intranet tcp_local    EE 1        (1)
adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com     (2)
siroe.com (siroe.com [192.160.253.66])

16-Feb-2007 15:41:34.73 tcp_local                 DE 1        (3)
adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com     (4)
thor.siroe.com dns;thor.siroe.com

(TCP|206.184.139.12|2788|192.160.253.66|25)                   (5)

(thor.siroe.com ESMTP Sendmail ready Thu 15 Feb 2007 21:37:29 -0700 [MST])     (6)

smtp;250 2.1.5 <marlowe@siroe.com>... Receipt ok              (7)
```

1. 此行显示了一 (1) 块邮件使用 ESMTP (EE) 从 tcp_intranet 通道到 tcp_local 通道入队列的日期和时间。
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。这里显示了信封 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) 块邮件使用 ESMTP (DE) 从 tcp_local 通道出队列的日期和时间，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，以及信封 To: 地址的当前格式。
5. 显示了与之建立连接的实际系统在 DNS 中名为 thor.siroe.com，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。

25.3.4.2 MTA 日志记录示例：包括可选日志记录字段

该示例显示了类似于示例 25–3 中所示的日志记录条目，其中 LOG_FILENAME=1 和 LOG_MESSAGE_ID=1 显示文件名（下面的 1 和 3）和邮件 ID（下面的 2 和 4）。. 特别是邮件 ID 可用于将条目与邮件相关联。

示例 25–2 MTA 日志记录：包括可选日志记录字段

```
16-Feb-2007 15:41:32.36 tcp_intranet tcp_local    EE 1
adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
/opt/SUNWmsgsr/data/queue/tcp_local/002/ZZf0r4i0Wdy51.01      (1)
<0JDJ00D02IBWDX00@sesta.com>                                  (2)
siroe.com (siroe.com [192.160.253.66])

16-Feb-2007 15:41:34.73 tcp_local                 DE 1
adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
/opt/SUNWmsgsr/data/queue/tcp_local/002/ZZf0r4i0Wdy51.01      (3)
<0JDJ00D02IBWDX00@sesta.com>                                  (4)
thor.siroe.com dns;thor.siroe.com
(TCP|206.184.139.12|2788|192.160.253.66|25)
(thor.siroe.com ESMTP Sendmail ready at Thu, 15 Feb 2007 21:37:29 -0700 [MST])
smtp;250 2.1.5 <marlowe@siroe.com>... Recipient ok
```

25.3.4.3 MTA 日志记录示例：发送到列表

此示例对启用 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 邮件列表 test-list@sesta.com，此邮件列表已扩展到 bob@sesta.com、carol@varrius.com 和 david@varrius.com。请注意每个收件人的原始信封 To: 地址对每个收件人都是 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 是如何保持一致的，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）。

示例 25–3 MTA 日志记录：发送到列表

```
20-Feb-2007 14:00:16.46 tcp_local    tcp_local    EE 1
adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
/opt/SUNWmsgsr/data/queue/tcp_local/004/ZZf0r2D0yuej4.01
<0JDQ00706R0FX100@sesta.com>
siroe.com (siroe.com [192.160.253.66])

20-Feb-2007 14:00:16.47 tcp_local    tcp_local    EE 1
adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
/opt/SUNWmsgsr/data/queue/tcp_local/004/ZZf0r2D0yuej4.01
<0JDQ00706R0FX100@sesta.com>
siroe.com (siroe.com [192.160.253.66])

20-Feb-2007 14:00:16.48 tcp_local    ims-ms       EE 1
adam@sesta.com rfc822;test-list@sesta.com bob@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/008/ZZf0r2D0yuej6.01
<0JDQ00706R0FX100@sesta.com>
siroe.com (siroe.com [192.160.253.66])

20-Feb-2007 14:00:16.68 ims-ms                    D 1
```

示例 25–3 MTA 日志记录：发送到列表 （续）

```
adam@sesta.com rfc822;test-list@sesta.com bob@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/008/ZZf0r2D0yuej6.01
<0JDQ00706R0FX100@sesta.com>

20-Feb-2007 14:00:17.73 tcp_local                DE 1
adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
/opt/SUNWmsgsr/data/queue/tcp_local/004/ZZf0r2D0yuej4.01
<0JDQ00706R0FX100@sesta.com>
gw.varrius.com dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
(gw.varrius.com -- SMTP Sendmail)
smtp;250 2.1.5 <carol@varrius.com >... Recipient ok

20-Feb-2007 14:00:17.75 tcp_local                DE 1
adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
/opt/SUNWmsgsr/data/queue/tcp_local/004/ZZf0r2D0yuej4.01
<0JDQ00706R0FX100@sesta.com>
gw.varrius.com dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
(gw.varrius.com -- SMTP Sendmail)
smtp;250 2.1.5 <david@varrius.com>... Recipient ok
```

25.3.4.4 MTA 日志记录：发送到不存在的域

此示例对尝试发送到不存在的域（此处为 `very.bogus.com`）进行了说明；即，发送到未被 MTA 的重写规则发现其不存在的、并且被 MTA 匹配到外发 TCP/IP 通道的域名。此示例假设 MTA 选项设置为 `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 [5] 中所示的“拒绝”条目 (R)，以及 [6] 中所示的 DNS 返回的错误（指示该域名为非法域名）。

由于提交邮件后地址被拒绝，MTA 将生成退回邮件给原发送人。MTA 将新拒绝邮件加入队列以发送给原发送人 (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（例如退回邮件）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 生成的退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 (3) 的邮件 ID。（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)。

示例 25–4 MTA 日志记录：发送到不存在的域

```
20-Feb-2007 14:17:07.77 tcp_intranet tcp_local    E 1
adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
/opt/SUNWmsgsr/data/queue/tcp_local/008/ZZf0r2D0CVaL0.00
```

示例 25–4 MTA 日志记录：发送到不存在的域 （续）

```
<0JDQ00903RS89T00@sesta.com>
siroe.com (siroe.com [192.160.253.66])

20-Feb-2007 14:17:08.24 tcp_local    process      E 1       (1)
rfc822;adam@sesta.com adam@sesta.com                        (2)
/opt/SUNWmsgsr/data/queue/process/ZZf0r2D0CVbR0.00
<0JDQ00904RSK9Z00@sesta.com>,<0JDQ00903RS89T00@sesta.com>   (3)
tcp-daemon.mailhost.sesta.com

20-Feb-2007 14:17:08.46 tcp_local    process      E 1       (4)
rfc822;postmaster@sesta.com postmaster@sesta.com
/opt/SUNWmsgsr/data/queue/process/ZZf0r2D0CVbR1.00
<0JDQ00906RSK9Z00@sesta.com>,<0JDQ00903RS89T00@sesta.com>
tcp-daemon.mailhost.sesta.com

20-Feb-2007 14:17:08.46 tcp_local                 R 1       (5)
adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
/opt/SUNWmsgsr/data/queue/tcp_local/008/ZZf0r2D0CVaL0.00
<0JDQ00903RS89T00@sesta.com>
Illegal host/domain name found                              (6)
(TCP active open: Failed gethostbyname() on very.bogus.com, resolver errno = 1)

20-Feb-2007 14:17:09.21 process      ims-ms       E 3       (7)
rfc822;adam@sesta.com adam@ims-ms-daemon                    (8)
/opt/SUNWmsgsr/data/queue/ims-ms/018/ZZf0r2D0CVbS1.00
<0JDQ00904RSK9Z00@sesta.com>
process-daemon.mailhost.sesta.com

20-Feb-2007 14:17:09.72 process      ims-ms       E 3
rfc822;postmaster@sesta.com postmaster@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/014/ZZf0r2D0CVbS2.00
<0JDQ00906RSK9Z00@sesta.com>
process-daemon.mailhost.sesta.com

20-Feb-2007 14:17:09.73 ims-ms                    D 3
rfc822;adam@sesta.com adam@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/018/ZZf0r2D0CVbS1.00
<0JDQ00904RSK9Z00@sesta.com>

20-Feb-2007 14:17:09.84 ims-ms                    D 3
rfc822;postmaster@sesta.com postmaster@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/014/ZZf0r2D0CVbS2.00
<0JDQ00906RSK9Z00@sesta.com>
```

25.3.4.5 MTA 日志记录示例：发送至不存在的远程用户

此示例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。但与示例 25–4 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。

示例 25–5 MTA 日志记录：发送至不存在的远程用户

```
26-Feb-2007 13:56:35.16 tcp_intranet tcp_local    EE 1
adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
/opt/SUNWmsgsr/data/queue/tcp_local/000/ZZf0s690a3mf2.01
<0JE100J08UU24H00@sesta.com>
siroe.com (siroe.com [192.160.253.66])

26-Feb-2007 13:56:35.19 tcp_local    process      E 1
rfc822;adam@sesta.com adam@sesta.com
/opt/SUNWmsgsr/data/queue/process/ZZf0s690a3ml2.00
<0JE100J09UUB4N00@sesta.com>,<0JE100J08UU24H00@sesta.com>
tcp-daemon.mailhost.sesta.com

26-Feb-2007 13:56:35.20 tcp_local    process      E 1
rfc822;postmaster@sesta.com postmaster@sesta.com
/opt/SUNWmsgsr/data/queue/process/ZZf0s690a3ml3.00
<0JE100J0BUUB4N00@sesta.com>,<0JE100J08UU24H00@sesta.com>
tcp-daemon.mailhost.sesta.com

26-Feb-2007 13:56:35.20 tcp_local                 RE 1          (1)
adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
/opt/SUNWmsgsr/data/queue/tcp_local/000/ZZf0s690a3mf2.01
<0JE100J08UU24H00@sesta.com>
thor.siroe.com dns;thor.siroe.com
(TCP|206.184.139.12|2788|192.160.253.66|25)                   (2)
(thor.siroe.com -- Server ESMTP [Sun Java System Messaging
Server 6.2-8.01 [built Feb 16 2007]])
smtp;550 5.1.1 unknown or illegal alias: nonesuch@siroe.com   (3)

26-Feb-2007 13:56:35.62 process      ims-ms       E 4
rfc822;adam@sesta.com adam@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/003/ZZf0s690a3mm5.00
<0JE100J09UUB4N00@sesta.com>
process-daemon.mailhost.sesta.com

26-Feb-2007 13:56:36.07 process      ims-ms       E 4
rfc822;postmaster@sesta.com postmaster@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/016/ZZf0s690a3nm7.01
```

示例 25–5 MTA 日志记录：发送至不存在的远程用户 （续）

```
<0JE100J0BUUB4N00@sesta.com>
process-daemon.mailhost.sesta.com

26-Feb-2007 13:56:35.83 ims-ms                    D 4
rfc822;adam@sesta.com adam@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/003/ZZf0s690a3mm5.00
<0JE100J09UUB4N00@sesta.com>

26-Feb-2007 13:56:36.08 ims-ms                    D 4
rfc822;postmaster@sesta.com postmaster@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/016/ZZf0s690a3nm7.01
<0JE100J0BUUB4N00@sesta.com>
```

25.3.4.6 MTA 日志记录示例：拒绝远程端提交邮件的尝试

此示例对当 MTA 拒绝远程端提交邮件的尝试时所产生的日志文件条目的类别进行了说明。（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，示例是对已使用 ORIG_SEND_ACCESS 映射设置了 SMTP 中继阻止（请参见第 497 页中的 “18.7 配置 SMTP 中继阻止”）的 MTA 而言的，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。

示例 25–6 MTA 日志记录：拒绝远程端提交邮件的尝试

```
26-Feb-2007 14:10:06.89 tcp_local                 JE 0  (1)
harold@varrius.com rfc822; alan@very.bogus.com                (2)
530 5.7.1 Relaying not allowed: alan@very.bogus.com           (3)
```

1. 此日志显示了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情况以 R 记录表示，如示例 25–4 和示例 25–5 中所示）。

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。

示例 25–6 MTA 日志记录：拒绝远程端提交邮件的尝试 （续）

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。

25.3.4.7 MTA 日志记录示例：多次传送尝试

此示例对在第一次尝试时不能发送邮件所产生的日志文件条目的类别进行了说明，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`。

示例 25–7 MTA 日志记录：多次传送尝试

```
26-Feb-2007 14:38:16.27 tcp_intranet tcp_local    EE 1           (1)
adam@sesta.com rfc822;user@some.org user@some.org
/opt/SUNWmsgsr/data/queue/tcp_local/001/ZZf0s690kN_y0.00
<0JE100L05WRJIC00@sesta.com>

26-Feb-2007 14:38:16.70 tcp_local                 Q 1                    (2)
adam@sesta.com rfc822;user@some.org user@some.org
/opt/SUNWmsgsr/data/queue/tcp_local/001/ZZf0s690kN_y0.00                 (3)
<0JE100L05WRJIC00@sesta.com>
TCP active open: Failed connect() 192.1.1.1:25  Error: no route to host  (4)

...several hours worth of entries...

26-Feb-2007 16:58:11.20 tcp_local                 Q 1                    (5)
adam@sesta.com rfc822;user@some.org user@some.org
/opt/SUNWmsgsr/data/queue/tcp_local/001/ZYf0s690kN_y0.01                 (6)
<0JE100L05WRJIC00@sesta.com>
TCP active open: Failed connect() 192.1.1.1:25    Error: no route to host

...several hours worth of entries...

26-Feb-2007 19:15:12.11 tcp_local                 Q 1
adam@sesta.com rfc822;user@some.org user@some.org
/opt/SUNWmsgsr/data/queue/tcp_local/001/ZXf0s690kN_y0.00                  (7)
<0JE100L05WRJIC00@sesta.com>
TCP active open: Failed connect() 192.1.1.1:25  Error: Connection refused (8)

...several hours worth of entries...

26-Feb-2007 22:41:12.63 tcp_local                 DE 1                    (9)
adam@sesta.com rfc822;user@some.org user@some.org
/opt/SUNWmsgsr/data/queue/tcp_local/001/ZXf0s690kN_y0.00
<0JE100L05WRJIC00@sesta.com>
```

示例 25–7 MTA 日志记录：多次传送尝试 （续）

```
host.some.org dns;host.some.org (TCP|206.184.139.12|2788|192.1.1.1|25)
(All set, fire away)
smtp;250 2.1.5 <user@some.org >... Recipient ok
```

1. 邮件进入 tcp_internal 通道—可能来自 POP 或 IMAP 客户端，或可能来自使用 MTA 作为 SMTP 中继的组织中的其他主机；MTA 将其加入到 tcp_local 外发通道队列。
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。与示例 25–4 不同，DNS 并非拒绝目标域名 some.org；而是，"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. 文件名现在为 ZY*，表示这是第二次尝试。
7. 第三次未成功尝试的文件名是 ZX*。
8. 下一次定期作业重新尝试传送，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邮件而无法在 MTA 尝试连接时接受连接。）
9. 最终对邮件取消排队。

25.3.4.8 MTA 日志记录：通过转换通道路由外来 SMTP 邮件

此示例对通过转换通道路由邮件的情况进行了说明。假设此站点具有 CONVERSIONS 映射表，例如：

```
CONVERSIONS
   IN-CHAN=tcp_local;OUT-CHAN=ims-ms;CONVERT Yes
```

本示例假设选项设置为 LOG_FILENAME=1 和 LOG_MESSAGE_ID=1。

示例 25–8 MTA 日志记录：通过转换通道路由外来 SMTP 邮件

```
26-Feb-2007 15:31:04.17 tcp_local    conversion   EE 1   (1)
amy@siroe.edu rfc822;bert@sesta.com bert@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/conversion/ZZf0s090wFwx2.01
<0JE100206Z7J5F00@siroe.edu>

26-Feb-2007 15:31:04.73 conversion   ims-ms       E 1          (2)
amy@siroe.edu rfc822;bert@sesta.com bert@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/007/ZZf0s090wMwq1.00
<0JE100206Z7J5F00@siroe.edu>
```

示例 25–8 MTA 日志记录：通过转换通道路由外来 SMTP 邮件 （续）

```
26-Feb-2007 15:31:04.73 conversion                D 1          (3)
amy@siroe.edu rfc822;bert@sesta.com bert@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/conversion/ZZf0s090wFwx2.01
<0JE100206Z7J5F00@siroe.edu>

26-Feb-2007 15:31:04.73 ims-ms                    D 1          (4)
amy@siroe.edu rfc822;bert@sesta.com bert@ims-ms-daemon
/opt/SUNWmsgsr/data/queue/ims-ms/007/ZZf0s090wMwq1.00
<0JE100206Z7J5F00@siroe.edu>
```

1. 来自外部用户 amy@siroe.edu 的邮件进入，其收件人地址为 `ims-ms` 通道收件人 bert@sesta.com 的地址。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 `ims-ms` 通道）。
2. 转换通道运行并将邮件排到 `ims-ms` 通道队列。
3. 然后转换通道可以使邮件出队列（删除旧邮件文件）。
4. 最后，`ims-ms` 通道使邮件出队列（传送）。

25.3.4.9 MTA 日志记录示例：出站连接日志记录

此示例说明了通过 `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 `LOG_PROCESS=1`、`LOG_MESSAGE_ID=1` 和 `LOG_FILENAME=1`。本示例显示了用户 `adam@sesta.com` 将同一邮件（请注意每个邮件副本的邮件 ID 都相同）发送给三个收件人 `bobby@hosta.sesta.com`、`carl@hosta.sesta.com` 和 `dave@hostb.sesta.com` 的情况。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，系统将在磁盘上为不同主机名的每组收件人分别创建邮件文件，其中 `bobby@hosta.sesta.com` 和 `carl@hosta.sesta.com` 收件人存储在同一邮件文件中，而 `dave@hostb.sesta.com` 收件人存储在另一邮件文件中。

示例 25–9 MTA 日志记录：出站连接日志记录

```
28-Feb-2007 09:13:19.18 409f.3.1 tcp_intranet tcp_local    EE 1
adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
/opt/SUNWmsgsr/data/queue/tcp_local/000/ZZf0s4g0G2Zt0.00           (1)
<0JE500C0371HRJ00@sesta.com>
siroe.com (siroe.com [192.160.253.66])

28-Feb-2007 09:13:19.18 409f.3.1 tcp_intranet tcp_local    EE 1
adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
/opt/SUNWmsgsr/data/queue/tcp_local/000/ZZf0s4g0G2Zt0.00           (2)
<0JE500C0371HRJ00@sesta.com>
siroe.com (siroe.com [192.160.253.66])
```

示例 25–9 MTA 日志记录：出站连接日志记录 （续）

```
28-Feb-2007 09:13:19.19 409f.3.2 tcp_intranet tcp_local    EE 1
adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
/opt/SUNWmsgsr/data/queue/tcp_local/004/ZZf0s4g0G2Zt1.00            (3)
<0JE500C0371HRJ00@sesta.com>
siroe.com (siroe.com [192.160.253.66])

28-Feb-2007 09:13:19.87 40a5.2.0 tcp_local    -  O                  (4)
TCP|206.184.139.12|5900|206.184.139.66|25
SMTP/hostb.sesta.com/mailhub.sesta.com                              (5)

28-Feb-2007 09:13:20.23 40a5.3.4 tcp_local    -  O                  (6)
TCP|206.184.139.12|5901|206.184.139.70|25
SMTP/hosta.sesta.com/hosta.sesta.com                                (7)

28-Feb-2007 09:13:20.50 40a5.2.5 tcp_local                 DE 1
adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
/opt/SUNWmsgsr/data/queue/tcp_local/000/ZZf0s4g0G2Zt0.00
<0JE500C0371HRJ00@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 [Sun Java System Messaging Server
6.2-8.01 [built Feb 16 2007]])
smtp;250 2.1.5 bobby@hosta.sesta.com and options OK.

28-Feb-2007 09:13:20.50 40a5.2.5 tcp_local                 DE 1
adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
/opt/SUNWmsgsr/data/queue/tcp_local/000/ZZf0s4g0G2Zt0.00
<0JE500C0371HRJ00@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 [Sun Java System Messaging Server
6.2-8.01 [built Feb 16 2007]])
smtp;250 2.1.5 carl@hosta.sesta.com and options OK.

28-Feb-2007 09:13:20.50 40a5.2.6 tcp_local    -  C                  (9)
TCP|206.184.139.12|5901|206.184.139.70|25
SMTP/hosta.sesta.com/hosta.sesta.com

28-Feb-2007 09:13:21.13 40a5.3.7 tcp_local                 DE 1
adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
/opt/SUNWmsgsr/data/queue/tcp_local/004/ZZf0s4g0G2Zt1.00
<0JE500C0371HRJ00@sesta.com>
mailhub.sesta.com dns;mailhub.sesta.com
(TCP|206.184.139.12|5900|206.184.139.66|25)
(mailhub.sesta.com ESMTP Sendmail ready at Tue, 27 Feb 2007 22:19:40 GMT)
smtp;250 2.1.5 <dave@hostb.sesta.com>... Recipient ok
```

示例 25–9 MTA 日志记录：出站连接日志记录 （续）

```
28-Feb-2007 09:13:21.33 40a5.3.8 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 40a5）。
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 客户端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 客户端在单独的线程中（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 客户端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. 由于完成了邮件（在本例中为 dave）的传送，因此连接 mailhub.sesta.com 关闭。

25.3.4.10 MTA 日志记录示例：入站连接日志记录

此示例说明了通过 LOG_CONNECTION=3 启用连接日志记录后外来 SMTP 邮件的日志输出。

示例 25–10 MTA 日志记录：入站连接日志记录

```
28-Feb-2007 11:50:59.10 tcp_local + O                  (1)
TCP|206.184.139.12|25|192.160.253.66|1244 SMTP         (2)

28-Feb-2007 11:51:15.12 tcp_local    ims-ms    EE 1
service@siroe.com rfc822;adam@sesta.com adam@ims-ms-daemon
```

示例 25–10 MTA 日志记录：入站连接日志记录 （续）

```
THOR.SIROE.COM (THOR.SIROE.COM [192.160.253.66])       (3)

28-Feb-2007 11:51:15.32 ims-ms                  D 1
service@siroe.com rfc822;adam@sesta.com adam@ims-ms-daemon

28-Feb-2007 11:51:15.66 tcp_local + C                  (4)
TCP|206.184.139.12|25|192.160.253.66|1244 SMTP
```

1. 远程系统打开一个连接。字符 `O` 表示此条目与打开连接有关；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. 在将外来 TCP/IP 通道 (`tcp_local`) 的邮件加入 `ims-ms` 通道收件人队列的条目中，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 行中声明的名称、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；请参见第 12 章行为。
4. 关闭入站连接。字符 `C` 表示此条目与关闭连接有关；字符 `+` 表示此条目与外来连接有关。

25.3.5 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*`/config/dispatcher.cnf` 文件中指定分发程序配置信息。安装时将创建一个默认的配置文件，可不必对其进行更改而直接使用。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。

表 25–5 分发程序调试位

位			用法
	十六进制值	十进制值	
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	基本服务分发程序其他调试。
4	x 00010	16	基本服务调试。

表 25–5 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。

▼ 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。**

   您还可以设置逻辑变量或环境变量 `IMTA_DISPATCHER_DEBUG` (UNIX)，它以十六进制将 32 位调试掩码定义为值 `FFFFFFFF`。上表介绍了每个位的含义。

▼ 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`，然后把对每项服务计算的值相加。系统的堆大小必须至少是此数目的两倍。**

25.4 管理消息存储、Admin 和 Default 服务的日志

本节介绍了消息存储（POP、IMAP 和 HTTP）、Admin 和 Default 服务的日志记录。（请参见表 25–1。）

对于这些服务，您可以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：

25.4.1 了解服务日志特性

本节描述了消息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。

25.4.1.1 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 733 页中的 “25.4.3 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对日志事件的搜索。表 25–6 对可用级别进行了说明。这些日志记录级别是 UNIX `syslog` 工具所定义的级别的子集。

表 25–6 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。每当发生严重问题或紧急情况（例如服务器无法访问邮箱或其运行所需的库）时，将一个事件写入日志。
Error	每当发生错误情况（例如尝试连接到客户端或其他服务器失败）时，将一个事件写入日志。
Warning	每当发生警告情况（例如服务器无法理解客户端所发送的通信）时，将一个事件写入日志。
Notice	每当发生通知（正常但重要的情况，例如用户登录失败或会话关闭）时，将一个事件写入日志。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，将一个事件写入日志。
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“**通知**”。

注 – 指定的日志记录越详细，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 733 页中的 “25.4.3 定义和设置服务日志记录选项”。

25.4.1.2 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 25–7 列出了 Messaging Server 为日志记录目的所标识的类别。

表 25–7 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）

表 25–7 日志事件的发生类别 （续）

设备	说明
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	与访问消息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 735 页中的 “25.4.4 搜索并查看服务日志”。

25.4.1.3 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 733 页中的 “25.4.3 定义和设置服务日志记录选项”。

25.4.2 了解服务日志文件格式

所有由 Messaging Server 创建的消息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 25–8 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 25–8 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 GMT +/- *hhmm* 表示。例如：`02/Jan/1999:13:08:21 -0700`

表 25–8 存储和管理日志文件组件 （续）

组件	定义
hostName	服务器在其上运行的主机名：例如，`showshoe`。 **注释**：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	事件所属的类别：例如，`General`（请参见示例 25–5）。
logLevel	事件所表示的日志记录级别：例如，`Notice`（请参见示例 25–4）。
eventMessage	可为任意长度的特定于事件的解释消息：例如，`Log created (894305624)`。

以下是三个已记录事件的示例：

```
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。以上示例中包含：0 115 0。第一个数字是客户端发送的字节数，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、类别或特定的进程 ID）来限制显示的事件。有关详细信息，请参见第 735 页中的 “25.4.4 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。

25.4.3 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消息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。

25.4.3.1 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轮转和备份策略。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。

25.4.3.2 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

允许的所有日志文件的最大大小总计：20 MB

允许的最小可用磁盘空间：5 MB

日志轮转时间：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。）

25.4.3.3 了解日志记录选项

您可以通过命令行来设置控制消息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。
- 选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选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。

25.4.4 搜索并查看服务日志

日志文件提供了用于查看消息存储和管理日志数据的基本界面。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。

25.4.4.1 搜索参数

以下是可以指定用于查看日志数据的有用搜索参数：

- **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今天的事件。
- **日志记录的级别**。您可以指定日志记录的级别（请参见第 730 页中的 “25.4.1.1 日志记录级别”）。例如，选取“紧急”查看服务器关闭的原因，或者选取“错误”查找失败的协议调用。
- **工具**。您可以指定工具（请参见第 731 页中的 “25.4.1.2 日志事件的类别”）。例如，如果确信服务器崩溃涉及磁盘错误，则选择“存储”，或如果问题在于 IMAP 协议命令错误，则选择“协议”。
- **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部分（请参见第 732 页中的 “25.4.2 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、进程 ID 和事件消息的任何部分（例如远程主机名、函数名、错误号等）。

  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`）

`?` 任何单个字符（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]`）

`\` 转义符：置于 `*`、`?`、`[` 或 `]` 之前以将这些符号用作字面值

注释：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

25.4.5 处理服务日志

本节介绍了如何通过使用 `configutil` 命令来处理服务日志，以便搜索和查看日志。其中包含以下各节：

- 第 737 页中的 “向系统日志发送服务日志”

▼ 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对应的 `syslog` 工具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。

25.4.5.1 禁用 HTTP 日志记录

如果系统不支持 HTTP 邮件访问（即 Webmail），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 Webmail 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* 指定了日志文件的最大数目。

▼ 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量。

▼ 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量。

25.4.5.2 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量。

25.4.6 使用消息存储日志记录的邮件跟踪

您可以通过邮件 ID 使用消息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。

要在消息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。

消息存储日志记录可以跟踪以下操作：

- 附加—消息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消息存储的邮件。
- 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，正文获取将参考检索邮件正文的某一部分的时间。
- 清除：IMAP 术语，此处已扩展为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.mstrace.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** 消息存储端日志。（**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"
```

25.4.7 其他消息存储日志记录功能

Messaging Server 提供了一种称为自动测量的功能，可以将用户的全部 IMAP 或 POP 会话捕获到文件中。此功能对调试客户端问题很有用。例如，如果用户抱怨他们的邮件访问客户端未按预期那样工作，则此功能可用于跟踪访问客户端和 Messaging Server 之间的交互活动。请参见第 587 页中的 “20.14.1.3 使用自动测量功能检查用户 IMAP/POP/Webmail 会话” 。

25.4.8 消息存储日志记录示例

记录在消息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。

25.4.8.1 消息存储日志记录示例：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送给客户端，但系统将记录真实原因（无效密码）。

示例 25–11 消息存储日志记录：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
```

25.4.8.2 消息存储日志记录：禁用的帐户

以下示例显示了用户无法登录的原因是由于帐户被禁用。此外，禁用的帐户被说明为 "(inactive)" 或 "(hold)"。 ”

示例 25–12 消息存储日志记录：禁用的帐户

```
[30/Aug/2004:16:53:31 -0700] vadar imapd[13027]: Account Notice: badlogin:
[192.18.126.64:40720] plaintext user3 account disabled (hold)
```

25.4.8.3 消息存储日志记录示例：附加的邮件

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。消息存储日志记录了所有通过 `ims_master` 和 `lmtp` 通道进入消息存储的邮件。记录用户 ID、文件夹、邮件大小和邮件 ID 的“附加”。

示例 25–13 消息存储日志记录：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>
```

25.4.8.4 消息存储日志记录示例：客户端检索的邮件

当客户端检索邮件时，消息存储日志将写入“获取”消息。消息存储日志将至少记录客户端对一个正文部分的所有获取。记录“获取”的用户 ID、文件夹和邮件 ID。

示例 25–14 消息存储日志记录：客户端检索的邮件

```
[31/Aug/2004:15:55:26 -0700] vadar imapd[13729]: Store Information:
fetch:user1:user/user1:<Roam.SIMC.2.0.6.1093051161.3655.user1@vad.siroe.com>
```

25.4.8.5 消息存储日志记录示例：从文件夹删除的邮件

示例 25–15 消息存储日志记录示例：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，消息存储将写入“清除”消息。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。

```
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>
```

25.4.8.6 消息存储日志记录示例：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。以下为常规登录邮件：

示例 25–16 消息存储日志记录：登录

```
[30/Aug/2004:16:53:13 -0700] vadar imapd[13027]: Account Information: login
[192.18.126.64:40718] user1 plaintext
```

◆ ◆ ◆ 第 26 章

26 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。其中包含以下各节：

相关主题（监视过程）可在第 27 章中找到。

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 中有关 MTA 配置和命令行实用程序的章节。

26.1 故障排除概述

对 MTA 进行故障排除的首要步骤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。

26.2 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。

26.2.1 检查 MTA 配置

使用`imsimta test -rewrite` 实用程序测试您的地址配置。使用该实用程序，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。有关详细信息，请参阅《Sun Java System Messaging Server 6.3 Administration Reference》中的第 2 章 “Message Transfer Agent Command-line Utilities”中关于 MTA 命令行实用程序的内容。

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。

26.2.2 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 邮件队列目录中。有关 `imsimta qm` 的详细信息，请参阅 《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimta qm” 中关于 MTA 命令行实用程序的内容以及第 788 页中的 “27.8.6 imsimta qm counters”。

如果 `imsimta test -rewrite` 输出看上去是正确的，请检查邮件是否确实放到了 MTA 邮件队列子目录中。要执行此操作，请启用目录 */msg-svr-base*`/log/` 中的邮件日志记录（有关 MTA 日志记录的详细信息，请参见第 707 页中的 “25.3 管理 MTA 邮件和连接日志”）。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。

26.2.3 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 `mailsrv`）。此帐户应该拥有以下目录、子目录和文件：

msg-svr-base/data/queue/
msg-svrbase/data/log
msg-svr-base/data/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
drwxr-x---   2 mailsrv  mail 512 Jan  4 16:09 /opt/SUNWmsgsr/data/queue/

ls -l -p -d /opt/SUNWmsgsr/data/log
drwxr-x---   2 mailsrv  mail  3072 Feb 16 12:07 /opt/SUNWmsgsr/data/log/

ls -l -p -d /opt/SUNWmsgsr/data/tmp
drwxr-x---   2 mailsrv  mail   512 Feb 16 12:55 /opt/SUNWmsgsr/data/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
```

26.2.4 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
mailsrv 9567 S 18416 9368  02:00:02  0:00  /opt/SUNWmsgsr/lib/tcp_smtp_server
mailsrv 6573 S 18112 5720  Jul_13    0:00  /opt/SUNWmsgsr/lib/job_controller
mailsrv 9568 S 18416 9432  02:00:02  0:00  /opt/SUNWmsgsr/lib/tcp_smtp_server
mailsrv 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 的详细信息，请参阅《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimta process”。

您还可以使用 `imsimta qm jobs` 按通道列出当前由作业控制器管理的所有活动的和暂挂的传送处理作业。为每个通道提供了额外的累积信息，例如成功传送的邮件文件数和那些重新排队以进行后续传送尝试的邮件的数量。命令语法如下所示：

```
jobs [-[no]hosts] [-[no]jobs] [-[no]messages] [channel-name]
```

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 `start-msg` 命令启动进程。有关详细信息，请参阅 《Sun Java System Messaging Server 6.3 Administration Reference》 中的“start-msg” 中关于 MTA 命令行实用程序的内容。

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正在处理分叉 (`fork()`) 子进程。但是，此类重复过程的时间范围很小。

26.2.5 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，则可以检查日志文件以查看发生的情况。所有 MTA 日志文件均在目录 */msg-svr-base*`/log` 中创建。表 26–1 显示了各种 MTA 处理作业的日志文件名称格式。

表 26–1 MTA 日志文件

文件名	日志文件内容
channel`_master.log-`*uniqueid*	*channel* 的主程序（通常为客户端上的程序）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，要获得详细的调试信息，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，要获得详细的调试信息，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（而非邮件）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，将创建此日志文件。

注 – 每个日志文件均使用唯一的 ID (*uniqueid*) 创建以避免覆写由同一通道以前创建的日志。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` 命令清除过时的日志文件。但请注意，默认情况下，此命令定期运行（请参见第 108 页中的 “4.6.2 预定义的自动任务”）。有关详细信息，请参见 《Sun Java System Messaging Server 6.3 Administration Reference》 中的“imsimta purge” 中关于 MTA 命令行实用程序的内容。

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` 文件中将 `mm_debug` 设置为非零值 (`mm_debug > 0`)，此文件所在目录为：`/`*msg-svr-base*` /config/`。

有关调试通道主程序和从程序的详细信息，请参见 Sun Java System Messaging Server Administration Reference。

26.2.6 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（特别是在为一个或多个通道启用调试后）将非常有帮助。

命令 `imsimta submit` 将通知 MTA 作业控制器运行通道。如果针对所述的通道启用了调试，则 `imsimta submit` 将在目录 `/`*msg-svr-base*`/log` 中创建一个日志文件，如表 26–1 所示。

命令 `imsimta run` 将在当前活动进程下执行通道的出站传送，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，请参阅 《Sun Java System Messaging Server 6.3 Administration Reference》 中的“Command Descriptions”。

26.2.7 启动和停止各个通道

在某些情况下，停止和启动各个通道可能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。

▼ 停止特定通道的出站处理（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` 命令的详细信息，请参见 《Sun Java System Messaging Server 6.3 Administration Reference》 中的“imsimta qm”。

26.2.7.1 从特定域或 IP 地址停止外来处理（进入通道队列）

将临时 SMTP 错误返回到客户主机时，如果要停止某个特定域或 IP 地址的入站邮件处理，请使用以下进程之一。执行此操作，邮件将不会保存在您的系统中。请参阅第 481 页中的 “18.1 第 1 部分：映射表”。

- 要停止特定主机或域名的入站处理，请将以下访问规则添加到 MTA 映射文件（通常为 */msg-svr-base*`/config/mappings`）的 ORIG_SEND_ACCESS 映射表中：

```
ORIG_SEND_ACCESS

  *|*@sesta.com|*|*        $X4.2.1|$NHost$ temporarily$ 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入站处理。

- 要停止特定 IP 地址的入站处理，请将以下访问规则添加到 MTA 映射文件（通常为 */msg-svr-base*`/config/mappings`）的 PORT_ACCESS 映射表中：

```
PORT_ACCESS

    TCP|*|25|IP_address_to_block|*    $N500$ can't$ connect$ now
```

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。

26.2.8 MTA 故障排除示例

本节说明如何逐步对特定 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”被称为“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 744 页中的 “26.2 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。

26.2.8.1 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，您可以在`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` 命令在目录 */ msg-svr-base*`/log` 的 `mail.log_current` 文件中搜索邮件的 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详细信息，请参阅第 708 页中的 “25.3.1 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。

26.2.8.2 手动启动和停止通道以收集数据

本节说明了如何手动启动和停止通道。请参见第 747 页中的 “26.2.7 启动和停止各个通道”。通过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 751 页中的 “识别邮件故障点”中介绍的内容。

▼ 手动启动和停止通道

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 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入站通道（或初始对话期间邮件被切换到的任意通道），使用 slave_debug 关键字。本示例中，slave_debug 关键字被添加到 tcp_local 通道。

   b. 将 master_debug 关键字添加到邮件所通过的并在第 749 页中的“ 26.2.8.1 识别邮件路径中的通道 ”中已经识别的其他通道。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 747 页中的“ 26.2.7 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，则该邮件将停留在此通道中。有关详细信息，请参见步骤 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 关键字添加到通道中。

   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将其加入邮件路径中的下一个目标通道队列。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，可以将文件另存为 tcp_intranet_master.keep，这样文件就不会被删除。

8 重复步骤 5 至步骤 7 直到邮件到达其最终目标。

在步骤 7 中复制的日志文件应该与在步骤 5 中复制的邮件文件相关联。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 中的 imta.cnf 文件的相应通道中删除 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有邮件组成部分。**

查看 SMTP 对话和数据以查看从客户端发送的内容。

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。这种情况下，问题可能发生在发件人的远程 SMTP 服务器或发件人的客户机上。

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（消息存储），则可以将邮件从服务器下载到客户机上，以确定邮件组成部分是在此传输期间还是在此之后丢失的。如果目标通道是 `tcp_*` 通道，则需要转至邮件路径中的 MTA。假定是 Messaging Server MTA，您将需要重复整个故障排除过程（请参见第 749 页中的 “26.2.8.1 识别邮件路径中的通道”、第 749 页中的 “26.2.8.2 手动启动和停止通道以收集数据”和本节内容）。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。

26.3 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。

26.3.1 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。

26.3.2 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. 重新建立所有客户端连接。

26.3.3 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。

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。有关详细信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimta process”。

26.3.4 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-*` 以获得相关错误消息。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，如果它是由 `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，因为它无法创建/访问套接字文件。此外，还可能出现与 Messaging Server 无关的其他问题。

26.3.5 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有关。以下技巧可用于识别造成外来 SMTP 连接超时的原因：

▼ 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，但是其他命令（如 ehlo 和 mail from）没有违反响应，则应运行 imsimta test -rewrite 以确保配置正确。

3 **如果 220 标题的响应时间较慢，并且在 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名称解析查找）：**

```
febe2c04 iii_res_send (fb7f4564, 28, fb7f4de0, 400, fb7f458c, fb7f4564) +
42c 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]
```

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，因此在 /etc/nsswitch.conf 文件中进行此更改可以提高性能。

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特征。例如，如果具有大量收件人的外来邮件超时，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。

26.3.6 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他主机连接运行完好，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。您可能会看到错误消息，例如“来自 smtp_open 的致命错误”。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，请使用诸如 PING、TRACEROUTE 和 NSLOOKUP 之类的实用程序。

以下示例显示了要查看邮件停留在等待传送到 `xtel.co.uk` 的队列中的原因时可能使用的步骤。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 329 页中的“12.4.3.5 TCP/IP MX 记录支持”。
2. 在此示例中，DNS（Domain Name Service，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，则可以跳过前两步。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。

26.3.6.1 创建新通道

在某些情况下，某个远程域可能出现故障，发送到该服务器的邮件数量可能会很大，以致外发通道队列将被无法传送的邮件填满。MTA 会尝试定期重新传送这些邮件（重试的频率和次数可以使用 `backoff` 关键字进行配置），正常情况下，不需要进行任何操作。但是，如果太多邮件阻塞在队列中，则其他邮件可能无法及时传送，因为所有通道作业都在处理积压的无法传送的邮件。

在这种情况下，您可以将这些邮件重新路由到在其自己的作业控制器池中运行的新通道。这将避免处理资源的争用并允许其他通道传送其邮件。下面介绍了此过程。我们先假定一个名为 siroe.com 的域。

▼ 创建新通道

1 创建名为 `tcp_siroe-daemon` 的新通道并为 `pool` 关键字添加新值。

在 */msg-svr-base/* `config/imta.cnf` 的通道块部分创建通道。该通道与常规外发 `tcp_*` 通道应具有相同的通道关键字。通常，该通道是处理所有出站 (Internet) 通信的 `tcp_local` 通道。由于 `siroe.com` 在 Internet 上，因此这就是要模仿的通道。新通道可能类似于如下所示：

```
tcp_siroe smtp nomx single_sys remotehost inner allowswitchchannel     \
dentnonenumeric subdirs 20 maxjobs 7 pool SMTP_SIROE maytlsserver      \
maysaslserver saslswitchchannel tcp_auth missingrecipientpolicy 0      \
tcp_siroe-daemon
```

注意新关键字-值对池 SMTP_SIROE。它指定传送到此通道的邮件将仅使用 SMTP_SIROE 池的计算机资源。另请注意，新通道的前后都需要留一个空白行。

2 将两个重写规则添加到 imta.cnf 文件的重写规则部分以将发往 siroe.com 的电子邮件定向到新通道。

新重写规则类似于如下所示：

```
siroe.com     $U%$D@tcp_siroe-daemon
.siroe.com      $U%$H$D@tcp_siroe-daemon
```

这些重写规则将发往 siroe.com（包括如 host1.siroe.com 或 hostA.host1.siroe.com 的地址）的邮件定向到正式主机名为 tcp_siroe-daemon 的新通道。这些规则的重写部分，

$U%$D 和 $U%$H$D，将保留邮件的原始地址。$U 复制原始地址的用户名。% 为分隔符，@ 位于用户名和域之间。$H 复制主机/域说明的不匹配部分（位于模式中点的左侧）。$D 复制域说明的匹配部分。

3 定义名为 SMTP_SIROE 的新作业控制器池。

在 */msg-svr-base/* config/job_controller.cnf 中添加以下内容：

```
[POOL=SMTP_SIROE]
job_limit=10
```

这将创建名为 SMTP_SIROE 的邮件资源池，该池最多可以允许 10 个作业同时运行。确保没有在该池定义和其他项之间留下任何空白行。有关作业和池的详细信息，请参见第 174 页中的 “8.7 作业控制器”。

4 重新启动 MTA。

发出以下命令：`imsimta cnbuild;imsimta restart`

该命令重新编译配置并重新启动作业控制器和分发程序。

本示例中，内部用户的大量电子邮件被发往名为 siroe.com 的特定远程站点。由于某些原因，siroe.com 临时不能接受外来 SMTP 连接，因此无法传送电子邮件。（此类情况并不是只在极少数情况下才发生。）

发往 siroe.com 的电子邮件传入时，外发通道队列（通常为 tcp_local）将被无法传送的邮件填满。MTA 会尝试定期重新传送这些邮件（重试的频率和次数可以使用 backoff 关键字进行配置），正常情况下，不需要进行任何操作。

但是，如果太多邮件阻塞在队列中，则其他邮件可能无法及时传送，因为所有通道作业都在处理积压的 siroe.com 邮件。在这种情况下，您可能希望将 siroe.com 邮件重新路由到在其自身的作业控制器池中运行的新通道（请参见第 174 页中的 “8.7 作业控制器”）。这将允许其他通道传送它们的邮件，而无需争用 siroe.com 邮件所使用的处理资源。下面将介绍如何创建新通道以解决此问题。

26.3.7 未传送 MTA 邮件

除了邮件传输问题，还有两种常见问题可能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，通道程序将在处理完新邮件后处理原来未处理的邮件。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` 后清除积压的邮件。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。

要获得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。

有关作业控制器的详细信息，请参见第 174 页中的 “8.7 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。

26.3.8 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 759 页中的 “26.3.8.1 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。您应该查看问题邮件文件在 MTA 队列区域时的副本、与问题邮件相关的 MTA 邮件日志条目（如果在 MTA 配置文件中为所述通道启用了

logging 通道关键字）和所述通道的 MTA 通道调试日志文件。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。

26.3.8.1 诊断和清理 .HELD 邮件

如果 MTA 检测到一个与邮件传送有关的严重问题，则邮件将被存储在 */msg-svr-base*/data/queue/ *channel* 中后缀为 .HELD 的文件中。例如：

```
% ls
ZZ0HXZ00G0EBRBCP.HELD
ZZ0HY200C0O6LGHU.HELD
ZZ0HYA006LP66O3H.HELD
ZZ0HZ7003EOQSE37.HELD
```

.HELD 文件的产生主要是由于以下三个原因：

- 循环邮件。MTA 检测到邮件通过建立某种 Received: 标题行进行循环。
- 用户或域状态被设置为 hold。通常在执行某些维护过程时（例如，在移动用户邮箱时），MTA 管理员会有意停止传送这些邮件。
- 可疑邮件。这些邮件满足某些成为可疑邮件的阈值，它们会被保留，在以后由 MTA 管理员手动检查。邮件成为 .HELD 邮件的原因如下：超过配置的最大信封收件人数量（请参见第 342 页中的 “12.5.9 多个地址扩展”中的 holdlimit 通道关键字）；基于相关邮件的某些可疑点运行了 《Sun Java System Messaging Server 6.3

Administration Reference》中的“imsimta qclean”、《Sun Java System Messaging Server 6.3 Administration Reference》中的“clean” 或 《Sun Java System Messaging Server 6.3 Administration Reference》中的“hold” 命令；使用了 Sieve 脚本的 `hold` 操作。

循环导致的 .HELD 邮件

邮件在服务器或通道之间的来回传送称为循环。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。循环邮件通常有大量的 `*Received:` 标题行。`Received:` 标题行将说明邮件循环的准确路径。 请仔细查看这些标题行中显示的主机名和所有收件人地址信息（例如，`for recipient` 子句或 `(ORCPT recipient)` 注释）。 导致这种邮件循环的原因之一是用户错误。

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` 的邮件应由主机 Y 处理。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。

另一个导致邮件循环的常见原因是，MTA 使用某个网络名接收发送给 MTA 主机的邮件，而 MTA 没有将该网络名识别（尚未配置为识别）为其自身名称中的一个。解决方案是将额外的名称添加到其中的名称被 MTA 识别为**自身**名称的列表中。请注意，MTA 用来确定邮件是否正在循环的阈值是可以配置的；请参见 `MAX_*RECEIVED_LINES` `option.dat` 选项（《Sun Java System Messaging Server 6.3 Administration Reference》中的“Option File Format and Available Options”）。同时请注意， MTA 可以配置为（请参见 `HELD_SNDOPR` 全局 MTA 选项）只要邮件由于超出此阈值而被强制设置为 `.HELD` 状态，就生成一则系统日志通知。如果收到 `Received count exceeded; message held.` 系统日志邮件，就说明发生了邮件循环。

您也可以通过运行《Sun Java System Messaging Server 6.3 Administration Reference》中的“release”或按照以下步骤来重新发送 `.HELD` 邮件。

1. 将 .HELD 扩展名将 .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*。

邮件可能会被再次标记为 .HELD，所以有必要多次执行这些步骤，因为 Received: 标题行会累积。如果仍存在问题，将像以前一样在同一通道下重新创建 *.HELD 文件。如果问题已经解决，则邮件将出队列并被传送。

如果您决定只是删除邮件而不尝试传送它们，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“clean”。

由于用户或域的 hold 状态导致的 .HELD 邮件

由于用户或域的 hold 状态导致的 .HELD 邮件（并且仅因这种原因导致的 .HELD 邮件）一般将存储在 hold 通道的队列区域中。即，hold 通道队列区域中的 .HELD 邮件文件可以认为是由于用户或域状态导致的 .HELD 邮件。

由于可疑特征导致的 .HELD 邮件

由于某些可疑特征导致的 .HELD 邮件必然会表现出相应特征。这些特征可以是站点已经选定为具有**可疑**特征的任何内容。MTA 管理员应该始终了解这些配置选项和操作。但是，如果您不是该 MTA 的唯一或原始管理员，请检查是否进行了以下方面的 MTA 配置：使用 holdlimit 通道关键字（第 342 页中的 “12.5.9 多个地址扩展”）、在基于地址的 *_ACCESS 映射表（在 MTA 映射文件中）中使用 $H 标志，或者在任何系统 Sieve 文件（系统级别的 imta.filter 文件，或者所有使用 sourcefilter 或 destinationfilter 通道关键字配置和指定的通道级别的 Sieve 过滤器；请参见第 369 页中的 “12.12.4 指定邮箱过滤器文件位置”）中使用 hold 操作；然后询问所有其他 MTA 管理员最近是否执行过任何手动命令行邮件 hold 操作（例如，通过 imsimta qm clean 命令）。同时请注意，无论是来自系统 Sieve 过滤器还是来自用户的个人 Sieve 过滤器，应用 Sieve 过滤器 hold 操作时都能可选地进行记录；有关更多信息，请参见 LOG_FILTER 全局 MTA 选项（《Sun Java System Messaging Server 6.3 Administration Reference》中的“Option File Format and Available Options”）。

26.3.9 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。有关详细信息，请参阅 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，八位字符通过 SMTP 进行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 客户端只有三种选项：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 客户端将邮件传输到其上）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。

26.3.10 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，因此过滤器通常被称作服务器端规则 (Server-side Rules, SSR)。

本节包括有关以下 SSR 主题的信息：

- 第 762 页中的 “26.3.10.1 测试 SSR 规则”
- 第 763 页中的 “26.3.10.2 常见语法问题”

另请参见第 509 页中的 “18.15 调试用户级别的过滤器”。

26.3.10.1 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` 通道以查看如何应用过滤器。结果显示在 `tcp_local_slave.log` 文件中。确保在目录 */msg-svr-base/*`config` 中的 `option.dat` 文件中添加 `mm_debug=5`，以获得足够的调试信息。

26.3.10.2 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：

  解析过滤器表达式时出现错误:...

  - 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，则将在输出的结尾显示以下错误消息：**地址列表错误 -- 4.7.1 过滤器语法错误：** `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
```

26.3.11 用户按下“发送电子邮件”按钮后响应缓慢

如果用户发送邮件时遇到延迟，这可能是由磁盘输入/输出降低（其原因是邮件队列磁盘大小不足）所致。用户按下其电子邮件客户端上的 "SEND" 按钮时，直到邮件被提交到邮件队列，MTA 才能完全接受邮件的回执。有关邮件队列大小调整的信息，可以在《》中找到。

26.3.12 地址的本地部分或接收字段中的星号

现在 MTA 在地址的本地部分及其构建的接收字段中查找 8 位字符（而不是仅 ASCII 字符）并用星号代替这些字符。

26.4 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 744 页中的 “26.2.1 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。有关每个子组件的详细信息，请参阅 Sun Java System Messaging Server Administration Reference 中关于 MTA 命令行实用程序和配置的章节以及本指南的第 5 章至第 10 章。本节包括以下类型的错误：

- 第 764 页中的 “26.4.1 mm_init 中的错误”

26.4.1 mm_init 中的错误

mm_init 中的错误通常表明 MTA 配置有问题。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：

26.4.1.1 别名的错误等值...

别名文件条目右侧部分的格式不正确。

26.4.1.2 无法打开别名包含文件...

无法打开别名文件所包含的文件。

26.4.1.3 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**出错行 #***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。

26.4.1.4 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 把配置文件的提示解释为通道定义。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。

26.4.1.5 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。

26.4.1.6 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。

26.4.1.7 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。有关详细信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimta chbuild”。

26.4.1.8 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 的详细信息，请参阅 《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimta chbuild”。

26.4.1.9 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。

26.4.1.10 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）。

26.4.1.11 通道没有正式主机名...

此错误表示通道定义块缺少所需的第二行（正式主机名行）。有关通道定义块的详细信息，请参见 Sun Java System Messaging Server Administration Reference 中关于 MTA 配置和命令行实用程序的章节以及第 12 章。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。

26.4.1.12 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，您可能会看到此情况。例如：

```
Original l Channel:
!delivery channel to local /var/mail store
l subdirs 20 viaaliasrequired maxjobs 7 pool LOCAL_POOL
walleroo.pocofronitas.thisnameismuchtoolongandreallymakesnosensebutitisan
example.monkey.gorilla.orangutan.antidisestablismentarianism.newt.salaman
der.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，请参阅 Sun Java System Messaging Server Administration Reference 中关于 MTA 配置的章节。

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。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。

26.4.2 编译的配置版本不匹配

`imsimta cnbuild` 实用程序的功能之一是将 MTA 配置信息编译为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。

26.4.3 交换空间错误

要确保操作正确，在邮件传送系统上配置足够的交换空间很重要。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]: 分叉失败：空间不足`

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剩余的交换空间大小以及您已使用的交换空间大小：

- 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`

26.4.4 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”错误或不可预测的行为。如果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 6.3 Administration Reference》中的“imsimta test”。

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 744 页中的 “26.2.3 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 744 页中的 “26.2.2 检查邮件队列目录” 。

26.4.5 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，请检查是否已正确配置 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 MX 支持。有关详细信息，请参见第 325 页中的 “12.4.3 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。

26.4.6 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_* errors` 错误通常是由于 DNS 或网络连接性问题所致，如果这是以前的工作通道或地址时，这种可能性更大。`os_smtp_read` 或 `os_smtp_write` 错误通常表示其他端异常中止了连接或由于网络问题而异常中止了连接。

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 27 章

27 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：

有关故障排除的过程，请参见第 26 章。

27.1 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。它可以监视所有消息存储、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。）请参见第 105 页中的 “4.5 失败的服务或未响应服务的自动重新启动” 和第 789 页中的 “27.8.9 使用 msprobe 和 watcher 功能进行监视” 。

27.2 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。

27.2.1 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件列表。属于此邮件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件列表的邮件，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件列表。

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）。

27.2.2 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）分别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 25 章。

27.2.3 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 789 页中的 “27.8.9 使用 msprobe 和 watcher 功能进行监视”

27.3 监视系统性能

虽然本章重点介绍的是 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 773 页中的 “27.3.1 监视端对端邮件传送时间”
- 第 773 页中的 “27.3.2 监视磁盘空间”
- 第 775 页中的 “27.3.3 监视 CPU 使用情况”

27.3.1 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。

27.3.1.1 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。

27.3.1.2 监视端对端邮件传送时间

- 使用发送和接收邮件的任一工具。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 782 页中的 “27.8.1 immonitor-access” 。

27.3.2 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 队列或写入到消息存储的空间，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。

消息存储分区将随着新邮件传送到邮箱而增长；例如，如果不强制消息存储配额，消息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。）

27.3.2.1 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消息存储，并且日志文件会溢出。

如果消息存储分区填满，则邮件访问守护进程可能会失败，消息存储数据可能会被破坏。消息存储维护实用程序（例如 `imexpire` 和 `reconstruct`）可以修复损坏并减少磁盘使用量。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。

27.3.2.2 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、消息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，以监视消息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消息存储的磁盘空间使用情况：

- 设置参数以监视消息存储磁盘空间的使用
- 达到磁盘使用量阈值时锁定消息存储分区

有关详细信息，请参见以下内容：第 774 页中的 “监视消息存储”和第 774 页中的 “监视消息存储分区”。

监视消息存储

建议消息存储的磁盘使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）来监视消息存储的磁盘使用量：

- `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
```

有关这些参数的更多信息，请参阅表 27–6。

监视消息存储分区

当邮件分区填充超过可用磁盘空间的指定百分比时，您可以停止向消息存储分区传送邮件。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。

消息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消息存储分区中的邮箱。
- 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` 参数如下所示：

- `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消息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消息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使用量。

有关管理日志记录空间的信息，请参见第 25 章。例如，要了解如何监视 `mail.log` 文件，请参见第 707 页中的 “25.3 管理 MTA 邮件和连接日志”。

27.3.3 监视 CPU 使用情况

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 周期数超出了正常范围。

27.3.3.1 CPU 使用情况问题的症状

系统响应时间长。用户的登录缓慢。传送率低。

27.3.3.2 监视 CPU 使用情况

监视 CPU 使用情况是一个特定于平台的任务。请参见相关的平台文档。

27.4 监视 MTA

本节包含以下几个部分：

27.4.1 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、传送被延迟或者传入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 172 页中的 “8.5.2 通道邮件队列”、第 755 页中的 “26.3.6 邮件未被排出队列”和第 757 页中的 “26.3.7 未传送 MTA 邮件”。

27.4.1.1 邮件队列问题的症状

- 磁盘空间使用量增长。
- 用户没有在合理的时间内收到邮件。
- 邮件队列大小异常大。

27.4.1.2 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` 和 `imsimta summarize`。请参见第 788 页中的 “27.8.6 imsimta qm counters”。

您也可以监视队列目录 (*msg-svr-base*`/data/queue/`) 中文件的数量。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。

27.4.2 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出现网络问题（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。

27.4.2.1 传送失败率的症状

没有外部症状。`mail.log_current` 中会出现很多 `Q` 记录。

27.4.2.2 监视传送失败率

传送失败将记录在 MTA 日志中，日志记录条目代码为 Q。可以在文件 *msg-svr-base*/data/log/mail.log_current 中查看该记录。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
```

27.4.3 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。

27.4.3.1 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。

27.4.3.2 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，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 连接的适当数量及其状态（ESTABLISHED、CLOSE_WAIT 等），以便确定某次特定的读取是否超出了正常范围。

如果发现很多连接处于 SYN_RECEIVED 状态，则可能是由网络断开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。它是由 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）。与此类似，MAX_LIFE_CONNS 可以指定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。

27.4.4 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。

27.4.4.1 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。

27.4.4.2 监视分发程序和作业控制器进程

检查是否存在名为 `dispatcher` 和 `job_controller` 的进程。请参见第 745 页中的 “26.2.4 检查作业控制器和分发程序是否正在运行” 。

27.5 监视 LDAP Directory Server

本节包含以下几个部分：

- 第 778 页中的 “27.5.1 监视 slapd”

27.5.1 监视 slapd

LDAP Directory Server (`slapd`) 为邮件服务系统提供目录信息。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需要使用 LDAP 进行查找的任何其他事务。

27.5.1.1 slapd 问题的症状

- 客户端 POP、IMAP 或 Webmail 验证失败或者比预期的速度慢。
- MTA 无法正常工作

27.5.1.2 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。
- 另请参见第 782 页中的 “27.8.1 immonitor-access” 。

27.6 监视邮件访问

本节包含以下几个部分：

27.6.1 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。

27.6.1.1 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 未在运行而您尝试直接连接至 IMAP，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
```

如果尝试与客户端连接，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.
```

27.6.1.2 监视 imapd、popd 和 httpd

- 可以使用 `watcher` 和 `msprobe` 进行监视。请参见第 105 页中的 “4.5 失败的服务或未响应服务的自动重新启动”和第 789 页中的 “27.8.9 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。服务器信息位于网络服务监视 MIB 中。
- 检查日志文件。

  查看 *msg-svr-base*/log/*service* 目录，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级联至该服务名称的日期。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 25 章。）

  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 782 页中的 “27.8.3 counterutil”和《Sun Java System Messaging Server 6.3 Administration Reference》中的“counterutil”。
- 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，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 791 页中的 “27.8.9.1 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 782 页中的 “27.8.1 immonitor-access”。

27.7 监视消息存储

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：

27.7.1 监视 stored

`stored` 可执行多种重要的任务，例如邮件数据库的死锁和处理操作、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 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` 的更多信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“stored”。

27.7.1.1 stored 问题的症状

没有外部症状。

27.7.1.2 监视 stored

- 检查 `stored` 进程是否在运行。`stored` 进程会在 *msg-svr-base*`/data/proc` 中创建一个 `pid` 文件并对其更新，该文件的名称为 `store`。该 `pid` 文件在恢复时显示 `init` 状态，在就绪时显示 `ready` 状态。例如：

```
231: cat 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。imapd 中断或数据库问题也会生成日志文件。
- 检查 *msg-svr-base*/config 中以下文件上的时间戳：

  stored.ckp—尝试进行检查点操作时改写该文件。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改写该文件。应当每 5 分钟标记一次时间戳。
  stored.per—每次按用户写出数据库时改写该文件。应当每 60 分钟标记一次时间戳
- 检查默认日志文件 *msg-svr-base*/log/default/default 中的 stored 邮件。
- 可以使用 watcher 和 msprobe 进行监视。请参见第 105 页中的 “4.5 失败的服务或未响应服务的自动重新启动”和第 789 页中的 “27.8.9 使用 msprobe 和 watcher 功能进行监视”。

27.7.2 监视消息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消息存储的性能。在死锁情况下，邮件将无法以正常的速度插入到存储中，最终将导致 ims-ms 通道队列增大。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。

27.7.2.1 消息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。

27.7.2.2 监视消息存储数据库锁定

使用命令 imcheck -s（**以前是** counterutil -o db_lock）

27.8 用于监视的实用程序和工具

以下工具可用于进行监视：

- 第 789 页中的 “27.8.8 用于邮箱配额检查的 imquotacheck”
- 第 789 页中的 “27.8.9 使用 msprobe 和 watcher 功能进行监视”

27.8.1 immonitor-access

`immonitor-access` 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 6.3 Administration Reference》中的“immonitor-access”。

27.8.2 imcheck

使用 `imcheck –s` 监视数据库统计信息，包括日志和事务。

27.8.3 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 = 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，我们将仅讨论 `alarm`、`diskusage`、`serverresponse`、`popstat`、`imapstat` 和 `httpstat` 计数器对象。有关 `counterutil` 命令的用法的详细信息，请参阅《Sun Java System Messaging Server 6.3 Administration Reference》中的“counterutil”。

27.8.3.1 counterutil 输出

counterutil 有多种标志。此实用程序的命令格式可能为：

```
counterutil -o CounterObject -i 5 -n 10
```

其中，

-o *CounterObject* 表示计数对象 alarm、diskusage、serverresponse、popstat、imapstat 和 httpstat。

-i 5 指定时间间隔为 5 秒。

-n 10 表示重复次数（默认值：无穷大）。

以下是 counterutil 的用法示例：

```
# 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
...
```

27.8.3.2 使用 counterutil 的警报统计信息

以下警报统计信息指的是由 stored 发送的警报。警报计数器可以提供以下统计信息：

表 27–1 counterutil alarm 统计信息

后缀	说明
alarm.countoverthreshold	超出阈值的次数。
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。

表 27–1 counterutil alarm 统计信息 （续）

后缀	说明
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]）。

27.8.3.3 使用 counterutil 的 IMAP、POP 和 HTTP 连接统计信息

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，可使用命令 `counterutil -o` *CounterObject* `-i 5 -n 10`。其中 *CounterObject* 代表计数器对象 `popstat`、`imapstat` 或 `httpstat`。`imapstat` 后缀的含义如表 27–2 中所示。`popstat` 和 `httpstat` 对象可以通过同样的格式和结构提供同样的信息。

表 27–2 counterutil imapstat 统计信息

后缀	说明
currentStartTime	当前 IMAP 服务器进程的开始时间。
lastConnectionTime	上次接受新客户端的时间。
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。

27.8.3.4 使用 counterutil 的磁盘使用情况统计信息

命令`counterutil -o diskusage` 可以生成以下信息：

表 27–3 counterutil diskstat 统计信息

后缀	说明
diskusage.availSpace	磁盘分区中的总的可用空间。

表 27–3 counterutil diskstat 统计信息 （续）

后缀	说明
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。

27.8.3.5 服务器响应统计信息

命令 counterutil -o serverresponse 可以生成以下信息。这些信息可用于检查服务器是否正在运行以及它们的响应速度。

表 27–4 counterutil serverresponse 统计信息

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。

27.8.4 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 25 章。

27.8.5 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。要获得精确的计数，请查看 MTA 日志记录，如第 25 章中所述。

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` 命令可以提供 MTA 通道邮件统计信息（请参见下文）。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，与该通道相关联的计数器便会减少，从而导致出现负的最小值。如果计数器出现这种情况，用当前值减去自计数器初始化以来曾经具有的最小值便可得到正确的“绝对”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（已取消排队）的邮件数。（即 `mail.log*` 文件中的 D 记录。）取消排队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取消排队操作。通常此值等于 `Received` 值与 `Stored` 值之差。

MTA 还跟踪了首次尝试时被取消排队的邮件数，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` 是在排出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 是失败的取消排队尝试次数（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。这包括首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 是首次尝试即传送成功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，因为通道取消排队（传送）的每封邮件都将导致至少一封新邮件加入队列（提交），但可能会多于一封。例如，如果一封邮件具有两个分别经由不同通道到达的收件人，则将需要进行两次加入队列操作。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，邮件将由其他任意通道加入队列，然后，转换通道将处理该邮件并将其加入到第三个通道中的队列，并在该邮件的自身队列中将其标记为已取消排队。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 tcp_local 这样的通道（不是“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 客户端部分。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* 客户端发送给其他 *SMTP* 主机的邮件：

```
elsewhere -> tcp_local E record Received
tcp_local              D record Delivered
```

通道的取消排队（传送）操作将导致至少一封新邮件加入队列（提交），但可能会多于一封。例如，如果一封邮件具有两个分别经由不同通道到达的收件人，则将需要进行两次加入队列操作。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。

27.8.5.1 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加入队列或取消排队时，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。

27.8.6 imsimta qm counters

`imsimta qm counters` 实用程序可显示 MTA 通道队列邮件计数器。只有 root 或 `mailsrv` 用户才能运行该实用程序。程序的输出字段与第 785 页中的 “27.8.5 imsimta 计数器”中所述的字段相同。另请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimta counters”。

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`**

27.8.7 使用 SNMP 的 MTA 监视

Messaging Server 支持通过简单网络管理协议 (Simple Network Management Protocol, SNMP) 进行系统监视。使用 SNMP 客户端（有时称为**网络管理器**），例如 Sun Net Manager 或 HP OpenView（没有随此产品一起提供），可以监视 Messaging Server 的特定部分。有关详细信息，请参见附录 A。

27.8.8 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             ajonk
no quota              5             no quota      2                andrt
no quota         355518             no quota      2500             ansri
 ...
```

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
```

27.8.9 使用 msprobe 和 watcher 功能进行监视

Messaging Server 提供了 watcher 和 msprobe 两个进程来监视各种系统服务。watcher 监视服务器崩溃并根据需要重新启动服务器。msprobe 监视服务器挂起（不响应）。具体来讲，msprobe 可以监视以下内容：

- **服务器响应时间**。msprobe 可以使用已启用服务器的协议命令连接至这些服务器并测定其响应时间。如果服务器响应时间超出报警阈值，系统将向服务器发送报警邮件（请参见第 791 页中的 “27.8.9.1 警报邮件”）；如果该响应时间超出指定的超时时长，将重新启动服务器。服务器响应时间同时记录到计数器数据库和默认日志文件中。可以使用 counterutil 来显示服务器响应时间的统计信息（第 782 页中的 “27.8.3 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，系统将重新启动分发程序。ens 无法自动重新启动。

- **磁盘使用量**。msprobe 检查每个消息存储分区的磁盘可用性和使用量。具体来讲，它可以检查消息存储 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 782 页中的 “27.8.3 counterutil”）显示磁盘使用量的统计信息。
- **消息存储 mboxlist 数据库日志文件积累**。日志文件积累是 mboxlist 数据库错误的迹象。msprobe 计算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，以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 由 configutil 选项（如表 27–5 所示）控制。有关详细信息，请参见第 105 页中的 “4.5 失败的服务或未响应服务的自动重新启动”。

表 27–5 msprobe 和 watcher configutil 选项

选项	说明
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) 更长的时间段值。默认值：600 秒
local.probe.service.timeout	特定服务器在重新启动之前的超时。*service* 可以是 imap、pop、http、cert、job_controller、smtp、lmtp、mmp 或 ens。 默认值：使用 service.readtimeout
local.probe.service.warningthreshold	警告消息被记录到 default 日志文件之前的特定服务器无响应秒数。*service* 可以是 imap、pop、http、cert、job_controller、smtp、lmtp、mmp 或 ens。 默认值：使用 local.probe.warningthreshold
local.probe.warningthreshold	警告消息被记录到 default 日志文件之前的服务器无响应秒数。 默认值：5 秒
local.queuedir	用于检查队列大小是否超过由 alarm.diskavail.msgalarmthreshold 定义的阈值的 MTA 队列目录。 默认值：无
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
local.schedule.msprobe	msprobe 运行计划。crontab 样式的时间安排字符串（请参见表 20–10。请注意，该字符串在默认情况下是自动设置的。请参见第 108 页中的 “4.6.2 预定义的自动任务”。） 要进行禁用：请将 local.schedule.msprobe.enable 设置为 NO。

表 27–5 msprobe 和 watcher configutil 选项 （续）

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、消息存储 (stored)、imsched 和 MMP。（LMTP/SMTP 服务器由分发程序监视，LMTP/SMTP 客户端由 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：on

27.8.9.1 警报邮件

msprobe 可以通过电子邮件向邮寄主管发出报警（请参见第 779 页中的 “27.6.1.2 监视 imapd、popd 和 httpd”），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。可以通过使用 configutil 命令设置报警参数完成此操作。表 27–6 显示了有用的报警参数及其默认设置。请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“configutil Parameters”。

表 27–6 有用的报警邮件 configutil 参数

参数	说明（括号中为默认设置）
larm.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。

表 27–6 有用的报警邮件 configutil 参数 （续）

参数	说明（括号中为默认设置）
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。
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 (Simple Network Management Protocol, SNMP) 进行系统监视。使用 SNMP 客户端（有时称为**网络管理器**），例如 Sun Net Manager 或 HP OpenView（未与此产品一起提供），您可以监视 Messaging Server 的特定部分。有关监视 Messaging Server 的更多信息，请参阅第 27 章。

本章介绍如何为 Messaging Server 启用 SNMP 支持。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 客户端查看此信息。有关如何使用 SNMP 客户端查看基于 SNMP 的信息的详细信息，请参见 SNMP 客户端文档。本文档还介绍了 Messaging Server SNMP 实现的某些可用数据，但完整的 MIB 详细资料可以从 RFC 2788 (`http://www.faqs.org/rfcs/rfc2788.html`) 和 RFC 2789 (`http://www.faqs.org/rfcs/rfc2788.html`) 获得。

本章包含以下几个部分：

A.1 SNMP 实现

Messaging Server 实现两个标准 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、入站连接的总数）。

注 – 有关 Messaging Server SNMP 监视信息的完整列表，请参阅 RFC 2788 和 RFC 2789。

运行 Solaris 和 Red Hat Linux 的平台支持 SNMP。 Solaris 9 操作系统中的 Messaging Server 使用 Solstice Enterprise Agent (SEA)。从 Solaris 10 操作系统开始，Messaging Server 支持开放源代码 Net-SNMP 监视框架，使得 Solaris 9 操作系统 Solstice Enterprise Agent (SEA) 技术成为历史（不再受支持）。此外，Net-SNMP 广泛用于 Linux 平台。Messaging Server 将在 Solaris 10 中使用其基于 Net-SNMP 的 SNMP 子代理，以后也会在 Linux 平台上使用。

通过采用 Net-SNMP 框架，Messaging Server 的 SNMP 子代理提供了新的功能：

- 支持 SNMP 版本 2c 和版本 3。这是通过 Net-SNMP 框架实现的。以前的 SNMP 技术 Solstice Enterprise Agent 只提供对 SNMP 版本 1 的支持。 增强的安全功能和访问控制是 SNMP 这两个版本的主要优点。
- 可以配置子代理作为“独立”SNMP 代理运行。这为站点提供了一些附加方法，可将运行在同一系统上的各种 SNMP 代理进行隔离。
- 在同一系统上运行的多个 Messaging Server“实例”可以同时被监视。该支持可通过以上第 2 项提供，也可以通过 SNMP 版本 3“上下文名称”来实现。这允许在故障转移群集中对 Messaging Server 进行 SNMP 监视。

对 Messaging Server SNMP 支持的限制如下：

- 在 Solaris 9 操作系统中，只能通过 SNMP 监视每台主机的一个 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。）

A.1.1 Messaging Server 中的 SNMP 操作

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。来自客户端的 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转发回客户端。图 A–1 显示了此过程。

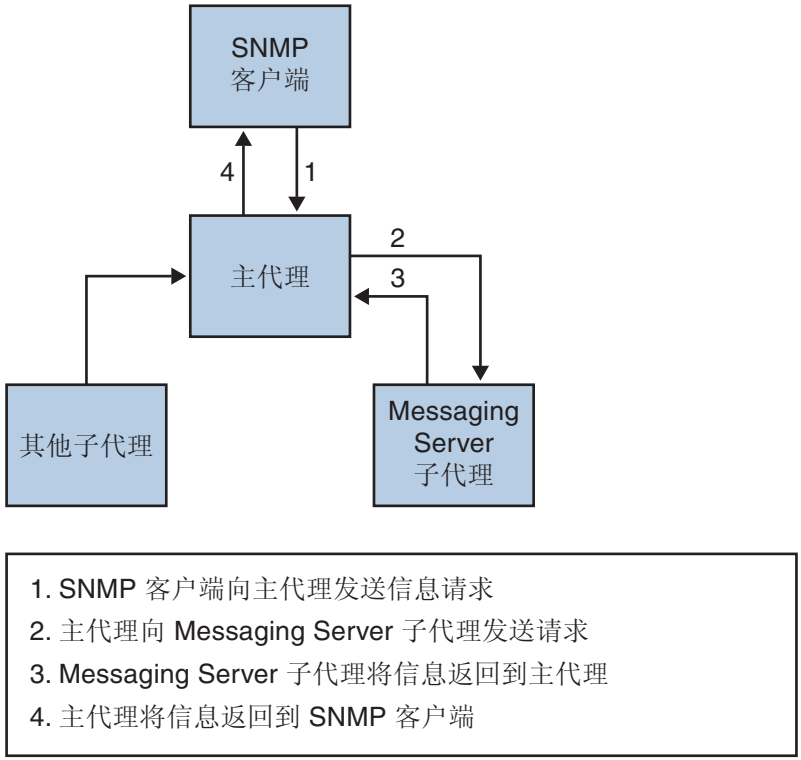


图 A–1 SNMP 信息流

A.2 在 Solaris 9 中为 Messaging Server 配置 SNMP 支持

尽管 SNMP 监视的开销非常小，但 Messaging Server 在出厂时仍被禁用了 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（未指定任何参数）将自动启动 SNMP 子代理进程和其他 Messaging Server 进程。

请注意，为使 Messaging Server SNMP 子代理能够操作，必须运行 Solaris 本机 SNMP 主代理。Solaris 本机 SNMP 主代理是 `snmpdx` 守护进程，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。零值（默认设置）将告知 Messaging Server 允许子代理自动选择任何可用的 UDP 端口。

两个 SNMP 子代理配置文件均放置在 `/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 实现的 MIB 是只读的，并且无需在 `ims.reg` 文件中指定端口号。如果指定了端口号，则将使用该端口号，除非您还使用 `configutil` 实用程序设置了另一个端口号。在这种情况下，使用 `configutil` 设置的端口号就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
```

注 – 在 Messaging Server 中启用 SNMP 支持时，通过 SNMP 在 Solaris 10 操作系统上进行的所有查询都必须连接到默认端口 16161。例如，如果使用开放源代码 SNMP 工具 *snmpwalk* 来查询 Messaging Server 的网络/邮件统计信息，应使用选项 `-p 16161`。

A.3 为 Solaris 10 操作系统配置 SNMP 支持

默认情况下，SNMP 监视在 Messaging Server 中是禁用的。试图最小化默认 Messaging Server 配置表示的服务数时选择默认设置。不要将此默认设置理解为使用 SNMP 监视会引起性能损耗。实际上，Messaging Server 的 SNMP 支持消耗非常少的资源，对 Messaging Server 的影响很小。当然，必须要注意的一点是，使用 Messaging Server 的 SNMP 支持之前需要一次性配置步骤。此外，平台 Net-SNMP 主代理的默认配置（`snmpd`）通常需要更改，以便运行子代理，如 Messaging Server。 该更改是下一节讨论的主题。

A.3.1 Net-SNMP 配置

Messaging Server 基于 Net-SNMP 的 SNMP 子代理使用 AgentX 协议与平台 SNMP 主代理进行通信 (RFC 2741)。Net-SNMP 主代理 `snmpd` 必须配置为允许使用 AgentX 协议。要完成此操作，请确保平台的 `snmpd.conf` 文件包含下行

```
master agentx
```

如果该行不存在，则添加该行并重新启动 `snmpd` 守护程序。请注意，将 SIGHUP 信号发送给守护程序是不够的。重新启动了 `snmpd` 守护程序之后，请查找 UNIX 域套接字，该套接字是 `snmpd` 为 AgentX 通信创建的。在 Solaris 和 Linux 系统中，该套接字默认情况下显示为特殊文件 `/var/agentx/master`；但是，其位置和名称可能会通过 `snmpd.con` 文件进行更改。

Solaris 10 操作系统 snmpd 配置如下所示：

```
%cp /etc/sma/snmp/snmpd.conf /etc/sma/snmp/snmpd.conf.save
% cat >> /etc/sma/snmp/snmpd.conf
# Messaging Server's subagent requires the AgentX protocol
master agentx
^D
% cat >> /etc/sma/snmp/snmpd.conf
% ls -al /var/agentx/
srwxrwxrwx 1 root root 0 Aug 9 13:58 /var/agentx/master
```

此外，在 Red Hat Enterprise Linux AS 3 系统中，默认 snmpd.conf 文件限制“公用”SNMP 社区可能会查看的信息。因此有必要删除该限制，或者将其扩展为包含 Messaging Server 子代理实现的 MIB。考虑到初始测试，建议采用后者。实现这一点的方式是，包含名为 "systemview" 的视图中的 OID 子树 mib-2.27 和 mib-2.28（如下所示）。对于实际部署，每个站点必须考虑其总体安全策略。请注意，SNMP 子代理提供的信息是“只读”的。

```
% cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.save
% cat >>/etc/snmp/snmpd.conf
# Messaging Server's subagent requires the AgentX protocol
master agentx
# Messaging Server's subagent exports mib-2.27 and .28
# Add the mib-2.27 and .28 OID subtrees to the systemview
view systemview included .1.3.6.1.2.1.27
view systemview included .1.3.6.1.2.1.28
^D
% /sbin/service snmpd restart
% ls -al /var/agentx/master
srwxr-xr-x 1 root root 0 Aug 8 21:20 /var/agentx/master
```

如果您将使用 SNMP v3 上下文名称来区分同时运行在同一主机上的不同 Messaging Server 实例的 MIB，则至少还需要配置一个 SNMP v3 以及用于 SNMP v3 查询的用户名和密码。

A.3.2 Messaging Server 子代理配置

至于 Messaging Server 的 SNMP 子代理的基本操作，您只需启用它并发出一个一次性手动启动命令。之后，无论何时启动或停止 Messaging Server，子代理将同样被启动或停止。在 Solaris 和 Linux 上实现此配置所需的命令如下：

```
% configutil -o local.snmp.enable -v 1
% start-msg snmp
```

运行后，可以使用 snmpwalk 命令通过命令行测试子代理。请参见示例下面适用于 Solaris 和 Linux 的屏幕截图。请注意，文件 rfc2248.txt 和 rfc2249.txt 是网络服务和

MTA MIB 的副本。在 Solaris 系统中，可以在 NETWORK-SERVICES-MIB.txt 和 MTA-MIB.txt 下的 /etc/sma/snmp/mibs/ 目录中找到这些文件。没有必要将这些文件提供给 snmpwalk 工具，但是，这样做允许 snmpwalk 输出每个 MIB 变量的名称，而不是它们的数字对象标识符 (OID)。

在 Solaris 上的基本测试：

```
% D=/opt/SUNWmsgsr/examples/mibs /usr/sfw/bin/snmpwalk -v 1 -c public \
    -m +$D/rfc2248.txt:$D/rfc2249.txt 127.0.0.1 mib-2.27
NETWORK-SERVICES-MIB::applName.1 = STRING: /opt/SUNWmsgsr MTA on mail.siroe.com
...
% D=/opt/SUNWmsgsr/examples/mibs /usr/sfw/bin/snmpwalk -v 1 -c public \
     -m +$D/rfc2248.txt:$D/rfc2249.txt 127.0.0.1 mib-2.28
MTA-MIB::mtaReceivedMessages.1 = Counter32: 1452
MTA-MIB::mtaStoredMessages.1 = Gauge32: 21
...
```

在 Linux 上的基本测试：

```
% export D=/opt/sun/messaging/examples/mibs
% /usr/bin/snmpwalk -v 1 -c public \
     -m +$D/rfc2248.txt:$D/rfc2249.txt 127.0.0.1 mib-2.27
NETWORK-SERVICES-MIB::applName.1 = STRING: /opt/sun/messaging MTA on mail.siroe.com
...
% /usr/bin/snmpwalk -v 1 -c public \
     -m +$D/rfc2248.txt:$D/rfc2249.txt 127.0.0.1 mib-2.28
MTA-MIB::mtaReceivedMessages.1 = Counter32: 21278
MTA-MIB::mtaStoredMessages.1 = Gauge32: 7
...
```

A.3.3 作为独立的 SNMP 代理运行

在将 Messaging Server SNMP 子代理配置为独立的 SNMP 代理运行之前，您必须首先决定该代理侦听 SNMP 请求的以太网接口和 UDP 端口。在默认情况下，该代理将使用 UDP 端口 161 来侦听所有可用的以太网接口。在大多数情况下，您需要更改此端口号，以便不影响平台的 SNMP 主代理 snmpd。在某些情况下，例如 HA 故障转移，您还需要将所有可用接口中的以太网接口 (INADDR_ANY) 更改为由其 IP 地址标识的特定接口。以太网接口和 UDP 端口这两个概念由 local.snmp.listenaddr 和 local.snmp.port 选项控制。

对以太网接口和 UDP 端口作出选择之后，应该将 local.snmp.standalone 选项的值设置为 1 并重新启动子代理。重新启动后，它将作为一个与 snmpd 和任何子代理无关的 SNMP 代理运行。

例如，要作为独立代理（侦听 IP 地址为 10.53.1.37 的以太网接口的 UDP 端口 9161）运行，请发出如下所示的命令。

配置为作为独立代理运行：

```
% configutil -o local.snmp.port -v 9161
% configutil -o local.snmp.listenaddr -v 10.53.1.37
% configutil -o local.snmp.standalone -v 1
% stop-msg snmp
% start-msg snmp
% snmpwalk -v 1 -c public 10.53.1.37:9161 .
SNMPv2-SMI::mib-2.27.1.1.2.1 = STRING: "/opt/SUNWmsgsr MTA on mail.siroe.com"
...
```

A.3.4 监视 Messaging Server 的多个实例

这里讨论了两种用于监视同一主机上运行的多个 Messaging Server 实例的技术。第一种技术，以独立模式运行子代理，这非常适于高可用性的故障转移 (HA) 配置，其中 Messaging Server 的单个实例可能会在主机之间动态地移动。第二种技术，使用 SNMP v3 上下文名称，其优点体现在 Messaging Server 的多个实例被限制在单个系统上的情况下，该技术需要限制由 SNMP 监视软件轮询的 IP 地址数（例如，当监视软件的许可具有基于 IP 地址的成本组件时）。后一种技术也可用于 HA 故障转移设置，但是需要轮询和独立模式技术一样多的 IP 地址。

A.3.5 将独立的代理用于高可用性故障转移

在需要 Messaging Server 的 SNMP 监视的高可用性故障转移中，建议将 Messaging Server 的 SNMP 子代理作为第 798 页中的 “A.3.3 作为独立的 SNMP 代理运行”中所描述的独立子代理运行。子代理运行在独立模式下时，Messaging Server 的每个 HA 实例都应该将其 `local.snmp.listenaddr` 选项设置为该实例的故障转移 IP 地址的值。要简化管理，每个实例应该使用相同的 UDP 端口，但该端口要与 `snmpd` 守护程序（运行在每个物理群集主机上）所使用的端口区别开。通常，这些守护程序将使用 UDP 端口 161，因此要使用 `local.snmp.port` 选项明确指定不同的端口号。

按给出的建议配置好 Messaging Server 的 SNMP 支持后，监视站可以通过其故障转移 IP 地址或主机名来监视每个 Messaging Server 实例，而不管实例运行在哪个物理群集主机上。而且，您可以确保 Messaging Server 的独立 SNMP 代理不会相互冲突，因为每个代理只侦听它自己的虚拟以太网接口，该接口由实例的唯一故障转移 IP 地址标识。（这些虚拟以太网接口由 HA 故障转移框架自动创建。）由于对 UDP 端口进行了仔细选择，因此代理不会与在群集中的系统上运行的 `snmpd` 守护程序冲突。

A.3.6 通过 SNMP v3 上下文名称区分多个实例

虽然使用第 798 页中的 “A.3.3 作为独立的 SNMP 代理运行”中所描述的以独立模式使用 Messaging Server 的 SNMP 支持没有什么不利，但一些站点还是希望使用更传统的子代理模式，同时仍具有监视同时运行在同一系统上的多个 Messaging Server 实例的功

能。例如，许可模型限制轮询 IP 地址数的 SNMP 监视系统。要实现此目标，请继续运行 Messaging Server 的 SNMP 子代理，并将 `local.snmp.standalone` 设置为 0。此外，为 `local.snmp.enablecontextname` 选项指定一个非零值，从而将每个 Messaging Server 实例配置为使用不同的 SNMP v3 上下文名称。如果需要的上下文名称不同于 `service.defaultdomain` 的值，则使用 `local.snmp.contextname` 选项设置所需的名称。重新启动每个 Messaging Server 的 SNMP 子代理实例之后，就可以通过包含正确上下文名称的 SNMP v3 查询来监视这些实例。运行在同一系统上的两个 Messaging Server 实例的 MIB 通过实例的 SNMP v3 上下文名称来区分，因此不会出现 MIB 对象标识符 (OID) 冲突。

A.3.7 Messaging Server 的基于 Net-SNMP 的 SNMP 子代理选项

以下选项只适用于 Messaging Server 的基于 Net-SNMP 的 SNMP 子代理。该子代理在运行 Solaris 10 以及更高版本的 Solaris 平台上使用，也可以在 Linux 平台上使用。以下介绍的选项不适用于为运行 Solaris 9 及更低操作系统的 Solaris 平台而提供的传统 SNMP 子代理。

以下介绍的选项是 `configutil` 选项。因此，可通过以下形式的命令来查看这些选项的值：

```
% configutil -o option-name
```

其中 *option-name* 是要显示选项值的选项的名称。要设置或更改选项的值，请使用以下形式的命令

```
% configutil -o option-name -v option-value
```

其中 *option-value* 是要设置的值。需要重新启动才能使这些选项的更改生效：

```
% stop-msg snmp
% start-msg snmp
```

接下来给出每个选项的说明及其默认值。

表 A–1 SNMP 子代理选项

选项（默认值）	说明

表 A–1 SNMP 子代理选项 （续）

local.snmp.启用 (0)	Messaging Server SNMP 子代理只在该选项值为 1 或 `true` 时才运行，在这种情况下，Messaging Server 将自动停止或启动子代理，并将其作为正常启动和关闭过程的一部分。默认情况下，该选项设置为 0，这样会禁用子代理的操作。在启用子代理之前，请确保平台的主代理已按照第 798 页中的 “A.3.3 作为独立的 SNMP 代理运行”中所描述的方法正确配置。
local.snmp.standalone (0)	Messaging Server 的 SNMP 支持通常作为 SNMP 子代理运行，并通过平台的 SNMP 主代理 `snmpd` 接收 SNMP 请求。该操作模式是默认设置，通过将该选项的值指定为 0 或 `false` 来选择此默认设置。但是，如第 798 页中的 “A.3.3 作为独立的 SNMP 代理运行”中所述，子代理可能会以 “独立” 模式运行，从而以独立于 `snmpd` 的 SNMP 代理运行。当以独立模式运行时，子代理（现在是 SNMP 代理）直接侦听以太网接口和 UDP 端口上的 SNMP 请求，以太网接口和 UDP 端口分别由 `local.snmp.listenaddr` 和 `local.snmp.port` 选项指定。要在此独立模式下运行，请将该选项的值指定为 1 或 `TRUE`。 以独立模式运行并不影响运行在同一系统上的其他 SNMP 主代理或子代理。
local.snmp.listenaddr (INADDR_ANY)	以独立模式运行时侦听 SNMP 请求的主机名或以太网接口的 IP 地址。默认情况下，侦听所有可用的接口。这对应于指定值 `INADDR_ANY`。可以通过指定与接口关联的 IP 地址或主机名来选择特定接口。此接口可以是物理接口，也可以是虚拟接口。 `local.snmp.standalone` 设置为 0 或 `FALSE` 时忽略该选项。
local.snmp.cachettl (30)	缓存监视数据的生存时间 (TTL)（以秒为单位）。该选项控制在使用从 Messaging Server 获得的新信息刷新监视数据之前，子代理报告相同监视数据的时间。除邮件循环信息外，默认情况下，缓存数据的时间不超过 30 秒。循环信息（通过扫描 `.HELD` 文件确定）每 10 分钟才更新一次。这是因为扫描所有盘上邮件队列会消耗资源。 请注意，子代理并不持续更新其监视数据：只有在收到 SNMP 请求，并且高速缓存的数据过期时（即，超过其生存时间）才进行更新。如果将生存时间 (TTL) 设置为 30 秒，并且每 5 分钟发出一次 SNMP 请求，则每个 SNMP 请求将导致子代理从 Messaging Server 中获得刷新的数据。即，每 5 分钟就可从 Messaging Server 中获得一次数据。另一方面，如果每 10 秒发出一次 SNMP 请求，则子代理将使用已缓存了 29 秒的数据来响应其中一些请求；Messaging Server 则每 30 秒被轮询一次。

表 A–1 SNMP 子代理选项 （续）

local.snmp.servertimeout (5)	子代理通过实际打开到每个服务的 TCP 连接，以及进行协议转换来确定每个所监视服务的操作状态。该超时值（以秒为单位）控制子代理等待响应协议转换中每个步骤的时间。默认情况下，使用的超时值为 5 秒。
local.snmp.directoryscan (1)	使用该选项控制子代理是否为 `.HELD` 邮件文件和最早的邮件文件执行盘上邮件队列扫描。该信息对应于 `mtaGroupLoopsDetected`、`mtaGroupOldestMessageStored` 和 `mtaGroupOldestMessageId` MIB 变量。当该选项的值为 1 或 `true` 时，将根据需要维护和更新此信息的缓存。具有大量排队邮件并且不需要这些特定 MIB 变量的站点应该考虑将该选项的值设置为 0 或 `false`。
local.snmp.enablecontextname (0)	子代理可以在 SNMP v3 **上下文名称** 下注册其 MIB。完成此操作后，可以仅通过 SNMP v3 客户端请求 MIB，该客户端在其 SNMP 请求中指定上下文名称。使用上下文名称允许多个独立的子代理在同一 OID 树下（即，同一 SNMP 主代理下）注册网络服务和 MTA MIB。有关详细信息，请参见第 799 页中的 “A.3.4 监视 Messaging Server 的多个实例”。 要启用 SNMP v3 上下文名称，请将该选项的值指定为 1 或 `true`。当完成此操作后，子代理将默认使用其上下文名称的 `service.defaultdomain` 选项的值。要对上下文名称使用别的值，请使用 `local.snmp.contextname` 选项。
local.snmp.contextname (service.defaultdomain)	使用 `local.snmp.enablecontextname` 启用 SNMP v3 上下文名称时，该选项可用来明确设置子代理用于其 MIB 的上下文名称。为该选项提供的值是字符串值，必须适合用作 SNMP v3 上下文名称。当 `local.snmp.enablecontextname` 的值为 0 或 `false` 时忽略该选项。

A.4 通过 SNMP 客户端监视

RFC 2788 (`http://www.faqs.org/rfcs/rfc2788.html`) 和 RFC 2789 (`http://www.faqs.org/rfcs/rfc2788.html`) 的基本 OID 为：

mib-2.27 = 1.3.6.1.2.1.27

mib-2.28 = 1.3.6.1.2.1.28

将您的 SNMP 客户端指向上述两个 OID，并将其作为“公用”社区访问。

如果要将 MIB 副本装入 SNMP 客户端，您可以在 *msg-svr-base*`/lib/config-templates` 目录的 `rfc2788.mib` 和 `rfc2789.mib` 文件名下找到 MIB 的 ASCII 副本。有关在 SNMP 客户端软件中装入 MIB 的指导信息，请参见 SNMP 客户端软件文档。某些较旧的 SNMP 客户端可能无法识别这些 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`。

A.5 来自 Messaging Server 的 SNMP 信息

本节概述了通过 SNMP 提供的 Messaging Server 信息。其中包含以下各小节：

有关更多信息，请参阅 RFC 2788 (`http://www.faqs.org/rfcs/rfc2788.html`) 和 RFC 2789 (`http://www.faqs.org/rfcs/rfc2788.html`) 中的单个 MIB 表。请注意，RFC/MIB 术语中将邮件传送服务（MTA、HTTP 等）称为**应用程序** (`appl`)，将 Messaging Server 网络连接称为**关联** (`assoc`)，将 MTA 通道称为 *MTA* **组** (`mtaGroups`)。

请注意，在可同时监视多个 Messaging Server 实例的平台上，`applTable` 中可能会包含多组 MTA 和服务器，其他表中可能会包含多个 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 客户端允许进行趋势分析，并在突然出现背离历史趋势的情况时发送警告。

A.5.1 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) 中的数据的示例。

```
          applTable:

applName.1  = mailsrv-1  MTA on mailsrv-1.west.sesta.com          (1)
applVersion.1 = 5.1
applUptime.1 = 7322                                 (2)
applOperStatus.1 = up                               (3)
applLastChange.1 = 7422                             (2)
applInboundAssociations.1 =                         (5)
applOutboundAssociations.1 =                        (2)
applAccumulatedInboundAssociations.1 = 873
```

```
applAccumulatedOutboundAssociations.1 = 234
applLastInboundActivity.1 = 1054822              (2)
applLastOutboundActivity.1 = 1054222             (2)
applRejectedInboundAssociations.1 = 0            (4)
applFailedOutboundAssociations.1 = 17
applDescription.1 = Sun Java System Messaging Server 6.1
applName.2     1 = mailsrv-1 HTTP WebMail svr. mailsrv-1.sesta.com     (1)
...
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
...
```

注释：

1. 应用程序 (`.appl*`) 后缀（`.1`、`.2` 等）为行编号 `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，表格的第一行提供 MTA 中的数据，第二行提供 POP 服务器中的数据，等等。

   等号后边的名称是受监视的 Messaging Server 实例的名称。在此示例中，实例名称是 mailsrv-1。

2. 这些是 SNMP 时间戳值，也是事件发生时的 `sysUpTime` 的值。`sysUpTime` 是 SNMP 主代理启动后以百分之一秒为单位的计数。

3. 通过已配置的 TCP 端口实际连接到 HTTP、IMAP、POP、SMTP 和 SMTP Submit 服务器，并使用相应协议（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，这些探测将显示为服务器的正常入站连接，并会影响每台服务器的 `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。尽管作业控制器中包含 "congested" 这一概念，但 MTA 状态中没有此概念。

4. 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，而不是被拒绝的入站连接尝试的数量。

A.5.1.1 applTable 的用法

监视列出的每个应用程序的服务器状态 (`applOperStatus`) 对于监视每台服务器至关重要。

如果自最后一次 MTA 入站活动（如 applLastInboundActivity 所示）至今已有很长一段时间，则可能出现了故障，从而无法连接。如果 applOperStatus=2 (down)，则受监视服务已关闭。如果 applOperStatus=1 (up)，则问题可能出现在其他地方。

A.5.2 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  = 129.146.198.167          (1)
    assocApplicationProtocol.1.1 = applTCPProtoID.25       (2)
    assocApplicationType.1.1 = peerinitiator(3)            (3)
    assocDuration.1.1 = 400                                (4)
...
```

注释：

在后缀 .x.y (1.1) 中，x 为应用程序索引 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。

1. 远程 SMTP 客户端的源 IP 地址。
2. 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 使用的 SMTP 协议。
3. 无法判断远程 SMTP 客户端是用户代理 (UA) 还是其他 MTA。因此，子代理始终报告 peer-initiator，而不报告 ua-initiator。
4. 这是 SNMP TimeInterval，单位为百分之一秒。在此示例中，连接已打开 4 秒钟。

A.5.2.1 assocTable 的用法

该表用来诊断活动问题。例如，如果突然有 200,000 个入站连接，查看此表可以知道它们的来源。

A.5.3 mtaTable

这是一维表格，其中一行用于 applTable 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（称为组）的总数。

以下是 applTable (mib-2.28.1.1) 中的数据的示例。

mtaTable:

```
    mtaReceivedMessages.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      (1)
    mtaFailedConvertedMessages.1 = 0
    mtaLoopsDetected.1 = 0                    (2)
```

注释：

后缀 .x (.1) 提供此应用程序在 applTable 中的行编号。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。

1. 对于转换通道，仅使用非零值。
2. 对当前存储在 MTA 邮件队列中的 .HELD 邮件文件进行计数。

A.5.3.1 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。

A.5.4 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的计数 (mtaGroupStoredMessages) 很重要：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) 中的数据的示例。

mtaGroupTable:

```
mtaGroupName.1.1 = tcp_intranet                    1
        ...
mtaGroupName.1.2 = ims-ms
        ...
```

```
mtaGroupName.1.3 = 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 = 03         2
    mtaGroupFailedConvertedMessages.1.3 = 0
    mtaGroupCreationTime.1.3 = 0
    mtaGroupHierarchy.1.3 = 0
    mtaGroupOldestMessageId.1.3 = <01IFBV8AT8HYB4T6UA@red.iplanet.com>
    mtaGroupLoopsDetected.1.3 = 0                        3
    mtaGroupLastOutboundAssociationAttempt.1.3 = 1054222
```

注释：

在后缀 .x.y（例如：1.1、1.2、1.3）中，x 为应用程序索引 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。

1. 所报告的通道的名称。在此示例中为 tcp_intranet 通道。
2. 对于转换通道，仅使用非零值。
3. 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。

A.5.4.1 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，退回在每晚进行，因此您需要使用 mtaGroupOldestMessageStored >（最长存在时间 + 24 小时）进行测试。

如果 mtaGroupLoopsDetected 大于 0，则检测到邮件循环。

A.5.5 mtaGroupAssociationTable

这是三维表格，其条目是 `assocTable` 的索引。对于 `applTable` 中的每个 MTA，都有一个二维子表格。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，通道当前正在使用的每个活动网络连接都有一个条目。该条目的值是 `assocTable` 的索引（由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` 中的相关通道关联起来。

以下是 `mtaGroupAssociationTable` (mib-2.28.3.1) 中的数据的示例。

`mtaGroupAssociationTable:`

```
mtaGroupAssociationIndex.1.3.1 = 1      1
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
```

注释：

在后缀 `.x.y.z` 中，`x` 为应用程序索引 `applIndex`，表示报告的是 `applTable` 中的哪个应用程序。在此示例中为 MTA。`y` 表示报告的是 `mtaGroupTable` 中的哪个通道。在此示例中，3 表示 tcp_local 通道。`z` 用于枚举向通道打开的或来自通道的关联。

1. 此处的值是 `assocTable` 的索引。特别是，`x` 和该值将分别成为 `applIndex` 和 `assocIndex` 在 `assocTable` 中的索引值。或者，换言之（忽略 `applIndex`），`assocTable` 中的第一行说明了由 tcp_local 通道所控制的网络连接。

A.5.6 mtaGroupErrorTable

这又是一个三维表格，它给出在尝试邮件传送时每个 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
    ...
```

注释：

1. 在后缀 `.x.y.z` 中，`x` 为应用程序索引 `applIndex`，表示报告的是 `applTable` 中的哪个应用程序。在此示例中为 MTA。`y` 表示报告的是 `mtaGroupTable` 中的哪个通道。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，分别表示此通道在尝试邮件传送时遇到的临时错误和永久性错误的计数。

A.5.6.1 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大可能表示向消息存储传送邮件时遇到了问题（例如，分区已满、`stored` 问题，等等）。

◆ ◆ ◆ 附 录 B

在 Messaging Server 中管理 Event Notification Service

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：

有关 ENS 和 ENS API 的更多信息，请参见《Sun Java Communications Suite 5 Event Notification Service Guide》。

B.1 在 Messaging Server 中装入 ENS Publisher

Event Notification Service (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。

启动 Messaging Server 时，ENS 和 iBiff（用于 Messaging Server 的 ENS Publisher）被绑定在一起。默认情况下启用了 ENS，但是未装入 iBIFF。（请参见第 811 页中的 “B.1 在 Messaging Server 中装入 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 Messaging Server。

▼ 在 Messaging Server 中装入 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 `mailsrv`。

1. 作为 `mailsrv` 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 `root` 时，请先停止然后重新启动 Messaging Server。

   cd *msg-svr-base* **/sbin**

   ./stop-msg

   ./start-msg

3. 现在准备通过 ENS 接收通知。请参见第 812 页中的“ B.2 运行样例 Event Notification Service 程序 ”

B.2 运行样例 Event Notification Service 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` 目录中。

▼ 运行样例 ENS 程序

1. 转至 *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` 示例。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 通知都应显示在 `asub` 窗口中。

4. 要接收由 iBiff 发布的通知，请编写与 `asub.c` 类似的程序。

   有关样例程序以及编写您自己的用于 ENS 的程序的更多信息，请参见《Sun Java Communications Suite 5 Event Notification Service Guide》。

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。

B.3 管理 Event Notification Service

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 的行为。

B.3.1 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 `root` 才能运行这些命令。

- 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**

▼ 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**

B.3.2 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正文的最大大小（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。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。

表 B–1 iBiff配置参数 （续）

参数	说明
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。

◆ ◆ ◆ 附 录 C

短消息服务 (Short Message Service, SMS)

本章介绍如何在 Sun™ ONE Messaging Server 上实现短消息服务 (Short Message Service, SMS)。本章包含以下主题：

C.1 介绍

Sun Java System Messaging Server 通过短消息服务 (Short Message Service, SMS) 来实现电子邮件至移动设备与移动设备至电子邮件之间的邮件服务。SMS 可配置为单向（仅电子邮件至移动设备）或双向（电子邮件至移动设备与移动设备至电子邮件）。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 C–1 说明了单向与双向 SMS 消息的逻辑流。

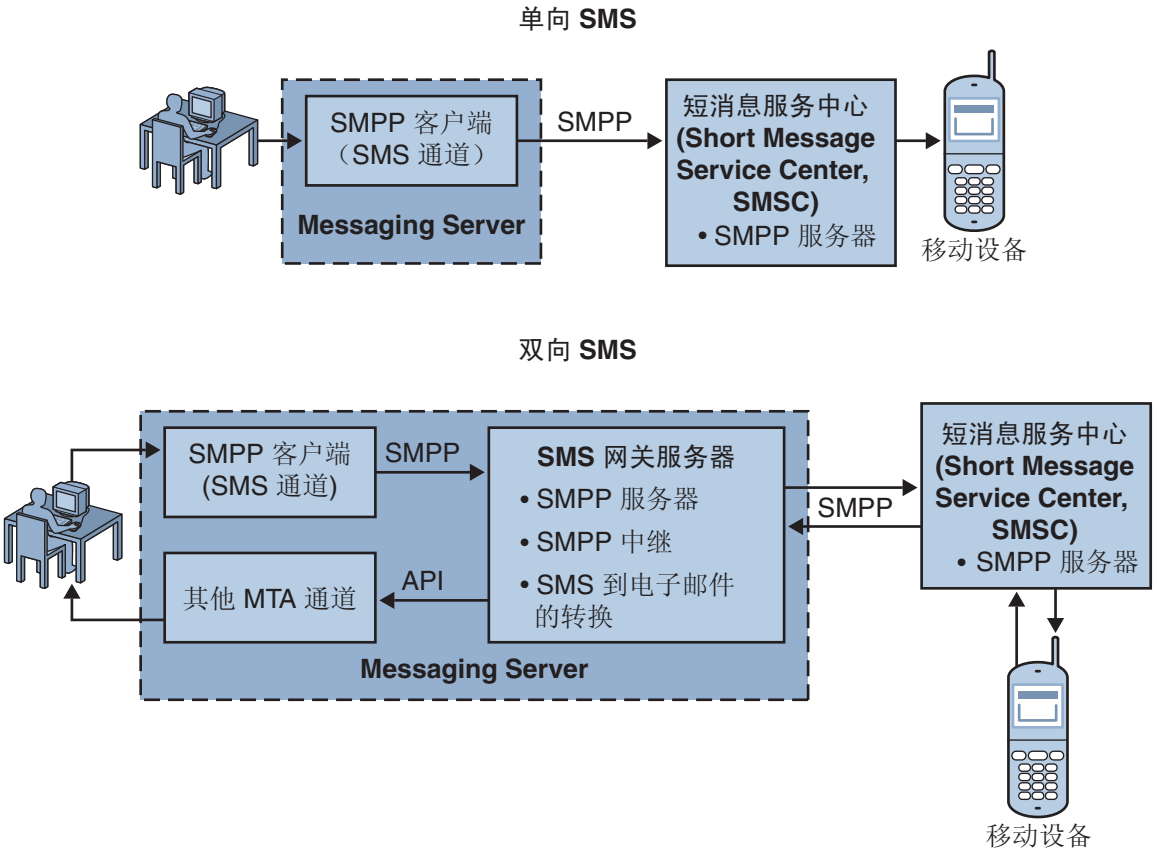


图 C–1 单向和双向 SMS 逻辑流

C.1.1 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 客户端（MTA SMS 通道）。此 SMS 通道将已排队的电子邮件消息转换成 SMS 消息，如第 819 页中的 “C.2.2 电子邮件到 SMS 的转换过程”中所述。这种转换程序包含对多部分 MIME 消息以及字符集转换问题的处理。

执行此功能时，SMS 通道起到了 (SMPP) 外部短消息实体 (ESME) 的作用。

C.1.1.1 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 客户端）（如前一主题中所述），还需要 SMS Gateway Server。Sun Java System Messaging Server 会将 SMS Gateway Server 作为其常规安装过程的一部分来安装，之后您必须对其进行配置。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 客户端。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 – 在 Windows 平台上，Sun Java System Messaging Server 不支持双向 SMS。

C.1.2 要求

本手册假定您已阅读了 Logica CMG 的 SMPP 规范和适用于您的 SMSC 的 SMPP 文档。

为了实现 SMS，您必须具备以下条件：

- 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 883 页中的 “C.6 SMS Gateway Server 存储要求”。

C.2 SMS 通道操作原理

SMS 通道是一种多线程通道，它将已排队的电子邮件消息转换成 SMS 消息，然后将其提交以传送至 SMSC。

本节包含以下通道操作主题：

- 第 826 页中的 “C.2.4 站点定义的地址有效性检查和转换”
- 第 828 页中的 “C.2.5 站点定义的文本转换”

C.2.1 将电子邮件定向到通道

按照第 831 页中的 “C.3 SMS 通道配置” 配置 SMS 通道时，一个或多个主机名将与该通道关联。为便于讨论，我们假定主机名 `sms.siroe.com` 就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` 可以是 SMS 目标地址（例如，无线电话号码、寻呼机 ID 等），也可以是以下格式的属性-值对列表：

```
/attribute1=value1/attribute2=value2/.../@sms.siroe.com
```

表 C–1 提供了可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 C–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`	使用指定的 `NPI` 值。选项 `USE_HEADER_FROM=0` 时忽略。
`FROM_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` 的值和 第 839 页中的 “MAX_MESSAGE_SIZE” 通道选项指定的值两者之中的较小值。
`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` 的值和 第 840 页中的 “MAX_PAGES_PER_MESSAGE” 通道选项指定的值两者之中的较小值。
`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 (Numeric Plan Indicator, NPI) 值。有关此属性接受的值的信息，请参见 第 842 页中的 “DEFAULT_DESTINATION_NPI” 通道选项的说明。使用此属性时，其值将覆盖 `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 第 839 页中的 “MAX_PAGE_SIZE” 通道选项指定的值两者之中的最小值。
`TO`	ID 的同义词。
`TO_NPI`	NPI 的同义词。
`TO_TON`	TON 的同义词。

表 C–1 SMS 属性 （续）

属性名称	属性值和用法
TON	为使用 ID 属性给定的目标 SMS 地址，指定一个数字类型 (Type of Number, TON) 值。有关此属性接受的值的信息，请参见 第 843 页中的 “DEFAULT_DESTINATION_TON” 通道选项的说明。使用此属性时，其值将覆盖 DEFAULT_DESTINATION_TON 通道选项所给定的值。

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 826 页中的 “C.2.4 站点定义的地址有效性检查和转换”。

C.2.2 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。

电子邮件消息的标题行和文本部分中所使用的字符集均将被转换成 Unicode，然后再转换成相应的 SMS 字符集。

如果没有 SMS_TEXT 映射表（请参见第 828 页中的 “C.2.5 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 C–2 中的说明进行处理。

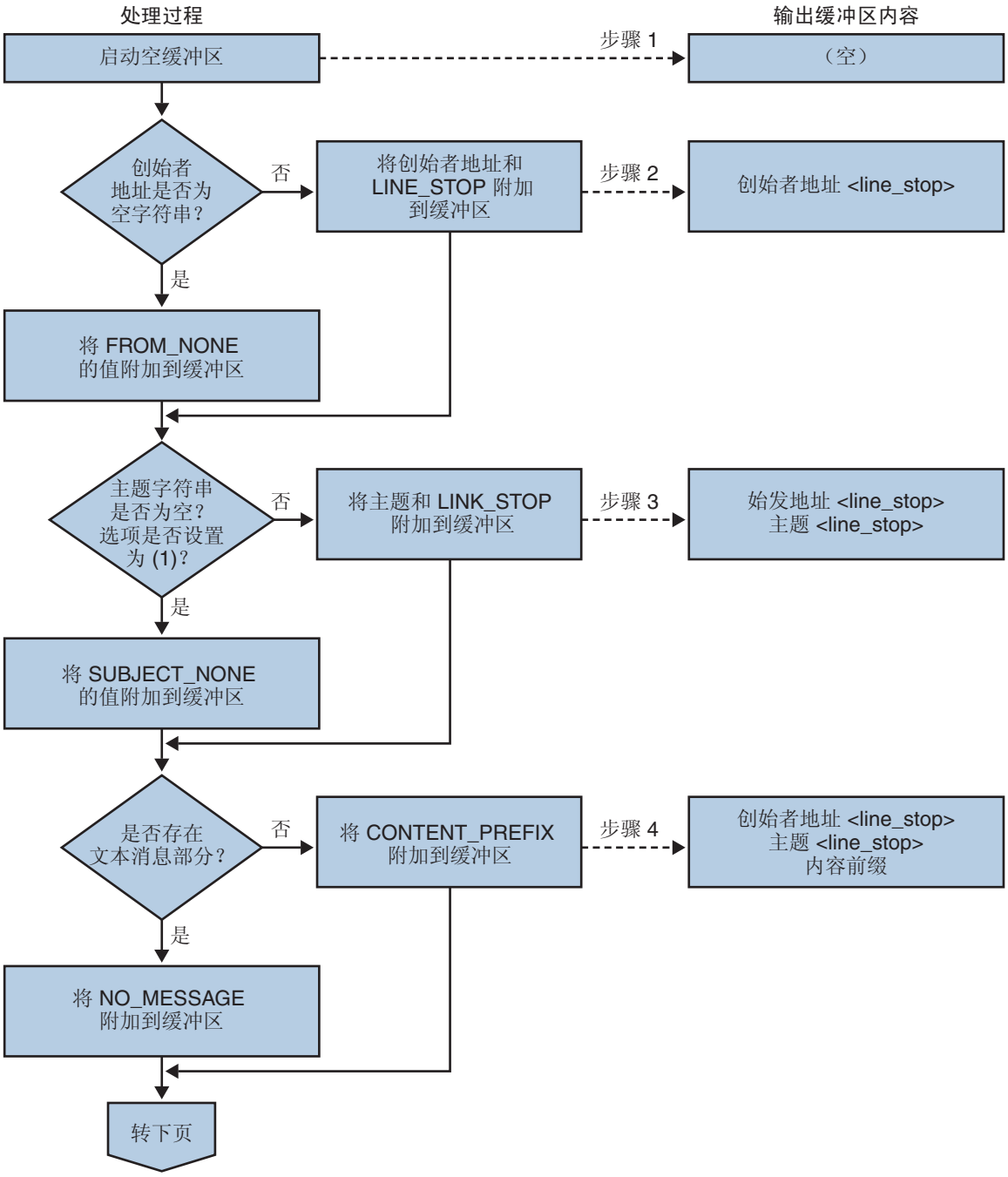


图 C–2 SMS 通道的电子邮件处理

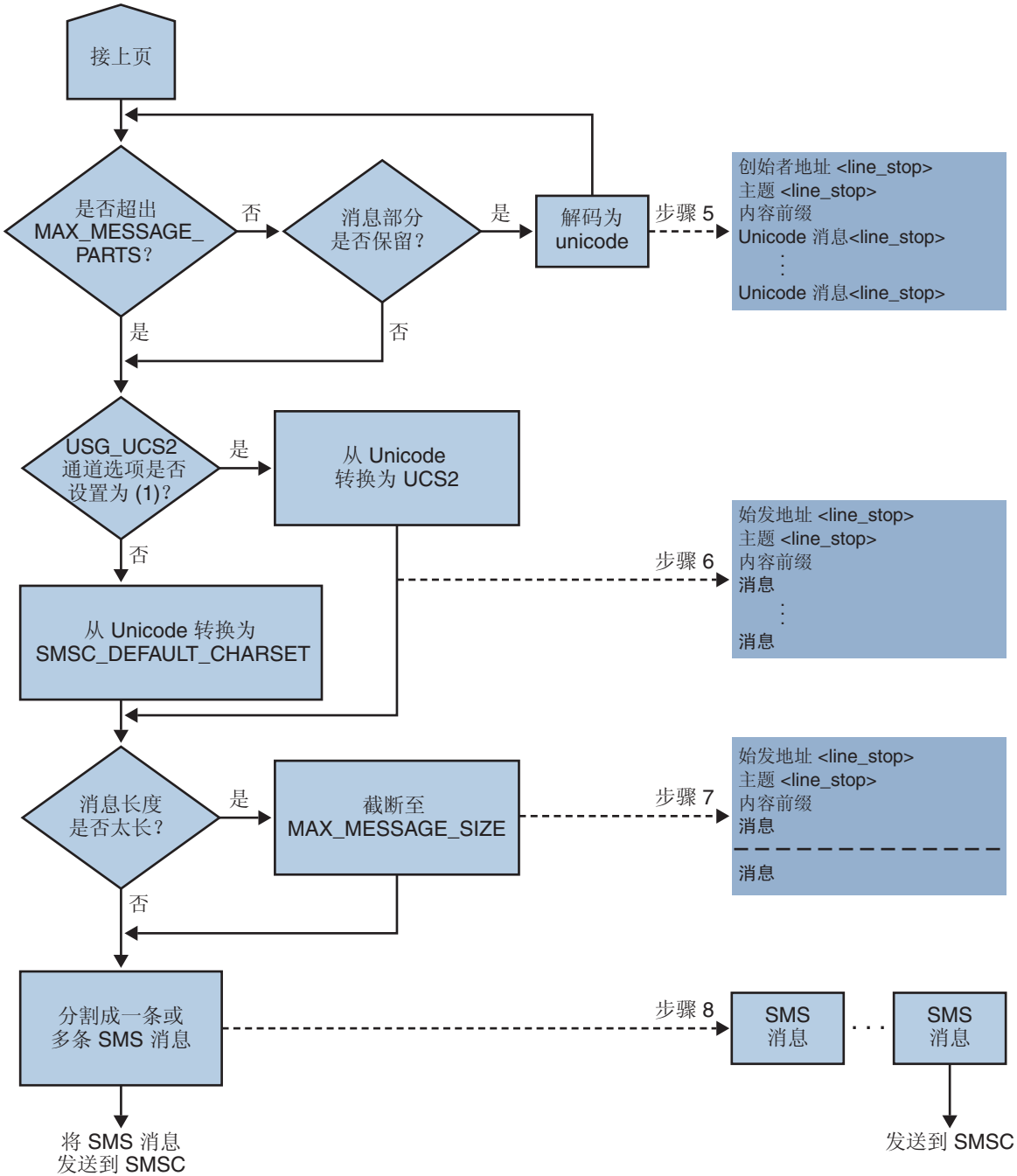


图 C–3 SMS 通道电子邮件处理（续）

以下步骤与图 C–2 中的编号框相对应：

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之一，这些源按首选项的降序显示：

   ```
   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，第 852 页中的 “FROM_NONE” 通道选项的值将会附加到缓冲区。

   但是，如果创始者地址是一个非空字符串，则 第 852 页中的 “FROM_FORMAT” 通道选项的处理结果和 `LINE_STOP` 通道选项的值均会附加到输出缓冲区。

   请注意，只有 第 841 页中的 “USE_HEADER_RESENT” 选项值为 1 时，才考虑 `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 第 852 页中的 “SUBJECT_NONE” 选项的值会附加到输出缓冲区。

   否则，第 852 页中的 “SUBJECT_FORMAT” 选项的处理结果和 第 852 页中的 “LINE_STOP” 通道选项的值均会附加到输出缓冲区。
4. 如果没有文本消息部分，则 第 852 页中的 “NO_MESSAGE” 通道选项的值会附加到输出缓冲区。

   若有文本消息部分，则 第 851 页中的 “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，则该文本部分就会被解码为 Unicode，并连同 `LINE_STOP` 通道选项的值一起附加到缓冲区。
6. 然后，输出缓冲区的结果将从 Unicode 转换成 SMSC 的默认字符集或 UCS2 (UTF-16)。SMSC 的默认字符集是通过 第 840 页中的 “SMSC_DEFAULT_CHARSET” 选项来指定的。
7. 转换完毕后，所得到的结果将被截断，以使之不超过 第 839 页中的 “MAX_MESSAGE_SIZE” 中设置的字节数。
8. 然后，在第 819 页中的 “C.2.2 电子邮件到 SMS 的转换过程” 中转换而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 消息都不会长于 `MAX_PAGE_SIZE` 中设置的字节数。最多将生成数量与 第 840 页中的 “MAX_PAGES_PER_MESSAGE” 中所设置数量相同的 SMS 消息。

注 – 由于一条电子邮件消息可能会有多个收件人，因此，可能需要对每个收件人地址都执行步骤 6 至步骤 8，这样将可以使用第 4 页的“将电子邮件定向到通道”中所述的 MAXLEN、MAXPAGES 或 PAGELEN 属性。

C.2.2.1 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's 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's meeting Msg:The staff meeting is at 14:30 today in the
big conference room.
```

C.2.3 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) 将通过 port 通道关键字来指定。

当有消息需要处理时，通道就会被启动。该通道将作为发送器绑定至 SMPP 服务器，并递交使用 ESME_ 通道选项（如第 848 页中的 “C.3.3.4 SMPP 选项”中所述）指定的证书。表 C–2 列出了 BIND_TRANSMITTER PDU（Protocol Data Unit，协议数据单元）中的字段集，并给出了它们的值：

表 C–2 生成的 BIND_TRANSMITTER PDU 中的字段

字段	值
system_id	第 848 页中的 “ESME_SYSTEM_ID” 通道选项；默认值为空字符串
password	第 848 页中的 “ESME_PASSWORD” 通道选项；默认值为空字符串
system_type	第 849 页中的 “ESME_SYSTEM_TYPE” 通道选项；默认值为空字符串
interface_version	0x34 表示 SMPP V3.4
addr_ton	第 848 页中的 “ESME_ADDRESS_TON” ；默认值为表示未知 TON 的 0x00
addr_npi	第 848 页中的 “ESME_ADDRESS_NPI” ；默认值为表示未知 NPI 的 0x00
addr_range	第 848 页中的 “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 UNBIND，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，则会发出 UNBIND，而 TCP/IP 连接将被关闭并建立一个新的连接和 BIND。如果远程 SMPP 服务器在完成其 SMS 消息发送之前发送了 UNBIND，也会发生类似情况。

然后，SMS 消息使用 SMPP SUBMIT_SM PDU 进行提交。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，仅当 第 841 页中的 “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，仅当 第 841 页中的 “USE_HEADER_RESENT” 选项的值为 1 时，才考虑 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必须都为 1 时，才考虑 Resent-reply-to: 标题行。）这两个选项的默认值均为值 0。因此，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 C–3 列出了 SUBMIT_SM PDU 中的强制性字段集：

表 C–3 生成的 SUBMIT_SM PDU 中的强制性字段

字段	值
service_type	第 846 页中的 “DEFAULT_SERVICE_TYPE” 通道选项；默认值为空字符串。
source_addr_ton	第 846 页中的 “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	第 846 页中的 “DEFAULT_SOURCE_NPI” 通道选项；默认值为 0x00。
source_addr	第 846 页中的 “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 第 843 页中的 “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 第 846 页中的 “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请参见第 818 页中的 “C.2.1 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，所有这些都表示一般优先级；请参见 第 844 页中的 “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	第 846 页中的 “DEFAULT_VALIDITY_PERIOD” 通道选项；默认值为空字符串，表示应使用 SMSC 的默认值。
registered_delivery	0x00，表示不使用已注册的传送。

表 C–3 生成的 SUBMIT_SM PDU 中的强制性字段 （续）

字段	值
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 819 页中的“C.2.2 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 819 页中的“C.2.2 电子邮件到 SMS 的转换过程”。

表 C–4 显示了 SUBMIT_SM PDU 中的可选字段：

表 C–4 生成的 SUBMIT_SM PDU 中的可选字段

字段	值
privacy	请参见第 845 页中的“DEFAULT_PRIVACY”通道关键字的说明；除非电子邮件消息包含 Sensitivity: 标题行，否则默认设置为不提供此字段。
sar_refnum	请参见第 848 页中的“USE_SAR”通道关键字的说明；默认设置为不提供这些字段。
sar_total	请参见上述的 sar_refnum。
sar_seqnum	请参见上述的 sar_refnum。

通道将保持与 SMPP 服务器的联结，直至它再没有要提交的 SMS 消息（消息队列为空）或者已超过第 849 页中的“MAX_PAGES_PER_BIND”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都有要提交的 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，一个给定的线程将提交一条 SMS 消息，然后在提交另一条 SMS 消息之前，先等待提交响应（即 SUBMIT_SM_RESP PDU）。

C.2.4 站点定义的地址有效性检查和转换

站点可能想要将有效性检查和转换应用于收件人电子邮件地址（如第 818 页中的“C.2.1 将电子邮件定向到通道”中所述）中已编码的 SMS 目标地址。

- 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）

前两项任务可专门使用 第 847 页中的 “DESTINATION_ADDRESS_NUMERIC” 和 第 847 页中的 “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，或者使用 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。

假设目标地址必须仅为数字格式，长度为 10 或 11 位且以字符串 "+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将调用名为 X-REWRITE-SMS-ADDRESS 的站点定义的映射表。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
```

如果使用上述设置，请确保 第 847 页中的 “DESTINATION_ADDRESS_NUMERIC” 选项的值为 0（默认值）。否则，"+" 将从 SMS 目标地址中删除。

C.2.5 站点定义的文本转换

站点可以使用转换规则表自定义第 819 页中的 “C.2.2 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来指定。

映射表的名称应为 *SMS_Channel*_TEXT，其中 *SMS_Channel* 为 SMS 通道的名称；例如，如果通道名为 sms，则映射表名为 SMS_TEXT，如果通道名为 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：

- 第 828 页中的 “C.2.5.1 消息标题条目”
- 第 829 页中的 “C.2.5.2 消息正文条目”

C.2.5.1 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，则将会使用映射文件的模式匹配和字符串替换功能将该标题行替换为替换文本 replacement-text。如果在替代文本中指定了元字符 $Y，则标题行的最终映射结果将会包含在 SMS 消息中。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，其中 From: 和 Subject: 分别缩写为 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，因此，例如标题行

```
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。

C.2.5.2 消息正文条目

这些条目建立了适用于每行消息正文的映射。每行消息正文将在并入被生成的 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*

如果消息正文中的某一行与 *pattern* 模式匹配，则会被替换文本 *replacement-text* 所替换。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|。

C.2.5.3 SMS 映射表示例

示例 C–1 中显示了一个 SMS_TEXT 映射表示例。每行末尾括号内的数字都对应于该表之后标题为第 829 页中的 “说明文本”一节中的条目编号。

示例 C–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

上述 SMS_TEXT 映射表示例中条目的说明如下：

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. 这两个条目会使 `From:` 和 `Subject:` 标题行包含在 SMS 消息中。`From:` 和 `Subject:` 分别缩写为 `F:` 和 `S:`。某些其他条目可以进一步影响 `From:` 和 `Subject:` 标题行。

   此条目将把包含 <...> 模式的 `From:` 标题行缩减至只剩下尖括号中的文本。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正文行中删除前导和后缀空格。
6. 这两个条目会将消息标题和正文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:` 标题行的正文：

```
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 – `imsimta` 测试映射实用程序可用于测试映射表。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 test` 实用程序的详细信息，请参见《Sun Java System Messaging Server 6.3 Administration Reference》中的“imsimta test”。

C.3 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。除了几种例外情况外，对于单向和双向功能，SMS 通道的设置均相同。这些例外情况将在第 858 页中的 “C.3.7 为双向 SMS 配置 SMS 通道”主题中说明。

本节包含以下主题：

C.3.1 添加 SMS 通道

将 SMS 通道添加至 Messaging Server 配置需要两个步骤：

1. 第 832 页中的 “C.3.1.1 添加通道定义和重写规则” 。
2. 第 834 页中的 “C.3.2 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：第 848 页中的 “ESME_PASSWORD” 、第 848 页中的 “ESME_SYSTEM_ID” 、第 839 页中的 “MAX_PAGE_SIZE” 、第 846 页中的 “DEFAULT_SOURCE_TON” 和 第 843 页中的 “DEFAULT_DESTINATION_TON” 。而且，如上所述，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 855 页中的 “C.3.4 添加附加 SMS 通道” 。

请注意以下说明：如果更改了 `imta.cnf` 文件，则必须重新编译。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。某些更改要在重新编译并重新启动 SMTP 服务器后才会生效。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。

C.3.1.1 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：

▼ 添加通道定义和重写规则

1 **将 SMS 通道添加到 MTA 的配置之前，需要为该通道挑选一个名称。通道的名称可以是 `sms` 或 `sms_x`，其中 `x` 是长度在一至三十六个字节之间的任何字符串，且不区分大小写。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前添加一个空白行：**

```
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* 是每个传送进程中 SMPP 服务器同时连接的最大数量，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 834 页中的 “C.3.1.2 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 856 页中的 “C.3.5 调整传送重试的频率”。

如果要为 `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，则为 `smpp-host-name` 指定 [127.0.0.1]。或者，请考虑使用第 849 页中的 “SMPP_SERVER” 通道选项。

注 – 对于 Sun Java System Messaging Server 6.1，使用 `master` 通道关键字已过时。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. **使用 `imsimta cnbuild` 命令重新编译此配置。**

6. **使用 `imsimta restart dispatcher` 命令重新启动 SMTP 服务器。**

7. **使用上述配置，将电子邮件消息寻址至 `id@smpp-host-name`（例如 `123456@smpp.siroe.com`），从而将其定向到通道。有关寻址的详细信息，请参见第 819 页中的 “C.2.2 电子邮件到 SMS 的转换过程”。**

8. **（可选）如果要对用户隐藏 SMPP 服务器的主机名，或者要将其他主机名与同一通道相关联，则请添加其他重写规则。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发送至 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，第 849 页中的 “SMPP_SERVER” 和 第 849 页中的 “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。使用 SMPP_PORT 选项时，无需同时使用 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。SMPP_SERVER 选项的其他用法会在第 855 页中的 “C.3.4 添加附加 SMS 通道”中进行介绍。

C.3.1.2 控制同时连接数目

threaddepth 通道关键字控制每个传送进程中，要指定给每个传送线程的消息数量。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)。第 849 页中的 “SMPP_MAX_CONNECTIONS” 选项控制传送进程中传送线程的最大数量。而 job_limit 选项对于通道运行时所在的作业控制器处理池而言，则控制同时执行的传送进程的最大数量。

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 服务器只允许单一连接，则 SMPP_MAX_CONNECTIONS 和 job_limit 都必须设置为 1。调整这些值时，应优先允许 job_limit 大于 1。

C.3.2 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，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，如果通道名为 sms_mway，则通道选项文件为：

```
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
```

有关可用的 SMS 通道选项以及各选项说明的列表，请参见第 835 页中的 “C.3.3 可用选项” 。

C.3.3 可用选项

SMS 通道包含许多选项，这些选项分为六大类：

- **电子邮件至 *SMS* 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**：调试和日志记录选项。

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 C–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
第 838 页中的 “GATEWAY_NOTIFICATIONS”	指定是否将电子邮件通知消息转换成 SMS 消息。	`0`
第 839 页中的 “MAX_MESSAGE_PARTS”	从电子邮件消息中提取的消息部分的最大数目	`2`
第 839 页中的 “MAX_MESSAGE_SIZE”	从电子邮件消息中提取的字节的最大数目	`960`
第 839 页中的 “MAX_PAGE_SIZE”	一条 SMS 消息中可容纳的字节的最大数目	`160`
第 840 页中的 “MAX_PAGES_PER_MESSAGE”	电子邮件消息分割成的 SMS 消息的最大数目	`6`
第 840 页中的 “ROUTE_TO”	将 SMS 消息路由到指定的 IP 主机名。	
第 840 页中的 “SMSC_DEFAULT_CHARSET”	SMSC 所使用的默认字符集。	`US-ASCII`
第 840 页中的 “USE_HEADER_FROM”	设置 SMS 源地址	`0`
第 841 页中的 “USE_HEADER_PRIORITY”	控制电子邮件消息标题中优先级信息的使用	`1`

表 C–5 SMS 通道选项 （续）

第 841 页中的 “USE_HEADER_REPLY_TO”	控制生成 SMS 源地址时 `Reply-to:` 标题行的使用	`0`
第 841 页中的 “USE_HEADER_RESENT”	控制生成创始者信息时 `Resent-*:` 标题行的使用	`0`
第 841 页中的 “USE_HEADER_SENSITIVITY”	控制电子邮件消息标题中保密性信息的使用	`1`
第 842 页中的 “USE_UCS2”	在 SMS 消息中使用 UCS2 字符集（如果可用）	`1`
SMS Gateway Server 选项		
第 842 页中的 “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		
第 842 页中的 “DEFAULT_DESTINATION_NPI”	默认 SMS 目标地址为 NPI	`0x00`
第 843 页中的 “DEFAULT_DESTINATION_TON”	默认 SMS 目标地址为 TON	`0x01`
第 844 页中的 “DEFAULT_PRIORITY”	SMS 消息的默认优先级设置	`0=GSM、CDMA` `1=TDMA`
第 845 页中的 “DEFAULT_PRIVACY”	SMS 消息的默认保密性值标志	`-1`
第 846 页中的 “DEFAULT_SERVICE_TYPE”	与提交的 SMS 消息相关联的 SMS 应用服务	N/A
第 846 页中的 “DEFAULT_SOURCE_ADDRESS”	默认 SMS 源地址	`0`
第 846 页中的 “DEFAULT_SOURCE_NPI”	默认的 SMS 源地址为 NPI	`0x00`
第 846 页中的 “DEFAULT_SOURCE_TON”	默认的 SMS 源地址为 TON	`0x01`
第 846 页中的 “DEFAULT_VALIDITY_PERIOD”	SMS 消息的默认有效期	N/A
第 847 页中的 “DESTINATION_ADDRESS_NUMERIC”	将 SMS 目标地址缩减为仅包含 0 至 9 个字符	`0`

表 C–5 SMS 通道选项 （续）

第 847 页中的 “DESTINATION_ADDRESS_PREFIX”	目标 SMS 地址带有前缀的文本字符串	N/A
第 847 页中的 “PROFILE”	要使用的 SMS 配置文件	GSM
第 848 页中的 “USE_SAR”	使用 SMS sar_ 字段排列多条 SMS 消息	0
SMPP 协议选项		
第 848 页中的 “ESME_ADDRESS_NPI”	绑定到 SMTP 服务器时要指定的 ESME NPI	0x00
第 848 页中的 “ESME_ADDRESS_TON”	绑定到 SMPP 服务器时要指定的 ESME TON	0x00
第 848 页中的 “ESME_IP_ADDRESS”	运行 Sun Java System MessagingServer 的主机的 IP 地址	N/A
第 848 页中的 “ESME_PASSWORD”	绑定到 SMPP 服务器时要递交的密码	N/A
第 848 页中的 “ESME_SYSTEM_ID”	绑定时要递交到 SMSC 的系统标识	N/A
第 849 页中的 “ESME_SYSTEM_TYPE”	绑定时要递交到 SMSC 的系统类型	N/A
第 849 页中的 “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
第 849 页中的 “REVERSE_ORDER”	多部分 SMS 消息的传输顺序	0
第 849 页中的 “SMPP_MAX_CONNECTIONS”	SMPP 服务器同时连接的最大数目	20
第 849 页中的 “SMPP_PORT”	对于单向 SMS，指 SMPP 服务器将侦听的 TCP 端口。对于双向 SMS，供 SMPP 中继的 LISTEN_PORT 使用的同一 TCP 端口。	N/A
第 849 页中的 “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
第 850 页中的 “TIMEOUT”	用 SMPP 服务器完成读写操作超时	30
本地化选项		
第 851 页中的 “CONTENT_PREFIX”	引入电子邮件消息内容的文本	Msg:

表 C–5 SMS 通道选项 （续）

第 851 页中的 “DSN_DELAYED_FORMAT”	用于传送延迟通知的格式化字符串	空字符串
第 851 页中的 “DSN_FAILED_FORMAT”	用于传送失败通知的格式化字符串	参见说明
第 851 页中的 “DSN_RELAYED_FORMAT”	用于中继通知的格式化字符串。	参见说明
第 851 页中的 “DSN_SUCCESS_FORMAT”	要成功传送通知的格式化字符串。	参见说明
第 852 页中的 “FROM_FORMAT”	指示电子邮件消息创始者时显示的文本	`$a`
第 852 页中的 “FROM_NONE”	没有创始者时显示的文本	N/A
第 852 页中的 “LANGUAGE”	要从其选择文本字段的语言组 (i-default)	`i-default`
第 852 页中的 “LINE_STOP”	从电子邮件消息中提取的、放置在各行末尾的文本	空格字符
第 852 页中的 “NO_MESSAGE”	表示消息无内容的文本	`]no message]`
第 852 页中的 “SUBJECT_FORMAT”	指示电子邮件消息的主题时显示的文本	`$s`
第 852 页中的 “SUBJECT_NONE”	电子邮件消息无主题时显示的文本	N/A

其他选项		
第 853 页中的 “DEBUG”	启用详细调试输出	6
第 871 页中的 “LISTEN_CONNECTION_MAX”	所有 SMPP 中继和服务器实例上允许的并行入站 TCP 连接的最大数量。	10,000
第 872 页中的 “LOG_PAGE_COUNT”	控制 `mail.log` 文件的邮件大小字段中记录的值，使记录的是页数而不是块。	0

C.3.3.1 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。请参见第 819 页中的 “C.2.2 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、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**）将多部分电子邮件消息转换成一条 SMS 消息时，只有第一批 MAX_MESSAGE_PARTS 指定数量的文本部分将会被转换。其余部分将被放弃。默认情况下，MAX_MESSAGE_PARTS 为 2。要使消息部分的数量不受限制，可指定值为 -1。指定值为 0 时，则不会将任何消息内容置于 SMS 消息中。仅使用电子邮件消息的标题行（例如 Subject:）生成 SMS 消息时，此设置会很有效。

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，可以设置从电子邮件消息生成的 SMS 消息中所能包含的总字节数的上限。具体来讲，MAX_MESSAGE_SIZE 指定的最大字节数将用于一条或多条生成的 SMS 消息。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。这对应于 MAX_MESSAGE_SIZE=960。要使字节数不受限制，可指定值为零。

所用的字节数在电子邮件消息从 Unicode 转换成 SMSC 的默认字符集或 UCS2 之后产生。这意味着，如果转换为 UCS2，则值为 960 个字节的 MAX_MESSAGE_SIZE 最多可产生 480 个字符，因为每个 UCS2 字符至少为两个字节长。

请注意，MAX_MESSAGE_SIZE 和 第 840 页中的 “MAX_PAGES_PER_MESSAGE” 选项都用于同一目的：限制所得的 SMS 消息的总大小。实际上，第 839 页中的 “MAX_PAGE_SIZE”=960 和 第 839 页中的 “MAX_PAGE_SIZE”=160 就表示 MAX_PAGES_PER_MESSAGE=6。那么为什么存在两种不同的选项呢？这是为了便于控制页面的整体大小或页数，而无需考虑单条 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 818 页中的 “C.2.1 将电子邮件定向到通道”中所述的 第 818 页中的 “C.2.1 将电子邮件定向到通道” 或 第 818 页中的 “C.2.1 将电子邮件定向到通道” 寻址属性时则很重要。

最后，请注意将使用这两个限制 MAX_MESSAGE_SIZE 和 MAX_PAGE_SIZE * MAX_PAGES_PER_MESSAGE 中较小的一个。

MAX_PAGE_SIZE

（**整数**，>= *10*）使用 MAX_PAGE_SIZE 选项可控制单条 SMS 消息中允许的最大字节数。默认情况下，使用的字节数值为 160。这对应于 MAX_PAGE_SIZE=160。

MAX_PAGES_PER_MESSAGE

（**整数**，*1* **至** *255*）使用此选项，可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，只把电子邮件消息中符合 MAX_PAGES_PER_MESSAGE 设置的部分转换成 SMS 消息。有关进一步的讨论，请参见 第 839 页中的 “MAX_PAGE_SIZE” 选项的说明。

默认情况下，MAX_PAGES_PER_MESSAGE 设置为 1 或 第 839 页中的 “MAX_MESSAGE_SIZE” 除以 第 839 页中的 “MAX_PAGE_SIZE” 的得数二者中的较大值。

ROUTE_TO

（**字符串**、*IP* **主机名**、*1* **至** *64* **个字节**）所有以配置文件为目标的 SMS 消息将使用以下格式的电子邮件地址，重新路由至指定的 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 选项互斥。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，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。接着，数据将会转换成 SMSC 的默认字符集或 UCS2，这取决于 第 842 页中的 “USE_UCS2” 选项的值以及 SMS 消息是否至少包含一个默认 SMSCC 字符集中所没有的字形。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: 地址传送至 SMSC。该值指示 From: 地址的来源及其具备的格式。表 C–6 显示了允许的值及其含义。

表 C–6 USE_HEADER_FROM 值

值	说明
0	始终不从 From: 地址设置 SMS 源地址。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*）此选项用于控制 RFC 822 Priority: 标题行的处理。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，以覆盖通过 第 844 页中的 “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，此选项用于控制是否考虑将 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: 标题行会被忽略。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 已弃用 Reply-to: 和 Resent-reply-to: 标题行。

USE_HEADER_RESENT

（*0* **或** *1*）当 USE_HEADER_FROM=1 时，此选项用于控制是否考虑将 Resent- 标题行用作 SMS 源地址。默认情况下，Resent- 标题行会被忽略。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 已弃用 Resent- 标题行。

USE_HEADER_SENSITIVITY

（*0* **或** *1*）USE_HEADER_SENSITIVITY 选项用于控制 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，以覆盖通过 第 845 页中的 “DEFAULT_PRIVACY” 选项指定的默认 SMS 保密性。这是默认情况，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 第 845 页中的 “DEFAULT_PRIVACY” 选项的说明。

USE_UCS2

（*0* **或** *1*）如果适用，通道将在其生成的 SMS 消息中使用 UCS2 字符集。这是一个默认行为，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 第 840 页中的 “SMSC_DEFAULT_CHARSET” 选项的说明。

表 C–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字形将由助记符号表示（例如用 "AE" 表示 AE-ligature）。

C.3.3.2 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。

C.3.3.3 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 值包含下表 C–8 中所找到的值：

表 C–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

表 C–8 数字规划指标值 （续）

值	说明
9	专用
10	ERMES
14	IP 地址 (Internet)
18	WAP 客户端 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 值包含下表 C–9 中所找到的值：

表 C–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 消息具有强制性优先级字段。下表 C–10 显示了 SMS 优先级值的解释：

表 C–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	紧急	紧急
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，则 `PROFILE=GSM` 和 `CDMA` 使用的默认优先级为 0，第 847 页中的 “PROFILE”=TDMA 的默认优先级为 `1`。

请注意，如果 第 841 页中的 “USE_HEADER_PRIORITY”=1 且电子邮件消息具有 RFC 822 `Priority:` 标题行，则将使用该标题行中指定的优先级来设置所得到的 SMS 消息的优先级。具体来讲，如果 `USE_HEADER_PRIORITY=0`，则 SMS 优先级标志会始终根据 `DEFAULT_PRIORITY` 选项来设置，而 RFC 822 `Priority:` 标题行则始终被忽略。如果 `USE_HEADER_PRIORITY=1`，则原始电子邮件消息的 RFC 822 `Priority:` 标题行将用于设置 SMS 消息的优先级标志。如果此标题行不存在，则使用 `DEFAULT_PRIORITY` 选项设置 SMS 优先级标志。

下表显示用于将 RFC 822 `Priority:` 标题行值转换成 SMS 优先级标志的映射：

表 C–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)

表 C–11 将 Priority 标题转换成 SMS 优先级标志的映射 （续）

RFC 822	SMS 优先级标志		
正常	非优先级 (0)	正常 (1)	正常 (0)
紧急	优先级 (1)	紧急 (2)	紧急 (2)

DEFAULT_PRIVACY

（**整数**，*-1*、*0* **至** *255*）是否要在 SMS 消息中设置保密性标志以及使用何值是通过 DEFAULT_PRIVACY 和 第 841 页中的 “USE_HEADER_SENSITIVITY” 选项来控制的。默认情况下，DEFAULT_PRIVACY 使用值 -1。下表 C–12 显示了将 DEFAULT_PRIVACY 和 第 841 页中的 “USE_HEADER_SENSITIVITY” 选项设置为不同值的结果。

表 C–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	始终将 SMS 保密性标志的值设置为 n。RFC 822 Sensitivity: 标题行则始终被忽略。
-1（默认值）	1（默认值）	仅当原始电子邮件消息包含 RFC 822 Sensitivity: 标题行时，才设置 SMS 消息的保密性标志。在这种情况下，将 SMS 保密性标志设置为与 Sensitivity: 标题行的值对应。该值为默认值。
n >= 0	1	将 SMS 消息的保密性标志设置为对应于原始电子邮件消息的 RFC 822 Sensitivity: 标题行。如果电子邮件消息不包含 Sensitivity: 标题行，则将 SMS 保密性标志的值设置为 n。

下表 C–13 显示了 SMS 保密性值的解释：

表 C–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

下表 C–14 显示了用于将 RFC 822 Sensitivity: 标题行值转换成 SMS 保密性值的映射：

表 C–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
个人	1（有限制）
专用	2（机密）
公司机密	3（秘密）

DEFAULT_SERVICE_TYPE

（**字符串**，*0* **至** *5* **个字节**）与通道生成的 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（cellular messaging，蜂窝式邮件服务）、CPT（cellular paging，蜂窝式呼叫）、VMN（voice mail notification，语音邮件通知）、VMA（voice mail alerting，语音邮件警报）、WAP（wireless application protocol，无线应用协议）和 USSD（unstructured supplementary data services，非结构化辅助数据服务）。

DEFAULT_SOURCE_ADDRESS

（**字符串**，*0* **至** *20* **个字节**）供电子邮件消息生成的 SMS 消息使用的源地址。请注意，当 USE_HEADER_FROM=1 时，使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，该值被禁用，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。有关典型 NPI 值表，请参见 第 842 页中的“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 第 843 页中的“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 消息不会被给定相对有效期；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。可以将这些值的单位指定为秒、分钟、小时或天。下表 C–15 指定了此选项的不同值的格式和说明：

表 C–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 0、0s、0m、0h 或 0d 的规范来选择 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*）使用此选项可删除从电子邮件信封 `To:` 地址所提取的 SMS 目标地址中的所有非数字字符。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，将禁用此删除功能，对应的选项值为 0。请注意，如果启用，则删除操作会在通过 第 847 页中的“DESTINATION_ADDRESS_PREFIX” 选项添加任何目标地址前缀之前完成。

DESTINATION_ADDRESS_PREFIX

（**字符串**）在某些实例中，可能需要确保所有 SMS 目标地址都带有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。要避免前缀被 第 847 页中的“DESTINATION_ADDRESS_NUMERIC” 选项删除，请在 `DESTINATION_ADDRESS_NUMERIC` 选项之后应用此选项。

PROFILE

（**字符串**）指定要与 SMSC 配合使用的 SMS 配置。可能的值为 `GSM`、`TDMA` 和 `CDMA`。如果没有指定，则假设为 GSM。此选项仅用于为其他通道选项（例如 第 844 页中的“DEFAULT_PRIORITY” 和 第 845 页中的“DEFAULT_PRIVACY”）选择默认值。

USE_SAR

（*0* **或** *1*）过大的电子邮件消息可能需要分割成多条 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。这将会生成“分段”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`，表示添加此排序信息（如果适用）。默认设置为不添加排序信息，对应于 `USE_SAR=0`。

指定 `USE_SAR=1` 时，第 849 页中的 “REVERSE_ORDER” 选项将被忽略。

C.3.3.4 SMPP 选项

以下选项可用于指定 SMPP 协议参数。这些名称以字符串 "`ESME_`" 开头的选项可用于识别用作外部短消息实体 (External Short Message Entity, ESME) 的 MTA；即，将 MTA 绑定至 SMPP 服务器，以便将 SMS 消息提交至此服务器的关联 SMSC 时。

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。有关典型 NPI 值表，请参见 第 842 页中的 “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 的值为 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 第 843 页中的 “DEFAULT_DESTINATION_TON” 选项的说明。

ESME_IP_ADDRESS

（**字符串，***0* **至** *15* **个字节**）绑定至 SMPP 服务器时，`BIND` PDU 表示客户端的（即 ESME 的）地址范围是一个 IP 地址。这一操作可通过将 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**）绑定至 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**）绑定至 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**）绑定至 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 服务器可能会限制单个绑定会话期间提交的 SMS 消息的最大数量。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` 错误并在单次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，这些 SMS 消息会按顺序 (`REVERSE_ORDER=0`) 或倒序 (`REVERSE_ORDER=1`) 提交至 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，使用 `REVERSE_ORDER=1`。

请注意，指定 第 848 页中的 “USE_SAR” =1 时，此选项将被忽略。

SMPP_MAX_CONNECTIONS

（**整数**，*1* **至** *50*）此选项控制每个进程中同时执行的 SMPP 连接的最大数量。由于每个连接都有一个相关联的线程，因此该选项还可用于限制每个进程中的“辅助”线程的最大数量。默认情况下，`SMPP_MAX_CONNECTIONS=20`。

SMPP_PORT

（**整数**，*1* **至** *65535*）可使用此选项或 `port` 通道关键字指定 SMPP 服务器侦听的 TCP 端口。此端口号必须通过这两种机制之一进行指定。如果同时使用这两种机制指定，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，请确保其端口与用于 SMPP 中继的 `LISTEN_PORT` 相同。

SMPP_SERVER

（**字符串**，*1* **至** *252* **个字节**）对于单向 SMS，默认情况下，要连接的 SMPP 服务器的 IP 主机名为与通道关联的正式主机名，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，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。

TIMEOUT

（**整数**，>= *2*）默认情况下，等待数据写入 SMPP 服务器完成或从 SMPP 服务器接收数据时，使用的超时时间为 30 秒。可使用 TIMEOUT 选项指定不同的超时值（以秒为单位）。指定值应至少为 1 秒。

C.3.3.5 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，这些字符串会引入电子邮件的 From: 地址和 Subject: 标题行。使用本节所述的通道选项，可为不同语言指定这些字符串的版本，并为该通道指定默认语言。示例 C–2 显示了选项文件的语言部分：

示例 C–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:
  ...
```

在每个 [language=x] 块中，都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] 块以外指定的本地化选项将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**）置于 SMS 消息中电子邮件消息本身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 第 838 页中的 “GATEWAY_NOTIFICATIONS” 设置为 1 才能使此选项生效。GATEWAY_NOTIFICATIONS=0 时，此选项将被忽略。

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 第 838 页中的 “GATEWAY_NOTIFICATIONS” 设置为 1 才能使此选项生效。GATEWAY_NOTIFICATIONS=0 时，此选项将被忽略。

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 第 838 页中的 “GATEWAY_NOTIFICATIONS” 设置为 1 才能使此选项生效。GATEWAY_NOTIFICATIONS=0 时，此选项将被忽略。

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 第 838 页中的 “GATEWAY_NOTIFICATIONS” 设置为 1 才能使此选项生效。GATEWAY_NOTIFICATIONS=0 时，此选项将被忽略。

FROM_FORMAT

（**字符串，*0* 至 *252* 个字节**）用于格式化创始者信息以插入到 SMS 消息中的格式化模板。默认全局值为 US-ASCII 字符串 "$a"，该字符串将替换创始者的电子邮件地址。请参见第 853 页中的 “C.3.3.6 格式化模板” 。

FROM_NONE

（**字符串，*0* 至 *252* 个字节**）没有创始者地址可供显示时置于 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**）用于从中选择文本字符串的默认语言组。如果未指定，则语言将取自主机的默认语言环境规范。如果主机的语言环境规范不可用或对应 "C"，则会使用 i-default。（i-default 对应于 “适用于国际读者的英语文本）

LINE_STOP

（**字符串，*0* 至 *252* 个字节**）置于 SMS 消息中从电子邮件消息提取的各行之间的文本字符串。默认全局值为 US-ASCII 空格字符 " "。

NO_MESSAGE

（**字符串，*0* 至 *252* 个字节**）置于 SMS 消息中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**）用于格式化 Subject: 标题行的内容，以显示在 SMS 消息中的格式化模板。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 853 页中的 “C.3.3.6 格式化模板” 。

有关 Subject: 标题行不存在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，即选择警告消息和错误消息。任何非零值都可为通道本身启用调试输出，这与在通道定义中指定 master_debug 相同。表 C–16 定义了 DEBUG 位掩码的位值。

表 C–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
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，正文数据
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。

C.3.3.6 格式化模板

使用 第 852 页中的 “FROM_FORMAT” 、第 852 页中的 “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，其中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>
```

下表 C–17 显示了可识别的替换序列：

表 C–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"）

表 C–17 替换序列 （续）

序列	说明
$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。如果该文本为空字符串，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
```

C.3.4 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，如果服务器用 `user@host.domain` 表示，则它会查找名为 "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，它会开始查找 ".domain" 的重写规则，如果找不到，则会查找点 (".") 规则。有关重写规则的更多信息，请参见第 11 章。

2. 为了使用不同的通道选项与同一 SMPP 服务器进行通信。

   要使用不同的通道选项与同一 SMPP 服务器进行通信，请在每个通道定义的 第 849 页中的 “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。要使它们能与同一 SMPP 服务器进行通信，请定义两个独立的通道，每个通道均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，若要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要在其通道选项文件中指定第 849 页中的 “SMPP_SERVER”=smpp.siroe.com。

C.3.5 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。如果该消息在一天之后仍不能传送，则 `notices 1` 通道关键字会把它作为不可传送的消息予以返回。

C.3.6 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/ (`http://www.mobilway.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 客户端的 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 客户端将停止并等待 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 字段是要连接的 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 第 849 页中的 “SMPP_SERVER” 和 第 849 页中的 “SMPP_PORT” 通道选项。将 "Account Login" 和 "Account Passwd" 的值分别用于 第 848 页中的 “ESME_SYSTEM_ID” 和 第 848 页中的 “ESME_PASSWORD” 通道选项。使用此信息时，您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
```

C.3.6.1 调试

要调试通道，请在此通道的定义中指定 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至通道的日志文件中。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。

C.3.7 为双向 SMS 配置 SMS 通道

有关配置 SMS 通道的常规指导，请参见上述从第 831 页中的 “C.3 SMS 通道配置” 开始的各个主题。将 SMS 通道配置为好像直接与远程 SMSC 通话一样，以下表 C–18 中列出的情况除外：

表 C–18 双向配置的异常情况

例外	解释
`master` 通道关键字	删除 `master` 通道关键字（如果存在）。 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 868 页中的 “C.5.7 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`	用于实例化 SMPP 中继的 `LISTEN_PORT` 设置所用的同一 TCP 端口（请参见第 865 页中的 “C.5.5.2 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，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 864 页中的 “C.5.5.1 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 862 页中的 “C.5.1 设置双向 SMS 路由选择” 中所提及的，远程 SMSC 需要配置为通过使用 `LISTEN_PORT` 选项指定的 TCP 端口号，将 SMS 地址（在 `DEFAULT_SOURCE_ADDRESS` 通道选项中定义）路由至 Gateway 的 SMP 服务器。（有关如何指定 `LISTEN_PORT`，请参见第 866 页中的 “C.5.5.3 SMPP 服务器”。）

请注意，多个 SMS 通道可使用同一 SMPP 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。

C.4 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 859 页中的 “C.4.1 SMS Gateway Server 功能”
- 第 859 页中的 “C.4.2 SMPP 中继和服务器性能”
- 第 860 页中的 “C.4.3 远程 SMPP 到 Gateway SMPP 的通信”

- 第 861 页中的 “C.4.4 SMS 回复和通知的处理”

C.4.1 SMS Gateway Server 功能

SMS Gateway Server 同时作为 SMPP 中继和服务器运行。它可被配置为具有每项功能的多个“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。

C.4.2 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 客户端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 客户端提交一条消息，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 客户端提交一条消息，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 中继仅适合与限定的 Sun Java System SMPP 客户端（即 Sun Java System Messaging Server 的 SMS 通道）配合使用。它不用于与任意 SMPP 客户端配合使用。

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，对应于以前由 SMS Gateway Server 的 SMPP 中继所中继的电子邮件至移动设备的消息。

所有其他 SMS 消息都将被 SMPP 服务器拒绝。

C.4.3 远程 SMPP 到 Gateway SMPP 的通信

远程 SMPP 客户端使用协议数据单元 (PDU) 与 Gateway SMPP 服务器进行通信。远程 SMPP 客户端发布 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 客户端的下一个请求 PDU 之前，先完成对一个请求 PDU 的响应。

以下表 C–19 列出 Gateway SMPP 服务器所处理的请求 PDU，并指定 Gateway SMPP 服务器的响应。

表 C–19 SMPP 服务器协议数据单元

请求 PDU	SMPP 服务器响应
BIND_TRANSMITTERBIND_TRANSCEIVERUNBIND	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_SMDATA_SM	尝试将目标 SMS 地址与唯一的 SMS 源地址或 Gateway 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 及 ESME_RINVCMDID 错误。
SUBMIT_MULTI	不支持。返回 GENERIC_NAK PDU 及 ESME_RINVCMDID 错误。
REPLACE_SM	不支持。返回 GENERIC_NAK PDU 及 ESME_RINVCMDID 错误。
CANCEL_SM	不支持。返回 GENERIC_NAK PDU 及 ESME_RINVCMDID 错误。
QUERY_SM	不支持。返回 GENERIC_NAK PDU 及 ESME_RINVCMDID 错误。
QUERY_LAST_MSGS	不支持。返回 GENERIC_NAK PDU 及 ESME_RINVCMDID 错误。
QUERY_MSG_DETAILS	不支持。返回 GENERIC_NAK PDU 及 ESME_RINVCMDID 错误。
ENQUIRE_LINK	返回 ENQUIRE_LINK_RESP PDU。
ALERT_NOTIFICATION	已接受但被忽略。

C.4.4 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，每个文件均表示由 `HASH_FILE_ROLLOVER_PERIOD` 指定秒数的事务（默认值为 30 分钟）。每个文件将保留由 `RECORD_LIFETIME` 指定的秒数（默认值为 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 Communications Suite 5 Deployment Planning Guide》。

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、）。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 服务器在其接受提交时返回的、最终收到的消息 ID。

C.4.4.1 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)，则会将收到的消息 ID（如果存在）与历史记录相比较。如果找到匹配地址，请转至步骤 8。[SMS Gateway Server 实际上允许将这些地址递交至 SMPP 中继或 SMPP 服务器。]
3. 如果没有匹配地址，则会将目标 SMS 地址与每个已配置的网关配置文件的 `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，则该消息必须是一个带有已收到消息 ID 的 `SUBMIT_SM` PDU。否则，将被视为是一个回复。

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. 如果是通知，则该 SMS 消息会根据 RFC 1892-1894 被转换成电子邮件传送状态通知 (Delivery Status Notification, DSN)。请注意，原始电子邮件消息的 ESMTP `NOTIFY` 标志 (RFC 1891) 将被接受（例如，如果 SMS 消息是“成功”DSN，而原始电子邮件消息仅请求“失败”通知，则该 SMS 通知将被放弃）。
9. 如果目标 SMS 地址与已配置的网关配置文件中的 `SELECT_RE` 选项相匹配，则该 SMS 消息会被视为是一条移动设备发出的消息，并按照该网关配置文件的 `PARSE_RE_n` 规则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。

C.5 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：

C.5.1 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：

- 第 863 页中的 “C.5.1.1 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。
- 第 863 页中的 “C.5.1.2 设置网关配置文件” —保留该前缀，以与 SMS Gateway Server 配合使用（通过设置网关配置文件）。
- 第 863 页中的 “C.5.1.3 配置 SMSC” —配置 SMSC，以将 SMS 目标地址路由至以此前缀为开头的 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。

C.5.1.1 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 `SELECT_RE` 网关配置文件选项即可完成此操作，如下所示：

  `SELECT_RE=`*prefix*

C.5.1.2 设置网关配置文件

然后，应设置 SMS Gateway Server 的网关配置文件，使所有中继的 SMS 源地址成为唯一地址。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` 进行显式设置。这样将得到如下格式的已中继 SMS 源地址：

`prefix``nnnnnnnnnn`

其中 nnnnnnnnnn 是唯一的十位数十进制数字。

C.5.1.3 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] 指定允许的十位数数字的值，{10, 10} 指定允许的最小十位数与最大十位数，而 {0, 1} 指定可有零或这些十位数数字之一。

C.5.2 启用和禁用 SMS Gateway Server

- 要启用 SMS Gateway Server，配置参数 `local.smsgateway.enable` 的值必须设置为 `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 Gateway Server，请使用以下命令将 `local.smsgateway.enable` 的值设置为 `0`：

  ```
  # configutil -o local.smsgateway.enable -v 0
  ```

C.5.3 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
```

C.5.4 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。其名称必须为：

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
```

C.5.5 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 864 页中的 “C.5.5.1 网关配置文件”
- 第 865 页中的 “C.5.5.2 SMPP 中继”
- 第 866 页中的 “C.5.5.3 SMPP 服务器”

C.5.5.1 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：

▼ 配置电子邮件至移动设备网关配置文件

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 `profile_name` 采用上述格式，其长度不得超过 11 个字节。此名称必须与 SMS 通道选项文件中 `GATEWAY_PROFILE` 通道选项的名称相同。文件名不区分大小写。有关有效通道选项的列表，请参见第 835 页中的 “C.3.3 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 的特性。**

3 **设置其他网关配置文件选项，以符合 SMS 通道的电子邮件特性。**

有关网关配置文件选项的完整说明，请参见第 876 页中的 “C.5.11 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。

C.5.5.2 SMPP 中继

要配置 SMPP 中继，请完成以下步骤：

▼ 配置 SMPP 中继

1 **将 SMPP 中继实例（选项组）添加至 SMS Gateway Server 的配置文件中。**

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。**

SMS 通道的 SMPP_PORT 选项所使用的值必须与中继的 LISTEN_PORT 选项所使用的值相匹配。请为 LISTEN_PORT 选择一个 TCP 端口号，此端口号应未被任何其他 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。

3 **设置 SERVER_HOST 选项。**

中继的 SERVER_HOST 选项应给定远程 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 选项应给定远程 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 872 页中的 “C.5.9 SMPP 中继选项” 。

C.5.5.3 SMPP 服务器

要配置 SMPP 服务器，请完成以下步骤：

▼ 配置 SMPP 服务器

1 **将 SMPP 服务器实例（选项组）添加至 SMS Gateway Server 的配置文件中。**

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 874 页中的 “C.5.10 SMPP 服务器选项” 。

C.5.6 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 867 页中的 “C.5.6.1 配置移动设备到电子邮件网关配置文件”
- 第 868 页中的 “C.5.6.2 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。

C.5.6.1 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至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：

▼ 配置网关配置文件

1 **将网关配置文件（选项组）添加至 SMS Gateway Server 配置文件中。**

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
```

任何不超过 11 个字符的名称均可用作配置文件的名称。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。

有关所有移动设备原始选项的完整说明，请参见第 876 页中的 “C.5.11 网关配置文件选项”。

C.5.6.2 配置移动设备到电子邮件 SMPP 服务器

添加 SMPP 服务器与添加电子邮件到移动设备 SMPP 服务器的过程相同（请参见第 866 页中的 “C.5.5.3 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。

C.5.7 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 868 页中的 “C.5.8 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 872 页中的 “C.5.9 SMPP 中继选项”
- 第 874 页中的 “C.5.10 SMPP 服务器选项”
- 第 876 页中的 “C.5.11 网关配置文件选项”

C.5.8 全局选项

SMS Gateway Server 目前有三类全局选项：

- 第 869 页中的 “C.5.8.1 线程调整选项”
- 第 870 页中的 “C.5.8.2 历史数据调整”
- 第 871 页中的 “C.5.8.3 其他”

必须在指定任何选项组之前，在配置文件顶部指定所有全局选项。表 C–20 列出了所有全局配置选项。

表 C–20 全局选项

选项	默认值	说明
第 871 页中的 “DEBUG”	6	选择已生成的诊断输出的类型
第 870 页中的 “HISTORY_FILE_DIRECTORY”		历史数据文件的绝对目录路径
第 870 页中的 “HISTORY_FILE_MODE”	0770	历史数据文件的权限
第 870 页中的 “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
第 871 页中的 “LISTEN_CONNECTION_MAX”	10,000	所有 SMPP 中继和服务器实例上并行入站连接的最大数目
第 870 页中的 “RECORD_LIFETIME”	3 天	历史数据归档文件中记录的有效期
第 869 页中的 “THREAD_COUNT_INITIAL”	10 个线程	工作人员线程的初始数目
第 869 页中的 “THREAD_COUNT_MAXIMUM”	50 个线程	工作人员线程的最大数目
第 869 页中的 “THREAD_STACK_SIZE”	64 Kb	各工作人员线程的堆栈大小

C.5.8.1 线程调整选项

各入站 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：第 869 页中的 “THREAD_COUNT_INITIAL”、第 869 页中的 “THREAD_COUNT_MAXIMUM”、第 869 页中的 “THREAD_STACK_SIZE”。

THREAD_COUNT_INITIAL

（**整数**，*> 0*）为工作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`）允许用于工作线程池的最大线程数量。默认值为 50 个线程。

THREAD_STACK_SIZE

（**整数**，*> 0*）工作线程池中每个工作线程的堆栈大小（字节）。默认值为 65,536 个字节 (64 Kb)。

C.5.8.2 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。每个历史文件只可于 HASH_FILE_ROLLOVER_PERIOD 指定的秒数内写入，超过此时间后，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 指定秒数的生存期，就会被从磁盘中删除。

以下选项用于调整历史文件：第 870 页中的 “HISTORY_FILE_DIRECTORY” 、第 870 页中的 “HISTORY_FILE_MODE” 、第 870 页中的 “HISTORY_FILE_ROLLOVER_PERIOD” 、第 870 页中的 “RECORD_LIFETIME” 。

HISTORY_FILE_DIRECTORY

（**字符串，绝对目录路径**）向其写入历史文件的目录的绝对路径。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/

使用的目录应位于一个速度适当的磁盘系统中，并且具有足够的可用空间用于预期存储；有关存储规划的信息，请参见第 883 页中的 “C.6 SMS Gateway Server 存储要求” 。鼓励各站点将此选项更改为一个更适当的值。

HISTORY_FILE_MODE

（**整数，八进制值**）与历史文件关联的文件权限。默认情况下，将使用值 0770（八进制）。

HISTORY_FILE_ROLLOVER_PERIOD

（**整数，秒**）每隔 HASH_FILE_ROLLOVER_PERIOD 指定的秒数，就会关闭当前历史文件，并且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*）历史记录的生存期（秒）。超过此有效期的记录将从内存中清除；超过此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）。保存在内存中的记录将由专用来管理内存中数据的线程彻底清除。这些清除操作每隔 HASH_FILE_ROLLOVER_PERIOD 指定的秒数执行一次。磁盘上的文件在必须打开新的历史记录时被清除。

C.5.8.3 其他

下面是其他选项：

DEBUG

（**整数**，**位掩码**）启用调试输出。默认值为 6，即选择警告消息和错误消息。

表 C–21 定义了 DEBUG 位掩码的位值。

表 C–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，正文数据
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。

LISTEN_CONNECTION_MAX

（**整数**，*>= 0*）所有 SMPP 中继和服务器实例上允许的并行入站 TCP 连接的最大数量。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。默认值：10,000

LOG_PAGE_COUNT

(0, 1, 2) 只有在使用 `logging` 通道关键字启用通道的日志记录时，`LOG_PAGE_CONT` SMS 通道选项才能生效。启用日志记录之后，此选项将控制 `mail.log` 文件的邮件大小字段中记录的值。该字段通常给出了基础邮件文件的块大小。当 `LOG_PAGE_COUNT` 为非零值时，日志文件中的邮件大小字段将改为记录传送的页数。

0 - 记录基础邮件文件的块大小。当未指定 `LOG_PAGE_COUNT` 时，此为默认行为。

1 - 当整个邮件成功地传送给收件人时，记录发送的页数。否则，即使有某些页发送给了收件人，记录的页数也为 0。

2 - 记录发送给收件人的页数，不管是否发送了整个邮件。

只有在邮件足够大而需要分为几页传送时，`LOG_PAGE_COUNT=1` 和 `LOG_PAGE_COUNT=2` 之间才会有差别。在这种情况下，传送所有的页之前可能会发生错误。例如，MTA 和远程 SMPP 服务器之间的网络中断。在这种情况下，将在以后尝试重新传送邮件。每次尝试时，先前已发送的页都会随没有发送的页再次发送。站点可以选择是否需要记录在这些失败的传送尝试期间成功发送的页数。

C.5.9 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 C–22 列出了 SMPP 中继的配置选项。

表 C–22 SMPP 中继选项

选项	默认值	说明
第 873 页中的 “C.5.9.1 LISTEN_BACKLOG”	255	入站 SMPP 客户端连接的连接待办事项
第 873 页中的 “LISTEN_CONNECTION_MAX”		并行入站连接的最大数目

表 C–22 SMPP 中继选项 （续）

选项	默认值	说明
第 873 页中的 “LISTEN_INTERFACE_ADDRESS”		入站 SMPP 客户端连接的网络接口
第 873 页中的 “LISTEN_PORT”		入站 SMPP 客户端连接的 TCP 端口
第 873 页中的 “LISTEN_RECEIVE_TIMEOUT”	600 s	读取 SMPP 客户端的入站连接超时
第 874 页中的 “LISTEN_TRANSMIT_TIMEOUT”	120 s	写入 SMPP 客户端的入站连接超时
第 874 页中的 “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
第 874 页中的 “SERVER_HOST”		要中继到的 SMPP 服务器的主机名或 IP 地址
第 874 页中的 “SERVER_PORT”		要中继到的 SMPP 服务器的 TCP 端口
第 874 页中的 “SERVER_RECEIVE_TIMEOUT”	600 s	读取出站 SMPP 服务器连接超时
第 874 页中的 “SERVER_TRANSMIT_TIMEOUT”	120 s	写入出站 SMPP 服务器连接超时

C.5.9.1 LISTEN_BACKLOG

（**整数，范围在** `[0,255]` **之间**）入站 SMPP 客户端连接的 TCP 堆栈所允许的积压连接请求。默认值为 255。

LISTEN_CONNECTION_MAX

（**整数，**>= *0*）允许用于此 SMPP 中继实例的并行入站 TCP 连接的最大数量。请注意，如果该值超过全局 `LISTEN_CONNECTION_MAX` 设置，则会被忽略。

LISTEN_INTERFACE_ADDRESS

（**字符串，**`"INADDR_ANY"` **或点分十进制** *IP* **地址**）侦听入站 SMPP 客户端连接的网络接口的 IP 地址。可以是字符串 `"INADDR_ANY"`（所有可用的接口）或是点分十进制形式的 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**）为接受入站 SMPP 客户端连接而绑定的 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 客户端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*）将数据发送至 SMPP 客户端时所允许的超时。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 客户端通信中继至的 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**）要中继至的远程 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*）将数据发送至 SMPP 服务器时所允许的超时。默认值为 120 秒（2 分钟）。

C.5.10 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 C–23 列出了 SMPP 服务器的配置选项。

表 C–23 SMPP 服务器选项

选项	默认值	说明
第 875 页中的 “C.5.10.1 LISTEN_BACKLOG”	255	入站 SMPP 服务器连接的连接待办事项
第 875 页中的 “LISTEN_CONNECTION_MAX”		并行入站连接的最大数目
第 875 页中的 “LISTEN_INTERFACE_ADDRESS”		入站 SMPP 服务器连接的网络接口
第 875 页中的 “LISTEN_PORT”		入站 SMPP 服务器连接的 TCP 端口
第 876 页中的 “LISTEN_RECEIVE_TIMEOUT”	600 s	入站 SMPP 服务器连接的读取超时
第 876 页中的 “LISTEN_TRANSMIT_TIMEOUT”	120 s	入站 SMPP 服务器连接的写入超时

C.5.10.1 LISTEN_BACKLOG

（**整数，范围在** *[0,255]* **之间**）入站 SMPP 客户端连接的 TCP 堆栈所允许的积压连接请求。默认值为 255。

LISTEN_CONNECTION_MAX

（**整数** >= *0*）允许用于此 SMPP 服务器实例的并行入站 TCP 连接的最大数目。请注意，如果该值超过全局 `LISTEN_CONNECTION_MAX` 设置，则会被忽略。

LISTEN_INTERFACE_ADDRESS

（**字符串，**`"INADDR_ANY"` **或点分十进制** *IP* **地址**）侦听入站 SMPP 客户端连接是否启用的网络接口的 IP 地址。可以是字符串 `"INADDR_ANY"`（所有可用的接口）或是点分十进制形式的 IP 地址。（例如 193.168.100.1。）默认值为 `"INADDR_ANY"`。

LISTEN_PORT

（**整数，***TCP* **端口号**）为接受入站 SMPP 客户端连接而绑定的 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 客户端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*）将数据发送至 SMPP 客户端时所允许的超时。默认值为 120 秒（2 分钟）。

C.5.11 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在选项组中进行声明，格式如下：

```
[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` 仅用于将该配置文件与其他原始配置文件区分开。

表 C–24 列出了 SMS Gateway Server 配置文件选项。

表 C–24 SMS Gateway Server 配置文件选项

选项	默认值	说明
第 877 页中的 “C.5.11.1 CHANNEL”	`sms`	用于对消息进行排入的通道
第 877 页中的 “EMAIL_BODY_CHARSET”	`US-ASCII`	电子邮件消息正文字符集
第 877 页中的 “EMAIL_HEADER_CHARSET”	`US-ASCII`	电子邮件消息标题字符集
第 877 页中的 “FROM_DOMAIN”		用于将电子邮件路由回 SMS 的域名
第 877 页中的 “PARSE_RE_0, PARSE_RE_1, ..., PARSE_RE_9”		用于解析 SMS 消息文本的正则表达式
第 879 页中的 “PROFILE”	`GSM`	在以下系统中运行的 SMS 配置文件：GSM、TDMA 或 CDMA
第 879 页中的 “SELECT_RE”		用于选择插件的正则表达式

表 C–24 SMS Gateway Server 配置文件选项 （续）

选项	默认值	说明
第 879 页中的 “SMSC_DEFAULT_CHARSET”	US-ASCII	SMSC 的默认字符集
第 879 页中的 “USE_SMS_PRIORITY”	0	Gateway SMS 的电子邮件优先级标志
第 880 页中的 “USE_SMS_PRIVACY”	0	Gateway SMS 的电子邮件保密性指示符

C.5.11.1 CHANNEL

（**字符串**，*1* **至** *40* **个字符**）用于将电子邮件消息加入队列的 MTA 通道的名称。如果未指定，则假定为 "sms"。指定的通道必须在 MTA 的配置中定义。

EMAIL_BODY_CHARSET

（**字符串**，**字符集名称**）用于在 SMS 文本插入到电子邮件消息的正文之前转换 SMS 文本的字符集。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**）用于在 SMS 文本插入到 RFC 822 `Subject:` 标题行之前转换 SMS 文本的字符集。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**）构建电子邮件消息的信封 `From:` 地址时，要附加至 SMS 源地址的域名。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，则将使用通过 `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**）对于移动设备始发的电子邮件，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 选项互斥。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。它们可以选择性地输出在 Subject: 标题行中用作字符串 1 的文本，以及在消息正文中用作字符串 2 的文本。任何未被正则表达式“消耗的”文本还可在消息正文中使用，其后跟的任何文本输出用作字符串 2 。

正则表达式的尝试顺序为 PARSE_RE_0、PARSE_RE_1、...，直至 PARSE_RE_9。如果没有指定任何正则表达式，则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。

```
(?:\(([^\)]*)\))?
```

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 ?: 可使外围括号不报告字符串。它们仅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 分量仅匹配零或一次，等效于表达式 {0,1}。

```
[ \t]*
```

忽略空格字符。

```
(.*)
```

消息正文的其余文本。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，转换的文本将使用先前从 UTF-8 转换为 UTF-16 的正则表达式进行评估。之后，评估结果将转换为针对目标电子邮件地址的 US-ASCII、针对 `Subject:` 文本的 `EMAIL_HEADER_CHARSET`（如果有）以及针对邮件正文的 `EMAIL_BODY_CHARSET`（如果有）。

PROFILE

（**字符串**，*"GSM"*、*"TDMA"* **或** *"CDMA"*）假定的 SMS 配置文件。目前此信息只用于将 SMS 优先级标志映射至 RFC 822 `Priority:` 标题行。因此，当 `USE_SMS_PRIORITY=0`（该选项的默认设置）时，此选项不生效。

SELECT_RE

（**字符串**，*US-ASCII* **正则表达式**）用于与每条 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，则此 SMS 消息将通过网关发送至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，因此此正则表达式也必须以 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（使用 `USE_SMS_PRIORITY=0`），SMS 消息中的优先级标志将被忽略，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`。表 C–25 显示了与电子邮件一起传送时，从 SMS 至电子邮件的映射：

表 C–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（无优先级）	无标题行（表示 Normal）
	1, 2, 3（优先级）	Urgent
TDMA	0（批量）	Nonurgent
	1（普通）	无标题行（表示 Normal）
	2（紧急）	Urgent
	3（非常紧急）	Urgent
CDMA	0（普通）	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: 标题行的值为 Nonurgent、Normal 和 Urgent。

USE_SMS_PRIVACY

（**整数，*0* 或 *1***）默认情况下（使用 USE_SMS_PRIVACY=0），SMS 保密性指标将被忽略，且不与电子邮件消息一起发送。要将此信息与电子邮件一起传送，请指定 USE_SMS_PRIVACY=1。表 C–26 显示了与电子邮件一起传送时，从 SMS 至电子邮件的映射：

表 C–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（限制）	Personal
2（机密）	Private
3（秘密）	Company-confidential

请注意，电子邮件 Sensitivity: 标题行的值为 Personal、Private 和 Company-confidential。

C.5.12 双向 SMS 配置示例

行为假设

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`

  并给定唯一的 SMS 源地址，范围为 `000`nnnnnnnnnn。
- 定址至 SMS 地址 `000` 的移动设备 SMS 消息将通过网关发送至电子邮件（带有从 SMS 消息文本开始处提取的电子邮件地址）。

  例如，如果 SMS 消息文本为：

  `jdoe@domain.com Interested in a movie?`

  则消息 "Interested in a movie?" 将被发送至 jdoe@domain.com。
- 发送至 `000`nnnnnnnnnn 的 SMS 通知将通过网关发送至电子邮件，并定向至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 的默认字符集为 UCS2（也可为 UTF-16）。

SMS 通道配置

要使上述行为生效，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）：

```
(blank line)
sms
sms.domain.com
```

SMS 通道选项文件

然后，通道的选项文件 `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` 应包含类似以下内容：

```
HISTORY_FILE_DIRECTORY=/sms_gateway_cache/
[SMPP_RELAY=relay1]
LISTEN_PORT=503SERVER_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。

C.5.12.1 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（针对回送测试）为 FROM_FORMAT、SUBJECT_FORMAT 和 CONTENT_PREFIX 选项指定空字符串。

执行回送测试

发送定址至 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。

C.6 SMS Gateway Server 存储要求

要确定您将用于 SMS Gateway Server 的资源数量，请使用从表 C–27 中的要求所生成的数字，以及预期每秒中继消息的数量和 RECORD_LIFETIME 设置。

表 C–27 包含历史记录、SMPP 中继和 SMPP 服务器的要求。

表 C–27 SMS Gateway Server 存储要求

组件	要求
内存中历史记录	每条中继的消息都需要 33+m+s 个字节的虚拟内存，其中 m 为此消息的 SMS 消息 ID 的长度 (1 <= m <= 64)，s 为此消息的 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。

表 C–27 SMS Gateway Server 存储要求 （续）

组件	要求
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 为 SMS 消息 ID 的平均长度，且 1<=m<=64 ■ s 为 SMS 源地址的平均长度，且 1 <= s <= 20 ■ a 为电子邮件地址的平均长度，且 3 <= a <= 129 ■ S 为 Subject: 标题行的的平均长度，且 0 <= S <= 80 ■ i 为电子邮件消息信封 ID 的平均长度，且 0 <= i <= 129 任何特定记录的大小都受到消息的信封 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。
SMPP 中继	每条已中继的 SMPP 会话将消耗两个 TCP 插槽：一个与本地 SMPP 客户端连接，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，如果预期每秒平均中继 50 条消息，SMS 源地址为 13 个字节长，SMS 消息 ID 为典型长度 12 个字节，电子邮件地址为 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。要减少所需的虚拟内存量或磁盘存储空间，请使用 RECORD_LIFETIME 选项，减少记录的保留时间长度。

◆ ◆ ◆ 附 录 D

安装工作单

本附录提供了用于规划安装的工作单。将介绍以下工作单：

D.1 Directory Server 安装

通过 Java Enterprise System 安装程序或以前的安装，您已经安装了 Directory Server。请将您的 Directory Server 安装和配置参数记录到表 D–1 中（该表是 Communications Suite Deployment Planning Guide 中显示的工作单的副本）。安装和配置 Administration Server 和 Messaging Server 时将需要这些参数。

表 D–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 48 页中的 “1.2 为 Messaging Server 配置准备 Directory Server”	
主机	此主机名为 IP 主机名，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 48 页中的 “1.2 为 Messaging Server 配置准备 Directory Server”	

表 D–1 Directory Server 安装参数 （续）

参数：	说明：	示例：	用于：	您的答案：
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 48 页中的“1.2 为 Messaging Server 配置准备 Directory Server”和第 49 页中的“1.3 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 48 页中的“1.2 为 Messaging Server 配置准备 Directory Server”	
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 48 页中的“1.2 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 48 页中的“1.2 为 Messaging Server 配置准备 Directory Server”和第 49 页中的“1.3 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 48 页中的“1.2 为 Messaging Server 配置准备 Directory Server”	

D.2 Directory Server 安装程序脚本 (comm_dssetup.pl)

运行 Directory Server 安装程序脚本 (`comm_dssetup.pl`) 为 Messaging Server 配置准备 Directory Server 时，请将安装参数记录在表 D–2 中。您需要将其中的某些参数用于 Messaging Server 初始运行时配置。

表 D–2 `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项）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	

D.3 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 D–3 中。您还可以参阅第 885 页中的 “D.1 Directory Server 安装”核对表以回答某些问题。

表 D–3 初始运行时配置参数

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/mps/SUNmsgsr/	
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 初始运行时配置中指定的用户相同。	mailsrv	
UNIX 系统组	特定 UNIX 系统用户所属的组。此系统组与您在 Administration Server 初始运行时配置中指定的组应不相同。	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	
默认电子邮件域	未指定域时使用的默认电子邮件	siroe.com	

表 D–3 初始运行时配置参数 （续）

参数	说明	示例	您的答案：
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

词汇表

有关本文档集中所使用的术语的完整列表，请参阅《Sun Java Enterprise System Glossary》。

索引

B

C

D

E

F

G

H

J

K

L

M

N

O

S

T

U

V

W

同

外

网

维

伪

委

硬

用

邮

作