管理员指南

iPlanet™ Messaging Server

5.2 版

2002 年 2 月

目录

列表清单

插图清单

关于本指南

本手册说明如何管理和配置 iPlanet Messaging Server。iPlanet Messaging Server 为使用开放式互联网标准的企业和各种规模的邮件主机在电子邮件方面的需求提供了功能强大而灵活的跨平台解决方案。

本章包含以下主题：

- 本手册的使用者
- 使用者需具备的基本知识
- 本手册的章节
- 印刷体约定
- 何处查找相关信息

本手册的使用者

如果您是您所在网站负责管理和配置 iPlanet Messaging Server 的人，则应阅读本手册。

使用者需具备的基本知识

本指南假定您对下列各部分有全面的了解：

- 互联网和万维网
- iPlanet Administration Server
- Netscape Directory Server 和 LDAP
- 电子邮件及电子邮件的基本原理
- Netscape Console

本手册的章节

本手册包含以下章节和附录：

- 关于本指南 （本章）
- 第 1 篇，“绪论”

  本章提供 iPlanet Messaging Server 的高层次综述。
- 第 2 篇，“配置一般邮件功能”

  本章说明 Messaging Server 的一般性任务，例如启动和停止服务，配置目录访问等。
- 第 3 篇，“配置 POP、 IMAP 和 HTTP 服务”

  本章介绍如何通过 iPlanet Console 或命令行实用程序来配置服务器以使其支持一项或多项服务。
- 第 4 篇，“配置和管理 Multiplexor 服务”

  本章提供有关 iPlanet Messaging Multiplexor（邮件多路复用器）以及 iPlanet Messenger Express Multiplexor 的使用方法，这两种多路复用器都是专用的邮件服务器，可用作多个邮件服务器的单点连接。
- 第 5 篇，“MTA 概念”

  本章说明 MTA 的一些基本原理。
- 第 6 篇，“关于 MTA 服务与配置”

  本章提供有关为您的服务器配置 MTA 服务的一般信息。
- 第 7 篇，“配置重写规则”

  本章说明如何配置 MTA 配置文件 `imta.cnf` 中的重写规则 （地址重写）。
- 第 8 篇，“配置通道定义”

  本章说明如何配置 MTA 配置文件 `imta.cnf` 中的通道定义。
- 第 9 篇，“使用预定义通道”

  本章说明如何使用预定义的 MTA 通道定义，如保存通道和转换通道。
- 第 10 篇，“邮件过滤与访问控制”

  本章说明如何控制对邮件服务器的访问以及如何使用映射表和服务器端规则（SSR）过滤邮件。
- 第 11 篇，“邮件存储库的管理”

  本章说明邮件存储目录体系，如何配置邮件存储分区、设置空间配额和过期策略等等。
- 第 12 篇，“配置安全和访问控制”

  本章说明 iPlanet Messaging Server 所具有的安全和访问控制功能。

- 第 13 篇，“日志记录和日志分析”

  本章说明如何查看和配置 MTA、邮件存储和邮件访问服务的服务日志。

- 第 14 篇，“MTA 故障诊断”

  本章说明在排除 “邮件传送代理”（MTA）程序故障时应使用的一些通用工具、方法及排障作业程序。

- 第 15 篇，“监控 iPlanet Messaging Server”

  本章说明与 iPlanet Messaging Server 的监控有关的事项。

- 附录 A，“SNMP 支持”

  本附录说明如何启用 SNMP 对 Messaging Server 的支持。同时以一览表之方式列出了 SNMP 提供的信息种类。

- 附录 B，“MTA 直接 LDAP 操作”

  本附录说明 MTA 的直接 LDAP 之运作方法。

- 附录 C，“在 iPlanet Messaging Server 中管理 Event Notification Service”

  该附录说明在 iPlanet Messaging Server 中启用和管理 iPlanet Event Notification Service 时，管理员需做事情。

- 附录 D，“管理邮件用户和邮件发送列表”

  本章说明如何使用 Console 界面创建并管理用户邮件帐户和邮件发送列表。

- 词汇表

  词汇表提供了本指南所用词汇和命名约定的定义。

印刷体约定

表 1　　印刷体约定

字体或符号	意义	范例
`AaBbCc123`	命令、文件、代码、目录、主机名、判别名、计算机屏幕输出之名称。	编辑您的 `msg.conf` 文件。 用 `ls -a` 列示所有文件。 错误：非法端口 #
`AaBbCc123`	用户输入的文字。	`%` **`cd madonna`**
the_variable	命令行占位符或变量。用实际名称或值替换。	`#` *Instance_Root*`/start-msg`
AaBbCc123	书名、新词或术语，或强调词。	**iPlanet Messaging Server Provisioning Guide**

命令行提示符

命令行提示符（例如：C-Shell 使用的 % 或 Korn shell 使用的 $）通常不在例子中予以显示。不同的操作系统使用不同的提示符。不论提示符如何，命令都须按文档显示的样子输入。

何处查找相关信息

iPlanet Messaging Server 提供有下列补充信息：

http://docs.iplanet.com/docs/manuals/messaging.html

下面列出了一些可提供的附加文档：

- **iPlanet Messaging Server 管理员指南**
- **iPlanet Messaging Server Installation Guide**
- **iPlanet Messaging Server Reference Manual**
- **iPlanet Messaging Server Schema Reference Manual**
- **iPlanet Messaging Server Provisioning Guide**
- **iPlanet Delegated Administrator for Messaging and Collaboration Installation and Administration Guide**

第 1 篇

绪论

iPlanet Messaging Server 是一个功能强大的、为满足企业和服务供应商大容量、高可靠性邮件处理需要而设计的基于因特网标准的邮件服务器。服务器由几个模块构成，模块为可以独立配置的组件，提供对几个基础性的标准电子邮件协议的支持。

Messaging Server 使用集中式的 LDAP 数据库存储有关用户、组和域的相关信息。某些有关服务器的配置信息也存储在 LDAP 数据库中，另一些则存储在一组配置文件中。

产品套件 Messaging Server 提供支持用户设备配置和服务器配置的工具。

本章包括以下各节：

- 对标准协议的支持
- 对托管域的支持
- 对用户设备配置的支持
- 对一体化通信的支持
- 对 Webmail 的支持
- 强有力的安全性和访问控制
- 易于操作的用户界面
- 安装后的目录和文件结构

对标准协议的支持

iPlanet Messaging Server 支持大部分与电子通信有关的国家、国际和工业标准。有关详细列表，请参见 **iPlanet Messaging Server Reference Manual** 附录 A。

对托管域的支持

Messaging Server 对托管域提供全面支持，托管是 ISP 通过委外方式提供的电子邮件域。即由 ISP 以运行和管理某组织机构的电子邮件服务之形式为其提供电子邮件域托管服务。一个托管域与其他的托管域共享同一部 Messaging Server 主机。在早期的 LDAP 式电子邮件系统中，域通常由一个或多个电子邮件服务器主机支持。在 Messaging Server 中，多个域则以托管形式使用单一的服务器。每一个托管域都有一 LDAP 条目，指向该域的用户和组容器，并提供各种与域有关的默认设置。

对用户设备配置的支持

Messaging Server 使用集中式的 LDAP 数据库存储有关用户、组和域的相关信息。 iPlanet Delegated Administrator for Messaging 以图形用户界面 Console 和一套命令行实用程序来管理组织机构的用户、组和域。

有关用户、组和域管理方面的详细信息，请参阅下列文件：

- **iPlanet Messaging Server Provisioning Guide** - 说明如何用 LDAP 创建域、用户、组、或管理员条目。
- **iPlanet Messaging Server Schema Reference Manual** - 说明 iPlanet Messaging Server 的模式。
- **iPlanet Messaging Server Reference Manual** - 说明 Delegated Administrator 在管理用户、组和域时使用的命令行工具。
- iPlanet Messaging Server Delegated Administrator Console 在线帮助。

备注	您也可通过 Console 界面创建用户和组，但建议您不要这样做，因为这样会使您无法用 Delegated Administrator 查看或修改这些条目。

对一体化通信的支持

iPlanet Messaging Server 可为全面的一体化通信解决方案提供平台基础；所谓一体化通信，既电子邮件、话音邮件、传真和其他形式的通信功能都使用一个单一邮件存储系统的概念。

对 Webmail 的支持

iPlanet Messaging Server 提供的 Messenger Express 是一个支持 web 功能的电子邮件程序，能够使最终用户通过与 Internet 相连的 HTTP 计算机系统中的浏览器访问他们自己的邮箱。Messenger Express 客户程序可向专用的 web 服务器发送邮件，该 web 服务器是 iPlanet Messaging Server 的组成部分。 HTTP 服务然后将邮件发送到本地 MTA 或远程 MTA，以便进行路由选择或传递。

强有力的安全性和访问控制

iPlanet Messaging Server 具有以下安全和访问控制功能：

- 支持口令登录 （POP、 IMAP、 HTTP 或 SMTP）和基于证书的登录。
- 支持的标准安全协议：传输层安全性 （TLS）、安全套接层 （SSL）和简单认证和安全层（SASL）
- 通过访问控制指令 （ACI）实现的授权管理 （Delegated administration）。
- POP、 IMAP 和 HTTP 的客户端访问过滤器。
- 使用系统级以及用户级和服务器端规则过滤未外界滥发的大批量电子邮件。

易于操作的用户界面

Messaging Server 包含几个模块，模块为可独立配置的组件，支持各种电子邮件传输和访问协议。

Messaging Server 提供一组完整的存储在本地服务器中的配置文件和一组命令行工具，供用户配置 MTA （邮件传送代理）。 Messaging Server 提供了图形用户界面 Console 和一组完整的命令行工具供用户配置邮件存储和邮件访问服务。

有关 MTA 配置和 MTA 存取配置方面的信息，请参阅本手册的以下章节：

- 第 5 篇，“MTA 概念”
- 第 6 篇，“关于 MTA 服务与配置”
- 第 7 篇，“配置重写规则”
- 第 8 篇，“配置通道定义”
- 第 9 篇，“使用预定义通道”
- 第 10 篇，“邮件过滤与访问控制”
- 第 12 篇，“配置安全和访问控制”
- 第 14 篇，“MTA 故障诊断”
- 第 15 篇，“监控 iPlanet Messaging Server”

还可参阅 **iPlanet Messaging Server Reference Manual**。

有关邮件存储和访问存储方面的配置信息，请参阅本手册的以下章节：

- 第 3 篇，“配置 POP、 IMAP 和 HTTP 服务”
- 第 11 篇，“邮件存储库的管理”
- 第 12 篇，“配置安全和访问控制”

还可参阅 **iPlanet Messaging Server Reference Manual**。

此外，也可参阅本手册的以下章节：

- 第 2 篇，“配置一般邮件功能”说明了 Messaging Server 的一般性任务，例如启动和停止服务，配置目录访问等。
- 第 4 篇，“配置和管理 Multiplexor 服务”说明了 iPlanet Messaging Multiplexor（MMP）的使用方法， Messaging Multiplexor 是一种专用邮件服务器，可充当多个邮件服务器的单点连接。

安装后的目录和文件结构

当安装 iPlanet Messaging Server 之后，其目录和文件将以表 1-1 中描述的结构排列。该表并非十分详尽，只显示典型服务器管理最常用任务的目录和文件。

表 1-1　安装后的目录和文件

目录	默认位置和说明
服务器根目录（*server_root*）	`/usr/iplanet/server5/` （默认位置）
	给定服务器组的所有服务器（即由给定 Administration Server 管理的所有服务器）都安装在该目录中。其中可能包含除 Messaging Server 之外的其他 iPlanet 服务器。
	该目录中还包含有可用来启动和停止管理服务的二进制可执行文件（`start-admin`、`stop-admin`）以及启动 Console 所需的二进制可执行文件（`startconsole`）。
实例目录（*instance_root* 或 *instance_directory*）	*server_root*/msg-*instance_name*/ （必须的位置）
	instance_name 是安装时指定的 Messaging Server 实例的名称。（默认值 = 服务器的主机名）
	该目录包含的配置文件是用来定义特定 Messaging Server 实例的配置文件。所有使用相同二进制文件的 Messaging Server 的多个实例可以存在于同一指定主机上。
	该目录还包含已安装的 Messaging Server 的一些二进制可执行文件，如 `configutil`、`start-msg` 和 `stop-msg` 等。
安装目录（*installDirectory*）	*server_root*`/bin/msg/` （必须的位置）
	该目录包含安装的 Messaging Server 一些二进制可执行文件。
配置文件目录 `config`	*instance_root*/config/ （必须的位置）
	包含一般性配置文件，如 `local.conf`、`msg.conf`、`sslpassword.conf`。
	`msg.conf` 文件中的值在安装时设定。Messaging Server 使用该文件获取启动时所需要的信息，如 LDAP 主机名和端口号。

表 1-1　安装后的目录和文件（接上页）

目录	默认位置和说明
MTA 目录 `imta`	*instance_root*/imta/ （必须的位置） 包含与 MTA 配置相关的几个目录：`bin`、`config`、`db`、`dl`、`programs`、`queue`、`tmp`。
MTA 配置目录 `config`	*instance_root*/imta/config/ （必须的位置） 包含 MTA 配置文件，如 `imta.cnf`、`dispatcher.cnf`、`job_controller.cnf`、`aliases`、`imta_tailor` 等。
MTA 队列目录 `queue`	*instance_root*/imta/queue/ （必须的位置） 包含若干邮件队列子目录。每个队列通道都在此目录中有一个子目录；例如：`ims-ms`、`tcp_intranet`、`tcp_local`、`autoreply`。
MTA 程序目录 程序	*instance_root*/`imta/programs/` （必须的位置） 包含用于处理用户邮件的网站提供之可执行程序（如果有的话）。
MTA 数据库目录 `db`	*instance_root*/`imta/db/` （必须的位置） 包含 MTA 使用的数据库：`aliasesdb.db`、`domaindb.db`、`profiledb.db`、`reversedb.db`、`ssrdb.db` 等。
邮件存储库目录 `store`	*instance_root*/store （必须的位置） 包含与邮件存储处理相关的目录：`mboxlist`、`partition`、`user`。 有关详细信息，请参阅第 265 页“邮件存储库目录布局”。
手册目录 `manual`	*server_root*/`manual` （必须的位置） 包含与服务器一起安装的文档。 `manual/en/admin/` 包含 Administration Server 文档。 `manual/en/msg/` 包含 Messaging Server 文档。 `manual/en/slapd/` 包含 Directory Server 文档。

第 2 篇

配置一般邮件功能

本章说明执行 Messaging Server 一般性任务的方法，例如怎样通过 Netscape Console（以下简称 Console）或命令行实用程序启动或停止服务以及配置目录访问等。此后的章节将分别说明各种 Messaging Server 服务 - 例如 POP、 IMAP、 HTTP 和 SMTP - 所特有的任务。本章包括以下各节：

- 管理邮件用户和邮件发送列表
- 查看基本服务器信息
- 启动和停止服务
- 配置自动回复邮件的语言
- 配置自动回复邮件的语言
- 启用单次登录 （SSO）
- 定制目录查找
- 加密设置

备注	最终用户帐户信息和特定域信息主要通过 iPlanet Delegated Administrator for Messaging 界面进行管理。有关详情，请参见 **iPlanet Delegated Administrator for Messaging and Collaboration Installation and Administration Guide** 以及伴随 Delegated Administrator 的联机帮助。

管理邮件用户和邮件发送列表

所有用户信息和邮件发送列表信息均作为条目保存在 LDAP 目录中。LDAP 用户目录能包含大量与组织机构相关的信息，如员工、成员、客户以及以这种或那种方式 “从属”于该组织的其他类型个体。这些个体构成了该组织的*用户*。

在 LDAP 目录中，每个用户条目由一系列的属性值来标识，用户信息的这种组织方式提高了搜索的效率。和用户相关的目录属性包括用户名称和其他标识信息，部门归属，工作分类，所处地理位置，管理者的姓名，直接报告者的姓名，对组织不同部分的访问权限，以及各种类型的首选项设置。

在使用电子邮件服务的组织中，差不多每个用户都有邮件帐户。在 iPlanet Messaging Server 系统中，邮件帐户信息不是就地存储在服务器中的，而是 LDAP 用户目录的一部分。每个邮件帐户的信息以邮件属性的形式附加于目录中的用户条目。

创建和管理邮件用户以及邮件发送列表等任务，涉及到在目录中创建和修改用户和邮件发送列表条目。这需要使用 iPlanet Delegated Administrator for Messaging、Delegated Administrator 命令行实用程序，或者直接修改 LDAP 目录。用户和邮件发送列表条目也可以通过 Console 创建，但建议不要这样做。（参阅附录 D。）

iPlanet Delegated Administrator for Messaging 完全支持对用户，组，家庭群组和托管域的管理。您可通过 Delegated Administrator 以代理的方式对用户和组进行管理，并为每个托管域建立管理员。 Delegated Administrator 为管理员管理用户和组，为最终用户管理各自邮件帐户提供了一个 GUI 界面。管理员也可以使用 Delegated Administrator 命令行实用程序来管理用户和组 （请参见 **iPlanet Messaging Server Reference Manual**）。有关 Delegated Administrator 在使用方面的详细信息，请参见 **iPlanet Delegated Administrator for Messaging and Collaboration Installation and Administration Guide** 以及 Delegated Administrator 联机帮助。有关使用 LDAP 工具管理用户、组和域的详细说明，请参见 **iPlanet Messaging Server Provisioning Guide**。

查看基本服务器信息

通过查看 Console 中的相关信息表，可以了解与已安装的 Messaging Server 有关的一些基本信息。

备注	如果安装 iPlanet Directory Server 5.1，必须通过 iPlanet Console 5.0 （随 Directory Server 5.1 一起安装）进行管理。 iPlanet Messaging Server 5.2 必须通过 Netscape Console 4.2（随 Messaging Server 5.2 一起安装）进行管理。

显示信息表：

1. 若需查看 Messaging Server 的信息，可在 Console 中将其打开。
2. 在左面板中选择服务器的图标。
3. 单击左面板中的 “配置”选项卡。
4. 如果 “信息”选项卡不在最前面，则在右面板中单击之。

   “信息”表随即出现。此表可显示服务器名称、服务器根目录、安装目录以及实例目录。

启动和停止服务

根据服务是否安装于 HA 环境中，服务的启动和停止是不同的。

在 HA 环境中启动和停止服务

当 Messaging Server 在 HA 控制下运行时，不能使用一般的 Messaging Server 启动、重启动和停止命令来控制各个 Messaging Server 服务。如果使用了这样的命令，就会使 HA 控制认为一个或多个服务已经意外停止，此刻需要尝试重启动所有的 Messaging Server 或全部废弃而转到另一个群集结点。

适当的启动、停止和重启动命令显示在下面的表格中。注意：没有启动、重启动或者停止一个单一的 Messaging Server 服务（如 SMTP）的 Sun Cluster 命令。Sun Cluster 的最小处理单位为一个人资源。由于 Messaging Server 在 Sun Cluster 中被认为是一种资源，因此 `scswitch` 命令是将所有的 Messaging Server 服务作为一个整体而发挥效用的。

表 2-1　在 Sun Cluster 3.0 环境中启动、停止、重启动

操作	个人资源	全部资源组
启动	`scswitch -e -j` *资源*	`scswitch -Z -g` *资源组*
重启动	`scswitch -n -j` *资源* `scswitch -e -j` *资源*	`scswitch -R -g` *资源组*
停止	`scswitch -n -j` *资源*	`scswitch -F -g` *资源组*

表 2-2　在 Sun Cluster 2.2 环境中启动、停止、重启动

操作	个人数据服务	全部已注册的数据服务
启动	hareg -y *数据服务*	hareg -Y
重启动	hareg -n *数据服务* hareg -y *数据服务*	hareg -N hareg -Y
停止	hareg -n *数据服务*	hareg -N

表 2-3　在 Veritas 1.1 环境中启动、停止、重启动

操作	个人资源	整个资源组
启动	hares -online *资源* -sys *系统*	hagrp -online *组* -sys *系统*
重启动	hares -online *资源* -sys *系统* hares -online *资源* -sys *系统*	hagrp -online *组* -sys *系统* hagrp -online *组* -sys *系统*
停止	hares -online *资源* -sys *系统*	hagrp -online *组* -sys *系统*

在非 HA 环境中启动和停止服务

可以通过 Console 或命令行启动或停止服务。

只需运行服务器实际使用的服务。例如，若需临时性地把 Messaging Server 的一个特定实例单独地用作邮件传送代理 （MTA），则可以只启动 MTA。若出于维护、修理或安全方面的原因需要关闭服务器，可以只关闭受影响的服务。（如果从不准备运行某个特定的服务，则应禁用之而不仅仅是将其关闭。）

备注	必须首先启用 POP、IMAP 和 HTTP 服务，然后才能进行启动或停止操作。有关详细信息，请参阅第 46 页 “启用和关闭服务”。

重要提示：如果服务器的某一进程出现崩溃，其它进程将挂起以等待崩溃的服务器进程的封锁。因此，如果任何服务器进程出现崩溃，应停止所有进程，然后重启所有进程。这包括 POP、IMAP、HTTP 和 MTA 进程，还有 `stored`（邮件存储）进程，以及任何用于修改邮件存储的实用程序，如 `mboxutil`、`deliver`、`reconstruct`、`readership` 和 `upgrade`。

Console 控制台提供的表格可用来启动和停止个别服务并查看与每项服务相关的状态信息。

对于每一种服务 - IMAP、POP、SMTP 和 HTTP - 表格都显示了服务的当前状态（开启或关闭）。如果服务正在运行，表格会显示上次启动的时间以及其它状态信息

启动、关闭或查看邮件服务状态：

1. 若需启动或停止 Messaging Server 的服务，可从 Console 将其打开。
2. 然后以下列两种方式转至 “一般服务配置”表：
   a. 单击 “任务”选项卡，然后单击 “启动 / 停止服务”。
   b. 单击 “配置”选项卡并选择左面板中的 Services 文件夹。然后单击右面板中的 “一般”选项卡。
3. “一般服务配置”表格随即出现。

   “进程控制”字段下的左列给出了服务器所支持的服务项，右列给出了每项服务的基本状态 （开或关；如果是开，则显示上次启动的时间）。
4. 若需查看当前运行服务项的状态信息，可选择 “进程控制”字段中的服务项。

   “服务状态”字段用于显示有关服务的状态信息。

   对于 POP、IMAP 和 HTTP，该字段可显示上次连接的时间，连接总数，当前连接次数，上次启动服务后的连接失败次数，和上次启动服务后的登录失败的次数。

   该字段中的信息有助于了解服务器所载负荷以及服务的可靠性，而且可就服务器的安全警示发生的攻击情况。
5. 若需启动某项服务，可在 “进程控制”字段中将其选取并单击 “启动”。
6. 若需关闭某项服务，可在 “进程控制”字段中将其选取并单击 “停止”。
7. 若需启动或关闭所有已启用的服务，可单击 “全部启动”或 “全部停止”按钮。

命令行 您可通过 `start-msg` 和 `stop-msg` 命令启动或停止任何一种邮件服务（`pop`、`imap`、`http`、`smtp`、`store`），如下例所示：

server_root`/msg-`*instance*`/start-msg imap`
server_root`/msg-`*instance*`/stop-msg pop`
server_root`/msg-`*instance*`/stop-msg smtp`

备注 `start-msg smtp` 和 `stop-msg smtp` 命令可用于启动和停止所有 MTA 服务，而不仅仅是 SMTP 服务器。当启动或停止 MTA 服务时要想获得更精细控制，可使用 `imsimta start` 和 `imsimta stop` 命令。有关详细信息，请参阅 **iPlanet Messaging Server Reference Manual**。

配置问候邮件

Messaging Server 可用于为每位新用户创建一封问候邮件。

Console 通过 Console 创建新用户贺信：

1. 在 Console 中打开要为之配置新用户贺信的 Messaging Server。
2. 单击“配置”选项卡。如果左面板中的服务器图标尚未突出显示，请将其选中。
3. 单击右面板中“其他”选项卡。
4. 然后便可根据需要创建发给新用户的问候邮件或进行更改。

   问候文本须编排为电子邮件格式，包括邮件头（至少包括一个主题行），然后空行，接着为邮件正文。

   创建邮件时，用邮件字段上方的下拉列表指定所用语言。如果需要，可使不同的语言创建数个邮件。基于“配置自动回复邮件的语言”中说明的信息，服务器尝试把邮件的正确语言版本发送给新用户。
5. 单击“保存”。

命令行 通过命令行创建新用户贺信：

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

配置自动回复邮件的语言

本节说明服务器怎样为其发送的通知和邮件选择特定的语言版本。还说明了用户怎样指定一种首选语言和怎样指定一种默认的服务器站点语言。

用户可创建服务器在指定的条件下自动发送的邮件。例如，用“I am on vacation”休假消息自动回复所有来件。用户创建这种邮件时，可以指定邮件所使用的语言。这样用户就可以创建不同语言版本的邮件以备服务器发送。

用户也可以指定一种首选语言，表示希望所收到的自动回复邮件是用该语言写的，如果该语言版本可用的话。

服务器将根据以下规则选择待发邮件的特定语言版本：

1. 如果正接收邮件的用户已选择了一种首选语言 （请参阅第 36 页 “设置用户首选语言”）而且邮件的指定语言版本也存在，服务器就会发送邮件的那个语言版本。例如，若用户已选择日语，而且邮件的日语版本也存在，则发送日语版本。如果一个域的首选语言可用，并且有相应的自动回复邮件，则使用该邮件。
2. 如果用户未选择首选语言，或虽已选择但没有所选语言版本的邮件，服务器则发送与默认站点语言相匹配的版本 （请参阅第 36 页 “配置服务器站点语言”）。例如，默认站点语言为西班牙语，而用户已选择了法语，但是不存在邮件的法语版本，服务器则发送邮件的西班牙语版本。
3. 如果仅有邮件的一个版本，那么不管首选语言或站点语言是什么，该版本将被发送。
4. 如果没有和用户首选语言、默认站点语言或域首选语言相匹配的可用邮件版本，并且有一个以上的语言版本，则将在用户 LDAP 条目中找到的第一个邮件文本发送出去。

设置用户首选语言

用户可以通过 iPlanet Delegated Administrator for Messaging 界面选择首选语言。有些邮件客户程序也允许用户指定一种首选语言。如果通过 Delegated Administrator 设置了首选语言，有关信息保存于 Directory Server 中。

当服务器发送邮件给服务器管理域以外的用户时，服务器并不知道这些用户的首选语言，除非服务器正在回复在其邮件头中指定了首选语言的来件。根据用户邮件客户机中指定的属性设置标题段 （`accept-language`， `Preferred-Language` 或者 `X-Accept-Language`）。

如果首选语言在多处设定 - 例如，如果用户在 Directory Server 中保存有首选语言属性，而在其邮件客户机中也指定了首选语言 - 服务器按照以下顺序选择首选语言：

1. 原邮件的 `accept-Language` 邮件头字段
2. 原邮件的 `Preferred-Language` 邮件头字段
3. 原始邮件的 `X-Accept-Language` 邮件头字段
4. 发件人的首选语言属性 （如果可在 LDAP 目录中找到）

设置域首选语言

域首选语言是为一个特定的域指定的默认语言。例如，要为一个名为 `mexico.siroe.com` 的域指定西班牙语，管理员可通过两种方法为托管域选择一种域首选语言：一是通过 iPlanet Delegated Administrator for Messaging 界面创建该域时选择 Preferred Language 选项，二是通过把 LDAP 属性 `preferredLanguage` 添加到该域的 LDAP 条目。

配置服务器站点语言

可以按如下方式为服务器指定一种默认的站点语言。如果用户没有设置首选语言，服务器则用站点语言发送邮件的具体语言版本。

Console 通过 Console 指定一种站点语言

1. 打开要配置的 Messaging Server。
2. 单击“配置”选项卡。
3. 在右面板中单击“其他”选项卡。
4. 从站点语言的下拉列表中选择要使用的语言。
5. 单击“保存”。

命令行 也可以用下面的命令行指定一种站点语言：

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

这里的 *value* 是本地支持的语言之一：

```
af      南非荷兰语
ca      加泰罗尼亚语
da      丹麦语
de      德语
en      英语
es      西班牙语
fi      芬兰语
fr      法语
ga      爱尔兰语
gl      加利西亚语
is      冰岛语
it      意大利语
ja      日语
nl      荷兰语
no      挪威语
pt      葡萄牙语
sv      瑞典语
```

启用单次登录（SSO）

“单次登录”可使最终用户一次认证即可使用多个应用软件。例如，用户可以登录到 Messenger Express，然后使用 iPlanet Delegated Administrator for Messaging 而无需重新认证。

若需在实用程序间启用单次登录功能，必须对每个实用程序进行配置。这一部分说明如何在 Messenger Express 和 Delegated Administrator 之间启动单次登录请参阅第 39 页“启动 Messenger Express 和 iPlanet Delegated Administrator for Messaging 之间的单次登录”。

Messenger Express SSO 配置参数

用 `configutil` 命令可以为 Messenger Express 修改如表 2-4 中所示的单次登录配置参数。有关 `configutil` 的详细说明，请参见 **iPlanet Messaging Server Reference Manual**。

表 2-4　Messenger Express 单次登录参数

参数	说明
`local.webmail.sso.enable`	启用或禁用所有单次登录功能，包括取回登录页时接受和检验由客户程序提交的 SSO cookie，若登录成功则返回一个 SSO cookie 给客户程序，并响应其它 SSO 成员对其自己 cookie 的检验请求。 如果设置为任何非零值，服务器将执行所有 SSO 功能。 如果设置为零值，服务器则不执行任何 SSO 功能。 默认值为零。
`local.webmail.sso.prefix`	当格式化由 HTTP 服务器设置的 SSO cookie 时，参数的字符串值被作为前缀值使用。服务器只识别带这个前缀的 SSO cookie，所有其它 SSO cookie 将被忽略。 空的参数值可有效地禁用服务器上的所有 SSO 功能。 默认值为空值。
`local.webmail.sso.id`	当格式化由 Messenger Express HTTP 服务器设置的 SSO cookie 时，参数的字符串值被用作实用程序的 ID 值。 默认值为空值。
`local.webmail.sso.cookiedomain`	参数的字符串值可用来设置由 Messenger Express HTTP 服务器设定的所有 SSO cookie 的 cookie 域的值。 默认值为空值。
`local.webmail.sso.singlesignoff`	如果设为非零值，该参数的整数值可在客户退出时清除客户机上的前缀与 local.webmail.sso.prefix 所配置的值相匹配的所有 SSO cookie。 如果设为零值， Messenger Express 将在客户退出时清除自己的 SSO cookie。 默认值为零。
`local.sso.`*appid*`.verifyurl`	为同级 SSO 主机设置校验 URL 的值。 *appid* 是同级 SSO 主机的实用程序 ID，其 SSO cookie 需予以承认。例如 Delegated Administrator 的 *appid* 是 `nda45`。 应为每个受托的同级 SSO 主机定义一个参数。校验 URL 的标准格式为： `http://`*nda- host*:*port*`/VerifySSO?`

因此，启动 Messenger Express 的单次登录需要按照以下步骤设置配置参数（默认域为 eng.siroe.com）

```
configutil -o local.sso.appid. verifyurl -v "http://nda-host:port/verifySSO?"
configutil -o local.webmail.sso.enable -v 1
configutil -o local.webmail.sso.prefix -v ssogrp1
configutil -o local.webmail.sso.id -v msg50
configutil -o local.webmail.sso.cookiedomain -v ".siroe.com"
configutil -o local.webmail.sso.singlesignoff -v 1
```

启动 Messenger Express 和 iPlanet Delegated Administrator for Messaging 之间的单次登录

要启动 Messenger Express 和 Delegated Administrator 之间的单次登录，必须执行以下的附加步骤：

1. 配置 Directory Server
   a. 在 Directory Server 中创建代理用户帐户条目
   b. 为认证代理程序创建一个 ACI（访问控制指令）
2. 配置 Delegated Administrator
   a. 添加用户代理程序凭证
   b. 添加单次登录 cookie 信息
   c. 添加合作服务器的校验 URL
3. 重启动 Enterprise Server

要配置 Directory Server，需使用 `ldapmodify` 实用程序。有关该实用程序的详细信息，请参见 Directory Server 文档。

配置 Delegated Administrator 时，需修改以下配置文件：

iDA_server_root`/nda/classes/netscape/nda/servlet/resource.properties`

Web_server_root`/https-`*instancename*`/config/servlets.properties`

Web_server_root`/https-`*instancename*`/config/contexts.properties`

步骤 1a. 创建用户代理帐户

用户代理帐户可将用户绑定到用于代理认证的 Directory Server 上。下面是用户代理帐户条目的例子。

```
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
```

步骤 1b. 为代理认证程序创建 ACI

然后用 `ldapmodify` 实用程序为在安装时创建的后缀创建 ACI：

- `osiroot` - 为您输入的用以存储用户数据的后缀
- `dcroot` - 为您输入的用以存储域信息的后缀
- `osiroot` - 为您输入的用以存储配置信息的后缀 （默认后缀为 `osiroot`）

下面是 ACI 条目的例子：

```
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";)
```

步骤 2a. 在 resource.properties 文件中添加用户代理凭证

配置代理认证的 Delegated Administrator 时，需去掉 Delegated Administrator *iDA_server_root*`/nda/classes/netscape/nda/servlet/resource.properties` 文件中以下条目的注释标记并加以修改：

`LDAPDatabaseInterface-ldapauthdn=`*Proxy_Auth_DN*

`LDAPDatabaseInterface-ldapauthdn=`*Proxy_Auth_Password*

例如：

```
LDAPDatabaseInterface-ldapauthdn=
   uid=proxy, ou=people, o=siroe.com, o=mailqa
   LDAPDatabaseInterface-ldapauthpw=proxypassword
```

步骤 2b. 添加单次登录 Cookie 信息

若需添加单次登录所需的 cookie 信息，可为 Delegated Administrator 定义一个上下文标识符，并为上下文指定一个 cookie 名，如下所示：

- 若需定义一个上下文标识符，请编辑 Enterprise Server *Web_Server_Root*/https-*instancename*/config/servlets.properties 文件，并且去掉所有包括文本 servlet.xxxxx.context=ims50 行的注释标记。
- 若需为 Delegated Administrator 配置中的上下文指定 cookie 名，需在 Delegated Administrator *iDA_Server_Root*/nda/classes/netscape/nda/servlet/resource.properties 文件中添加以下条目：

  ```
  NDAAuth-singleSignOnId=ssogrp1-
  NDAAuth-applicationId=nda45
  ```

- 若需为 Enterprise Server 参数的内容指定 cookie 名称，需在 Enterprise Server *Web_Server_Root*/https-*instancename*/config/contexts.properties 文件中添加以下条目：

  ```
  context.ims50.sessionCookie=ssogrp1-nda45
  ```

步骤 2c. 添加合作服务器的校验 URL

校验接收到的单次登录 cookie 时， Delegated Administrator 必须知道在与谁联系。所以必须为所有已知的合作服务器提供校验 URL。

在以下的例子中，我们假定安装了 Messenger Express，且其应用程序 ID 为 msg50。编辑 Delegated Administrator *iDA_server_root*/nda/classes/netscape/nda/servlet/resource.properties 文件，并且添加一个如下的条目：

```
verificationurl-ssogrp1-msg50=http://webmail_hostname:port/VerifySSO?
verificationurl-ssogrp1-nda45=http://nda_hostname:port/VerifySSO?
```

步骤 3. 重启动 Enterprise Server

在按照步骤 1a 到 2c 中的描述改变了配置后，必须重启动 Enterprise Server 以使更改生效。

定制目录查找

若没有一个基于 LDAP 的目录系统 （诸如 iPlanet Directory Server）， iPlanet Messaging Server 则不能运行。 Messaging Server 和 Console 出于以下三个目的需要进行目录访问：

- 当首次安装 Messaging Server 时，须输入服务器配置所需的各种设置。这些设置存储在一个中心 *configuration directory* 目录中。配置与此目录的连接是安装过程的一部分。
- 为邮件用户或邮件组创建或更新帐户信息时，信息存储在一个称为 *user directory* 的目录中。服务器组的 Administration Server 已在安装时配置，所以当访问“用户”和“组”时， Console 将按默认设置连接到该用户目录。该用户目录定义了您的 *管理拓扑*，即一系列 iPlanet 服务器共享同一配置目录和用户目录。
- 当选择邮件路径并向邮箱发送邮件时， Messaging Server 要查找用户目录中有关发件人和收件人的信息。按照默设置， Messaging Server 将查看其 Administration Server 已被配置使用的同一用户目录。

可用下列方法修改每个目录配置的设置：

- Console 的 Administration Server 界面可用来更改配置目录的连接设置。（有关信息，请参见 **Managing Servers with Netscape Console** 中的“管理服务器”一章。）
- 当更改用户和组信息时， Console 的 Users 和 Groups 界面可用来暂时连接到一个不同于默认目录的用户目录。（有关信息，请参见 **Managing Servers with Netscape Console** 中的“用户和组”一章。）
- Console 的 Messaging Server 界面可用来配置 Messaging Server 以便连接到另一用户目录，即不同于 Administration Server 所定义的默认用户目录。这就是本节介绍的配置任务。

为用户和组查找功能重新配置 Messaging Server 以便连接到不同的用户目录，这项任务完全是可选的。在多数情况下，定义服务器管理域的用户目录就是该域所有服务器使用的用户目录。

备注 若需为 Messaging Server 查找功能指定一个自定义的用户目录，则在每次访问 Console 的 Users 和 Groups 界面以更改目录的用户或组信息时，都必须指定相同的目录。有关详细信息，请参阅附录 D，“管理邮件用户和邮件发送列表”。

Console 若需用 Console 修改 Messaging Server LDAP 用户查找设置，请按下列步骤操作：

1. 从 Console 打开 Messaging Server，即需自定义其 LDAP 连接的邮件服务器。
2. 单击“配置”选项卡。
3. 在左面板选择 Services 文件夹。

4. 在右面板中选择 LDAP 选项卡。 LDAP 表格随即出现。

   LDAP 表格此时将显示配置目录和用户目录的配置设定情况。但配置目录的设定值在表中为只读格式。如果需要修改，可参见 **Managing Servers with Netscape Console** 中的“管理服务器”一章。

5. 若需更改用户目录连接设置，可单击标有“使用特定于 Messaging Server 的目录设置”的复选框。

6. 通过输入或修改任何下列信息来更新 LDAP 配置 （关于目录概念的解释，包括对*判别名*这样术语的定义，请参阅 **Directory Server Administrator's Guide**）：

   主机名：主机的名称，此主机上驻留的目录中包含您安装的用户信息。这种主机一般与 Messaging Server 主机不同，尽管对于非常小的安装可能相同。

   端口号：目录主机上的端口号，即 Messaging Server 在查找用户时必须访问的目录。该端口号由目录管理员定义，不必是默认端口号 （389）。

   Base DN：目录条目判别名的搜索基，它代表用户查找的起始点。为加速查找过程，搜索基在目录树中应尽量靠近被查找的信息。如果安装目录树有一个“people”或者“users”分枝，这种分枝就是合理的出发点。

   Bind DN：当连接到需查找的 directory server 上时， Messaging Server 用来代表其自身的判别名。Bind DN 必须是用户目录条目判别名，此目录对用户部分有优先搜索权。如果目录允许匿名搜索访问，则可保持此条目的空白状态。

7. 若需更改与 Bind DN 相关连的口令，以便向用于用户查找的 LDAP 目录认证此 Messaging Server，可单击 Change Bind 口令按钮。 Password-Entry 窗口随即打开，此时便可输入更新的口令。

   自定的安全策略决定了在此情况下用什么口令。最初，口令被设置为无口令。如果已指定允许匿名访问 （即保持 Bind DN 字段的空白状态），就不必使用口令。

   这一步骤可更新服务器配置中储存的口令，但无法改变 LDAP 服务器中的口令。按照默认设置，这一帐户也可以用于 PAB 查找。口令改变后需执行以下两个步骤。

8. 修改 `local.ugldapbinddn` 配置属性中所指定的用户的口令。这一用户帐户存在于 `local.ugldaphost` 配置属性中指定的目录服务器中。

9. 如果将同样的帐户用于 `local.service.pab.ldapbinddn` 和 `local.service.pab.ldaphost` 属性中指定的 PAB 访问中，那么必须更新保存在 `local.service.pab.ldappasswd` 中的口令。

要返回到使用默认用户目录，取消“使用区分邮件服务器的目录设置”的复选标记。

命令行 也可在命令行设定用户目录连接设置的值，如下所示：一定也要按照上述的步骤 8 和步骤 9 设置 LDAP 和 PAB 的口令。

指定是否使用 Messaging Server 专用的目录设置：

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

指定用户查找所需的 LDAP 主机名：

```
configutil -olocal.ugldaphost -v name
```

指定用户查找所需的 LDAP 端口号：

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

指定用户查找所需的 LDAP base DN：

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

指定用户查找所需的 LDAP bind DN：

```
configutil -olocal.ugldapbinddn -v binddn
```

加密设置

可用 Console 启用“安全套接层”（SSL）为 Messaging Server 加密和认证，并选择具体的加密密码，即服务器在所有服务中支持的密码。

虽然这是一般性的配置任务，但仍然放在第 12 篇，“配置安全和访问控制”中的 “启用 SSL 和选择密码”一节中进行说明，该节还包含了涉及 Messaging Server 的所有安全性和访问控制方面的背景信息。

第 3 篇

配置 POP、 IMAP 和 HTTP 服务

iPlanet Messaging Server 支持客户访问邮箱所用的邮局协议（POP3）、 Internet 邮件访问协议 4（IMAP4）以及超文本传输协议（HTTP）。IMAP 和 POP 两个通信协议均属 Internet 标准邮箱协议。 Messenger Express 是一基于 web 的电子邮件程序，可使最终用户利用浏览器访问他们的邮箱，浏览器运行于使用 HTTP 协议的与 Internet 连接的计算机系统。

本章将说明如何通过 iPlanet Console 或命令行实用程序来配置服务器以使其支持一项或多项服务。

备注	如果安装的是 iPlanet Directory Server 5.1，您则必须通过 iPlanet Console 5.0（与 Directory Server 5.1 一起安装）对其进行管理。 iPlanet Messaging Server 5.2 必须通过 Netscape Console 4.2（与 Messaging Server 5.2 一起安装）进行管理。

有关配置简单邮件传输协议（SMTP）服务的信息，请参阅第 6 篇，“关于 MTA 服务与配置”。

本章包括以下各节：

- 一般配置
- 登录要求
- 性能参数
- 客户访问控制
- 配置 POP 服务
- 配置 IMAP 服务
- 配置 HTTP 服务

一般配置

对 Messaging Server 的 POP、IMAP 及 HTTP 服务的一般功能之配置，有启用和关闭服务、指定端口号以及 （可选）修改发送给连接客户机的服务标志区等选项。本节提供的是背景信息，至于完成这些设置所需的具体步骤，请参阅第 51 页 “配置 POP 服务”、第 52 页 “配置 IMAP 服务”以及第 54 页 “配置 HTTP 服务”。

启用和关闭服务

您可控制任何特定的 Messaging Server 实例，以决定其 POP、 IMAP 或 HTTP 服务是否可用。这不同于启动和停止服务操作（参阅第 33 页“启动和停止服务”）；若需使 POP、IMAP 或 HTTP 发挥效用，就必须同时启用并启动之。

与启动和停止服务相比，启用一项服务是一更 “全局性”的进程。例如，“启用”之设置在系统的各种再引导程序上都有，但于再引导后，您必须重新启动一项以前 “停止”了的服务。

对于不准备使用的服务，您不必将其启用。例如，若一个 Messaging Server 实例只作为邮件传送代理 （MTA）使用，则应关闭 POP、 IMAP 和 HTTP。若只用于 POP 服务，则应关闭 IMAP 和 HTTP。若只用于基于 web 的电子邮件，则应关闭 POP 和 IMAP。

您可在服务器级上启用或关闭服务。这一过程将在本节中详述。您还可通过设定专门的 LDAP 属性而在用户级上启用或关闭服务。有关详细信息，请参阅 **iPlanet Messaging Server Provisioning Guide**。

指定端口号

对于每一项服务，您可指定服务器使用该服务的连接端口号：

- 若需启用 POP 服务，可为服务器指定用于 POP 连接的端口号。默认值为 110。
- 若需启用 IMAP 服务，可为服务器指定用于 IMAP 连接的端口号。默认值为 143。
- 若需启用 HTTP 服务，可为服务器指定用于 HTTP 连接的端口号。默认值为 80。

在某些情况下，可能需要指定一个不同于默认值的端口号；例如，一台主机上运行两个或更多的 IMAP 实例，或同一主机既作为 IMAP 服务器又作为 Messaging Multiplexor 服务器使用。（有关 Multiplexor 方面的信息，请参阅第 4 篇，“配置和管理 Multiplexor 服务”。）

指定端口号时，需注意以下几点：

- 端口号可为从 1 到 65535 的任何数。
- 确保所选端口为尚未占用或为另一项服务所保留。

加密通信端口

Messaging Server 可通过安全套接层 （SSL）协议支持与 IMAP 和 HTTP 客户机的加密通信。有关在 Messaging Server 中对 SSL 支持的一般信息，请参阅第 308 页 “配置加密的和基于证书的认证”。

IMAP Over SSL

可接受默认的 IMAP over SSL 端口号 （993），也可对 IMAP over SSL 指定另一端口。

由于当前大部分 IMAP 客户机都需要分开的端口，因此 Messaging Server 提供了可以分开的 IMAP 和 IMAP over SSL 端口的选项。IMAP 和 IMAP over SSL 采用同一端口进行通信的作法是一种新兴标准。只要 Messaging Server 有已安装的 SSL 证书 （参阅第 310 页 “索取证书”），就可支持同端口的 IMAP over SSL。

HTTP Over SSL

可接受默认的 HTTP over SSL 端口号 （443），也可为 HTTP 指定一个分开的端口。

服务标志区

当某客户机首次连接到 Messaging Server 的 POP 或 IMAP 端口时，服务器将向该客户机发送一个标识文字串。此服务标志 （通常不向客户机用户显示）将服务器标识为 iPlanet Messaging Server，并显示服务器版本号。服务标志主要用于客户机故障排除或问题隔离。

如果要向连接的客户机发送不同的讯息，可替换 POP 服务或 IMAP 服务的默认标志区。

您可通过 iPlanet Console 或 `configutil` 实用程序（`service.imap.banner`, `service.pop.banner`）设置服务标志区。有关 `configutil` 的语法细节，请参阅 **iPlanet Messaging Server Reference Manual**。

登录要求

可控制用户登录到 POP、 IMAP 或 HTTP 服务以检索邮件的方式。可允许基于口令的登录（适用于所有服务项），以及基于证书的登录（适用于 IMAP 或 HTTP 服务）。本节提供背景信息，至于完成这些设置的具体步骤，可参阅第 51 页 “配置 POP 服务” 、第 52 页 “配置 IMAP 服务”或第 54 页 “配置 HTTP 服务”。此外，您还可指定 POP 登录所需的有效登录分割符。

设置 POP 客户程序的登录分割符

对于某些 POP 邮件客户程序而言，通信服务器将不接受 `@` 为登录分割符 （如 `uid@domain` 地址中的 `@`） 。这些客户程序包括 Netscape Messenger 4.76、 Netscape Messenger 6.0 和 Windows 2000 上的 Microsoft Outlook Express。解决这一问题的迂回方法如下：

1. 请用下列命令使 + 成为有效的分割符：

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

2. 通知 POP 客户程序用户登录时应使用 + 作为登录分割符，不要使用 `@`。

基于口令的登录

在典型的邮件系统中，用户通常以在邮件客户程序中输入一个口令之形式访问他们的 POP、IMAP 或 HTTP 邮箱。客户机将口令发送给服务器，服务器据此认证用户。若用户被认证通过，服务器将基于访问控制规则决定是否准许用户访问储存在该服务器中的特定邮箱。

若允许口令登录，用户即可通过输入口令访问 POP、 IMAP 或 HTTP。（基于口令的登录是 POP 服务的唯一认证方式）。口令储存于 LDAP 目录中。目录策略决定了哪些口令策略（如最短长度等）有效。

若不允许用口令登录到 IMAP 或 HTTP 服务，则禁止基于口令的认证。于是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 服务中口令传递的安全性，可要求口令在发送到服务器之前先经过加密处理。在对口令进行加密处理时，须为登录选择一个最短密码长度要求。

- 如果选择 0，则表示不要求加密。口令则以明码发送，或根据客户程序的安全策略加密发送。
- 如果选择一个非零值，客户机在建立与服务器的 SSL 会话时则必须使用密钥长度不小于指定长度的密码，以便加密客户机发送的任何 IMAP 或 HTTP 用户口令。

若客户机所配置的加密密钥长度大于服务器支持的最大长度，或服务器所配置的加密密钥长度大于客户机所支持的长度，则无法实现基于口令的登录。有关设置服务器所支持的各种密码及密钥长度的信息，请参阅第 312 页 “启用 SSL 和选择密码”。

基于证书的登录

除了基于口令的认证外， iPlanet 服务器还支持通过检查数字证书而对用户进行认证之策略。与提供口令不同的是，客户机在与服务器建立 SSL 会话时提供的是用户证书。若证书验证有效，用户则被认证通过。

有关设置 Messaging Server 以使 IMAP 或 HTTP 服务采用基于证书的用户登录方面的说明，请参阅第 314 页 “设置基于证书的登录”。

启用基于证书的登录功能时，无需取消 IMAP 或 HTTP 系统表单中 “允许口令登录”复选框的选中状态。若该复选框已被选中（这是它的默认状态），且已执行设置基于证书的登录所需的任务，那么基于口令的登录和基于认证的登录会同时得到支持。因此，若客户机建立了 SSL 会话并提供了证书，服务器则将使用基于证书的登录。若客户机没有使用 SSL 或没有提供客户证书，则会发送一个口令。

性能参数

您可为 Messaging Server 的 POP、 IMAP 或 HTTP 服务项设置一些基本的性能参数。基于硬件能力和用户基数，您可调整这些参数，使服务发挥最大效用。本节提供背景信息，至于完成这些设置的具体步骤，可参阅第 51 页 “配置 POP 服务” 、第 52 页 “配置 IMAP 服务”或第 54 页 “配置 HTTP 服务”。

进程数量

Messaging Server 可将其工作分解到几个执行进程中，这在某些情况下可提高效率。这一能力对多处理器服务器尤其有用，因为通过调节服务器进程的数量可将多任务更有效地分配于硬件处理器中。

但是，在多进程中分派任务，以及从一个进程转换到另一进程，也是要付出开销的。多进程的优点将随着每一个新进程的添加而减少。对于大多数配置而言，一个简单的经验法则是：使服务器计算机中的每个硬件处理器有一个进程，最多不超过四个。最恰当的配置因情况而异，此经验法则只具有进行分析的出发点的意义。

备注：在某些平台上，可能需要增加进程数量以绕过针对该平台的、可能影响其性能的某些极限值 （如文件描述符的最大数量等）。

对每一 POP、 IMAP 或 HTTP 服务项，其默认的进程数量都是 1。

每一进程的连接数

POP、 IMAP 或 HTTP 服务能同时维持的客户连接数越多，对客户机就越便利。若客户机由于无法获得连接而被拒绝服务，它们就只能等待，直到有其他客户机断开连接时为止。

另一方面，每一个开通的连接都要耗费内存资源，且对服务器的 I/O 子系统产生需求。因此，服务器所能同时支持的会话数量是有限度的。（有可能通过增加服务器内存或 I/O 容量来提高限度。）

在这方面， IMAP、 HTTP 以及 POP 有不同的需求：

- 与 POP 和 HTTP 连接相比， IMAP 连接一般来说是长命的。当用户连接到 IMAP 下载邮件时，连接会一直持续下去，直到用户退出或连接超时为止。相比之下，POP 或 HTTP 连接通常在提供了 POP 或 HTTP 请求后会立即关闭。
- IMAP 和 HTTP 连接通常比 POP 连接更有效率。每一次 POP 的再次连接都需要重新进行用户认证。而 IMAP 连接则只需要一次认证，这是由于在 IMAP 会话期间（从登录到注销）连接一直维持开通状态。 HTTP 连接通常较短暂，但用户不必每次连接时重新认证，因为 HTTP 会话（从登录到注销）允许多重连接。因此，相对于 IMAP 或 HTTP 连接而言， POP 连接要付出大的多的性能开销。 iPlanet Messaging Server 尤其如此，因为它是通过打开的但又空闲的 IMAP 连接和多重 HTTP 连接，在设计上有要求非常低的开销。

备注	关于 HTTP 会话安全的详细信息，请参阅第 304 页 “关于 HTTP 安全性”。

因此，在某个给定用户需求的某个给定时刻，Messaging Server 可支持比 POP 连接更多的打开的 IMAP 连接或 HTTP 连接。

IMAP 的默认值为 4000 ； HTTP 的默认值为每进程为 6000 个连接； POP 的默认值为 600。这些默认值粗略地代表了典型配置的服务器计算机所能处理的等量需求。最恰当的配置因情况而异，这些默认值只供您用作一般的参考。

每一进程的线程数

除了支持多进程外， Messaging Server 还可通过再将工作细分到多线程而使性能进一步改善。服务器对线程的使用极大地提高了执行效率，因为正在运行的命令并不妨碍其他命令的执行。线程可按照执行过程中的需求创建或删除，最多可达到所设置的最大数量。

多个同时执行的线程意味着更多的客户请求可在没有耽搁的情况下得到处理，这样便可使大量的客户快速获得服务。然而，在线程间分派任务是要付出开销的，因此服务器使用的线程数量要有一个限度。

对于 POP、IMAP 和 HTTP 而言，默认的最大值为每一进程 250 线程。尽管 IMAP 和 HTTP 的默认连接数大于 POP 的默认连接数，但对于相应的线程数，三个默认值相等。这是基于这样的假定：在具有相同最大线程数的情况下， POP 连接虽然较少但很忙碌，而能被高效处理的 IMAP 和 HTTP 连接则较多。最佳配置因情况而异，但这些默认值已经足够大，因而看不出有增大这些值的必要；这些默认值可为大多数系统提供合理的性能。

切断空闲连接

为了收回与无应答客户连接的系统资源，IMAP4、POP3 以及 HTTP 协议允许服务器单方面切断已空闲了一段特定时间的连接。

各协议规范都要求服务器在最短时间段内保持空闲连接的开通状态。对于 POP，默认时间为 10 分钟；对于 IMAP，默认时间为 30 分钟，对于 HTTP，默认时间为 3 分钟。您可在这些默认值的基础上增加空闲时间，但不能缩短这个时间。

若 POP 或 IMAP 连接被切断，用户须重新认证才能重新建立连接。相比而言，若 HTTP 连接被切断，由于 HTTP 会话仍处于开通状态，因而不需重新认证。关于 HTTP 会话安全的详细信息，请参阅第 304 页 “关于 HTTP 安全性”。

空闲的 POP 连接常常是由于出现某种问题 （如崩溃或中断）致使客户机无法应答而造成的。另一方面，空闲的 IMAP 连接则是经常发生的情况。为了使 IMAP 用户免受被单方面切断的困扰， IMAP 客户机可在小于 30 分钟的时间间隔内有规律地向 IMAP 服务器发送命令。

注销 HTTP 客户机

HTTP 会话可跨越多个连接。当连接被切断时， HTTP 客户机并未注销。然而，如果空闲的 HTTP 会话持续了一段时间后，服务器会自动切断该 HTTP 会话时段并注销该客户机 （默认时间段为 2 小时）。当会话时段被切断后，客户机会话 ID 变为无效，客户机须重新认证才能建立另一个会话。有关 HTTP 安全和会话 ID 的详细信息，请参阅第 304 页 “关于 HTTP 安全性”。

客户访问控制

iPlanet Messaging Server 包含访问控制功能，您可用该功能以决定那些客户可使用 POP、IMAP 或 HTTP （以及 SMTP）邮件服务。您可基于多种标准创建灵活的访问过滤器，用以允许或拒绝客户的访问。

客户访问控制是 iPlanet Messaging Server 的重要安全特性。有关客户访问控制过滤器的创建方法及使用实例方面的信息，请参阅第 317 页“配置 POP、IMAP 和 HTTP 服务的客户访问权”和第 328 页 “配置客户机访问 SMTP 服务”。

配置 POP 服务

您可通过 `configutil` 命令或用 iPlanet Console（控制台）对 Messaging Server 的 POP 服务进行基本配置。本章将介绍一些较常用的 POP 服务选项。详细列表请见 **iPlanet Messaging Server Reference Manual**。

有关详细信息，还可参见：

- 启用和关闭服务
- 设置 POP 客户程序的登录分割符
- 指定端口号
- 每一进程的连接数
- 切断空闲连接
- 每一进程的线程数
- 进程数量

Console 用 Console 配置 POP 服务：

1. 从 iPlanet Console 中打开需配置的 Messaging Server。
2. 单击 “配置”选项卡并打开左面板中的 Services 文件夹。
3. 选择 POP。
4. 单击右面板中的 “系统”选项卡。
5. 若需启用该服务项，选中标有“启用端口上的 POP 服务”复选框，然后指定一个端口号。
6. 按下列方式指定连接设置：
   - 设置每一进程的最大网络连接数。有关详细信息，请参阅第 49 页 “每一进程的连接数”。
   - 设置连接的最大空闲时间。有关详细信息，请参阅第 50 页 “切断空闲连接”。
7. 按下方式指定进程设置：
   - 设置每一进程的最大线程数量。有关详细信息，请参阅第 50 页“每一进程的线程数”。
   - 设置最大进程数量。有关详细信息，请参阅第 49 页 “进程数量”。
8. 如有需要，可在 POP 服务标志区字段中的指定一服务标志区。
9. 单击 “保存”。

备注 POP 服务的基于口令的登录功能将自动启用。

命令行 在命令行中，请按如下方式设置 POP 属性值：

启用或关闭 POP 服务：

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

指定端口号：

```
configutil -o service.pop.port -v 端口号
```

设置每一进程的最大网络连接数：

```
configutil -o service.pop.maxsessions -v 端口号
```

设置连接的最大空闲时间：

```
configutil -o service.pop.idletimeout -v 端口号
```

设置每一进程的最大线程数量：

```
configutil -o service.pop.maxthreads -v 端口号
```

设置最大进程数：

```
configutil -o service.pop.numprocesses -v 端口号
```

指定一个协议欢迎标志区：

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

配置 IMAP 服务

您可通过 `configutil` 命令或用 iPlanet Console（控制台）对 Messaging Server 的 IMAP 服务进行基本配置。本章将介绍一些较常用的 IMAP 服务选项。详细列表请见 **iPlanet Messaging Server Reference Manual**。与之相关的详细信息，还可参见：

- 启用和关闭服务
- 指定端口号
- 基于口令的登录
- 每一进程的连接数
- 切断空闲连接
- 每一进程的线程数
- 进程数量

Console 从 Console 配置 IMAP 服务：

1. 从 iPlanet Console 中打开需配置的 Messaging Server。
2. 单击“配置”选项卡并打开左面板中的 Services 文件夹。
3. 选择 IMAP。

4. 单击右面板中的 “系统”选项卡。
5. 若需启用该项服务，选中标有 “启用端口上的 IMAP 服务”的复选框，然后指定一个端口号。
6. 如有需要，可启用基于口令的登录功能。
7. 按下列方式指定连接设置：
   - 设置每一进程的最大网络连接数。有关详细信息，请参阅第 49 页“每一进程的连接数”。
   - 设置连接的最大空闲时间。有关详细信息，请参阅第 50 页 “切断空闲连接”。
8. 按下方式指定进程设置：
   - 设置每一进程的最大线程数量。有关详细信息，请参阅第 50 页“每一进程的线程数”。
   - 设置最大进程数量。有关详细信息，请参阅第 49 页 “进程数量”。
9. 如有需要，可在 IMAP 服务标志区字段中指定一个服务标志区。
10. 单击 “保存”。

命令行 按下列方式在命令行中设置 IMAP 属性值：

启用或关闭 IMAP 服务：

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

指定端口号：

```
configutil -o service.imap.port -v 端口号
```

为 IMAP over SSL 启用一分开的端口：

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

指定 IMAP over SSL 的端口号：

```
configutil -o service.imap.sslport -v 端口号
```

启用和关闭 IMAP 服务的口令登录：

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

其中的 *值* 为下列值之一：

```
 -1 - 关闭口令登录
  0 - 启用不加密口令登录
 40 - 启用口令登录并指定加密强度
128 - 启用口令登录并指定加密强度
```

设置每一进程的最大网络连接数：

```
configutil -o service.imap.maxsessions -v 端口号
```

设置连接的最大空闲时间：

```
configutil -o service.imap.idletimeout -v 端口号
```

设置每一进程的最大线程数量：

```
configutil -o service.imap.maxthreads -v 端口号
```

设置最大进程数：

```
configutil -o service.imap.numprocesses -v 端口号
```

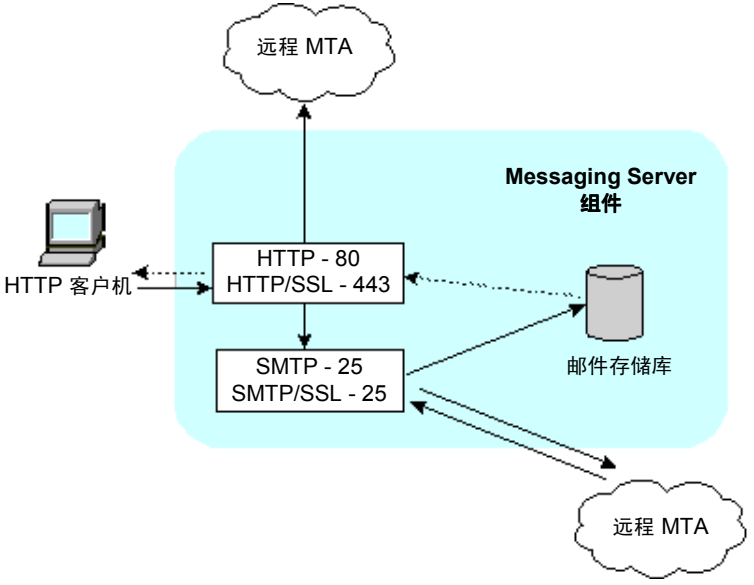
指定一个协议欢迎标志区：

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

配置 HTTP 服务

POP 和 IMAP 客户机可将邮件直接发送给 iPlanet Messaging Server MTA 进行路由选择或传递。而 HTTP 客户机则将邮件发送到一个专用的 web 服务器，该服务器是 iPlanet Messaging Server 的组成部分。HTTP 服务随后将邮件发送到本地 MTA 或远程 MTA 进行路由转换或传递，如图 3-1 所示。

图 3-1 HTTP 服务组件



HTTP 的许多配置参数与 POP 和 IMAP 服务使用的参数相似。这些参数包括连接设置参数和进程设置参数。本章将介绍一些较常用的 HTTP 服务选项。详细列表请见 **iPlanet Messaging Server Reference Manual**。有关详细信息，还可参见：

- 启用和关闭服务
- 指定端口号

- 基于口令的登录
- 每一进程的连接数
- 切断空闲连接
- 注销 HTTP 客户机
- 每一进程的线程数
- 进程数量

有些参数是特别针对 HTTP 服务的，其中包括邮件设置参数和 MTA 设置参数。

邮件设置 当 HTTP 客户构建一个带附件的邮件时，该附件被上载到服务器并保存在一个文件中。在邮件被发送到 MTA 进行路由选择或传递之前，HTTP 服务将检索附件并构建邮件。您可接受默认的附件假脱机目录，或指定一个备用目录。还可指定容许的附件大小的最大值。

MTA 设置 在默认状态下， HTTP 服务将外发邮件发送到本地 MTA 进行路由选择或传递。也有可能需要把 HTTP 服务配置成将邮件发送到远程 MTA。例如，当站点是一托管服务且大部分收件人不在本地主机的同一域内时。若需将邮件发送到远程 MTA，则需指定远程主机名以及远程主机的 SMTP 端口号。

Console 用 iPlanet Console 配置 HTTP 服务：

1. 从 iPlanet Console 中打开需配置的 Messaging Server。
2. 单击 “配置”选项卡并打开左面板中的 Services 文件夹。
3. 选择 HTTP。
4. 单击右面板中的 “系统”选项卡。
5. 若需启用该项服务，可选中标有 “启用端口上的 HTTP 服务”复选框，然后指定一个端口号。
6. 如有需要，可启用基于口令的登录功能。
7. 按下列方式指定连接设置：
   - 设置每一进程的最大网络连接数。有关详细信息，请参阅第 49 页 “每一进程的连接数”。
   - 设置连接的最大空闲时间。有关详细信息，请参阅第 50 页 “切断空闲连接”。
   - 设置客户会话最大空闲时间。有关详细信息，请参阅第 50 页“注销 HTTP 客户机”。
8. 按下方式指定进程设置：
   - 设置每一进程的最大线程数量。有关详细信息，请参阅第 50 页“每一进程的线程数”。
   - 设置最大进程数量。有关详细信息，请参阅第 49 页 “进程数量”。

9. 按下列方式指定邮件设置：

- 如有需要，可指定附件假脱机目录。
- 如有需要，可指定出站邮件大小的最大值。请注意，这里包括所有以 base64 编码的附件，而 base64 编码需要 33% 的额外空间。因此，如果控制台有 5 MB 的限制，其结果是：一封邮件和附件的最大大小应在 3.75M 左右。

有关详细信息，请参阅第 55 页 “邮件设置”。

10. 按下列方式指定 MTA 设置：

- 如有需要，可指定一个备用 MTA 主机名。
- 如有需要，可指定一个备用 MTA 端口。

有关详细信息，请参阅第 55 页 “MTA 设置”。

11. 单击 “保存”。

命令行 按下列方式在命令行中设定 HTTP 属性的值：

启用和关闭 HTTP 服务：

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

指定端口号：

```
configutil -o service.http.port -v 端口号
```

为 HTTP over SSL 启用一分开的端口：

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

指定 HTTP over SSL 的端口号：

```
configutil -o service.http.sslport -v 端口号
```

启用或关闭口令登录：

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

其中的*值*为下列值之一：

```
 -1 - 关闭口令登录
  0 - 启用不加密口令登录
 40 - 启用口令登录并指定加密强度
128 - 启用口令登录并指定加密强度
```

设置每一进程的最大网络连接数：

```
configutil -o service.http.maxsessions -v 端口号
```

设置连接的最大空闲时间：

```
configutil -o service.http.idletimeout -v 端口号
```

设置客户会话最大空闲时间：

```
configutil -o service.http.sessiontimeout -v 端口号
```

设置每一进程的最大线程数量：

```
configutil -o service.http.maxthreads -v 端口号
```

设置最大进程数：

```
configutil -o service.http.numprocesses -v 端口号
```

指定客户外发邮件的附件假脱机目录：

```
configutil -o service.http.spooldir -v 目录路径
```

指定邮件大小的最大值：

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

其中的 *大小* 是字节数。请注意，这里包括所有以 base64 编码的附件，而 base64 编码需要 33% 的额外空间。因此，如果控制台有 5 MB 的限制，其结果是：一封邮件和附件的最大大小应在 3.75M 左右。

指定备用 MTA 主机名：

```
configutil -o service.http.smtphost -v 主机名
```

指定备用 MTA 主机名端口号：

```
configutil -o service.http.smtpport -v 端口号
```

第 4 篇

配置和管理 Multiplexor 服务

本章说明随 iPlanet Messaging Server 一起提供的两种 Multiplexor（多路复用器），即用于标准邮件协议（POP、IMAP 和 SMTP）的 Messaging Multiplexor（MMP）和用于 Messenger Express 网络界面的 Messenger Express Multiplexor。

本章包含下列主题：

- 关于 MMP 服务
- 关于 iPlanet Messaging Multiplexor (MMP)

备注	有关安装 MMP 的说明，请参阅 **iPlanet Messaging Server Installation Guide**。有关 MMP 配置参数的详细信息，请参阅 **iPlanet Messaging Server Reference Manual**。

- 关于 Messenger Express Multiplexor

关于 MMP 服务

MMP 在取得水平伸缩性 （通过增加计算机数量支持更多用户的能力）方面是必不可少的，因为它提供了可用于非直接连接多邮件存储库的单一域名。 MMP 还能提供安全上的好处。

当 MMP 由 iPlanet Messaging Server 分别管理时， Messenger Express Multiplexor 内置于包含 iPlanet 邮件存储库及邮件访问安装中的 HTTP 服务中 （`mshttpd`）。

Multiplexor 的优点

在高负荷使用的邮件服务器上的邮件存储库会变得非常庞大。因此将用户邮箱和用户连接分布在多个服务器上能提高系统容量和性能。此外，使用多个小型服务器会比使用一个大规模、高容量、多处理器的计算机更具有成本效益。

当邮件服务器安装的规模需要使用多个邮件库时，您所在公司或企业将会在几个方面受益于 MMP。用户与邮件库之间的非直接连接以及可在数个邮件服务器之间对用户帐户进行重新配置之简便性，具有如下益处：

- **简化用户管理**

  由于所有用户都连接到一个服务器上（或者多个服务器，如果为 POP、IMAP、SMTP 或网络访问分别配置 Multiplexor 计算机的话），所以可以预先配置邮件客户程序，并向所有用户发布统一的登录信息。这不仅简化了管理任务，而且减少了发布错误登录信息的可能性。

  在极高负荷的情况下，可使用相同配置的多个 Multiplexor 服务器，并通过 DNS 的循环反复或使用负荷平衡系统管理通往这些服务器的连接。

  由于 MMP 是使用存储在 LDAP 目录中的信息来查找每个用户的 Messaging Server，因此对于系统管理员来讲，将用户移至一个新的服务器十分简单，且对于用户来讲是透明的。管理员可以将用户的邮箱从一个 Messaging Server 移至另一个，然后更新用户在 LDAP 目录中的条目。而用户的邮箱地址、邮箱访问以及其它客户机首选项无须改变。

- **性能上的提高**

  如果单个机器的邮件存储库增长过大，可通过将部分邮件库移动到其它计算机的方法来平衡负荷。

  可以将不同类的用户分配到不同的计算机。例如，您可以通过选择将重要用户放置在容量更大、性能更强的机器上。

  MMP 具有某些缓存功能，这样较慢的客户机连接（例如通过调制解调器）不会使 Messaging Server 慢下来。

- **降低成本**

  由于一个 Multiplexor 就可以高效管理多个 Messaging Server，因此可以通过购买多个小型服务器降低总费用，因为多台小型机器的价格可能低于一台大型机。

- **提高伸缩性**

  使用 MMP 可以轻松地扩展配置。当性能或存储容量需要提高时可陆续增加计算机，而不用替换现有的设备。

- **降低用户停机时间**

  使用 MMP 将巨大的用户群分散到多个小型存储机上，从而隔离了用户停机时间。当某个服务器发生故障时，只有出故障的服务器用户会受到影响。

- **增强安全性**

  您可将安装有 MMP 的服务器作为防火墙机器使用。将所有客户机的连接路由选定在该计算机后，便可限制外部计算机对内部邮件存储计算机的访问。MMP 可支持与客户机的未加密和加密通讯。

关于 iPlanet Messaging Multiplexor

iPlanet Messaging Multiplexor（MMP）是一部专用的邮件服务器，可用作多个后端邮件服务器的单一连接点。通过 Messaging Multiplexor，大规模邮件服务提供商可将 POP 和 IMAP 用户邮箱分布到多台计算机上，以提高邮件库容量。所有用户都可连接到这部单一的 Multiplexor 上，然后由其将每个连接重新定向到适当的邮件服务器上。

如果需为很多用户提供电子邮件服务，可通过安装并配置 Messaging Multiplexor 使整个邮件服务器阵列作为一个单主机出现在邮件用户面前。

Messaging Multiplexor 是作为 iPlanet Messaging Server 的组成部分提供的。可以在安装 Messaging Server 或其它 iPlanet 服务器的同时安装 MMP，也可以在以后单独安装。

MMP 支持：

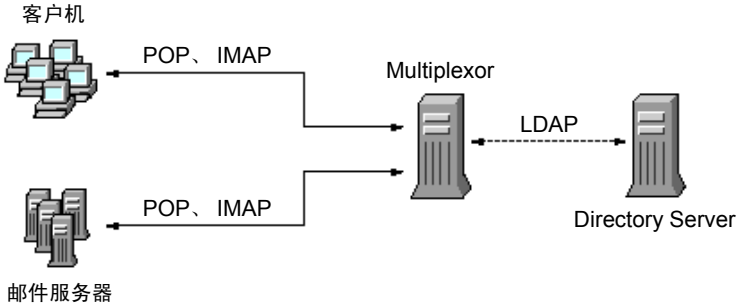
- 与邮件客户机的未加密和加密 （SSL）通讯。
- 有关基于证书的客户认证说明，请见第 62 页 “基于证书的客户认证”。
- 有关用户预认证方面的说明，请见第 63 页 “用户预认证”。
- 虚拟域可在不同的 IP 地址上监听，并可在用户 ID 上自动添加域名。有关说明，请见第 64 页 “MMP 虚拟域”。
- 可在不同的计算机上安装多 MMP （每台计算机一个）。请参阅 **iPlanet Messaging Server Installation Guide**。
- 有关在一台服务器机器上安装的多个 Multiplexor 实例的说明，请见第 65 页 “多重 Messaging Multiplexor 实例”。多实例可用于备用配置，如 SSL 或不能通过虚拟域处理的监听端口。
- 强化 LDAP 搜索功能
- 为旧 POP 客户机提供的 POP before SMTP 服务。有关详细信息，请参阅第 325 页“启用 POP Before SMTP”。

MMP 的工作原理

iPlanet MMP 是一种能够在多个服务器机器上分配邮件用户的多线程服务器。 MMP 可用来处理目的地为其他服务器 （用户邮箱所驻留的计算机）的入站客户机连接。客户机首先连接到 MMP 本身，由 MMP 确定该用户所需的服务器，将之连接到该服务器，然后在客户机和服务器间传送数据。这种能力可使互联网服务供应商及其它大型用户设施能够将邮件库分散在多台计算机上（以提高容量），同时又能以单一邮件主机之形式面向用户（以提高效率）和外部客户 （以提高安全性）。

图 4-1 所示为在安装有 MMP 的系统中客户机与服务器的相互关系。

图 4-1 在安装有 MMP 的系统中的客户机和服务器



所有 POP、IMAP 和 SMTP 客户机都能使用 Messaging Multiplexor。MMP 的任务是接受连接，执行 LDAP 目录查找，并选择恰当的路由连接。与通常的邮件服务器系统一样，每个用户都在特定的 Messaging Server 上分配有特定的地址和邮箱。但所有连接都是通过 MMP 发送的。

以下是建立用户连接所涉及的具体步骤：

1. 用户的客户机连接到 MMP， MMP 接受初步的认证信息 （用户名）。
2. MMP 查询 Directory Server 以决定哪一 Messaging Server 包含该用户邮箱。
3. MMP 连接到正确的 Messaging Server，重新认证，然后在连接持续期间充当连通管道。

加密 （SSL）选项

iPlanet Messaging Multiplexor 既支持 Messaging Server 与邮件客户程序间的不加密通讯，也支持它们间的加密 （SSL）通讯。

当 SSL 被启用时，MMP IMAP 和 SMTP 服务便可支持 STARTTLS，MMP 也可通过配置来监听 SSL IMAP、 POP 和 SMTP 连接的附加端口。

为了启用 IMAP、 POP 和 SMTP 服务的 SSL 加密功能，需分别编辑 `ImapProxyAService.cfg`、 `PopProxyAService.cfg` 和 `SmtpProxyAService.cfg` 三个文件。同时还必须编辑 `AService.cfg` 文件中的 `default:ServiceList` 选项以包括所有 IMAP、 POP 和 SMTP 服务器端口的列表，而不管其安全状态如何。

在默认状态下，由于 SSL 配置参数被加上了注释标记，因此 SSL 未被启用。要启用 SSL，您必须安装 SSL 服务器证书。然后应该去掉注释标记以设置 SSL 参数。若需查阅 SSL 参数列表，请参阅 **iPlanet Messaging Server Reference Manual**。

基于证书的客户认证

MMP 可使用证书映射文件（`certmap`）以使客户的证书匹配用户 / 用户组 Directory Server 中的正确用户。

在使用基于证书的客户认证时，还须启用第 62 页 “加密 （SSL）选项”中说明的 SSL 加密功能。

还必须配置一个存储管理员。可以使用邮件管理员，但建议为此创建独特的用户 ID，如 mmpstore，以便在需要时设置权限。

请注意 MMP 不支持 certmap 插件。但 MMP 接受在 certmap.conf 文件中的强化 DNComps 和 FilterComps 属性值条目。这些增强格式条目使用下列格式：

mapname:DNComps *FROMATTR=TOATTR*
mapname:FilterComps *FROMATTR=TOATTR*

于是证书 subjectDN 中的 *FROMATTR* 值可用于构成一个 LDAP 查询，并具有 *TOATTR=value* 元素。例如，一个 subjectDN 为 “cn=Pilar Lorca, ou=pilar o=siroe.com”的证书能够使用下行所示元素而映射到 “(uid=pilar)”的 LDAP 查询：

mapname:FilterComps ou=uid

若需启用 IMAP 服务的基于证书的认证，请按下列步骤操作：

1. 确定准备作为存储管理员的用户 ID。

   虽然可使用邮件管理员达到此目的，但建议为存储管理员创建一个独特的用户 ID（例如，mmpstore）。

2. 检查 SSL 加密功能是否已经（或即将）启用，即像在第 62 页 “加密 （SSL）选项”中说明的那样。

3. 通过在配置文件中指定 certmap.conf 文件的位置来配置 MMP 使用基于证书的客户认证。

4. 至少要安装一个受托的 CA 证书，如在第 311 页 “安装委托 CA 证书”中说明的那样。

用户预认证

MMP 可向您提供一个预认证用户所需的选项，您可通过该选项将用户作为到访用户绑定到目录，并记录结果。

备注 启用用户预认证功能将降低服务器性能。

日志条目采用如下格式：

日期 时间 (sid 0x*hex*) 用户 *名称*预认证客户 IP *地址*服务器 IP *地址*

其中 *日期*采用 yyyymmdd 的格式，*时间* 是 UTC （标准国际协调时，也就是 GMT （格林威治标准时间））并以格式 hhmmss 表示，*hex* 是以十六进制数表示的会话标识。(sid)，用户 *名称*包括虚拟域 （如果有的话）以及点分断格式的 IP 地址。

MMP 虚拟域

一个 MMP 虚拟域是一套与某服务器 IP 地址相关联的配置设置。这种形式的主要用途在于可为每一个服务器 IP 地址提供不同的默认域。

用户可以用短格式的用户 ID 或是形如 `user@domain` 的全限定用户 ID 认证到 MMP。如果提供的是短格式用户 ID，MMP 将附加默认域设置，如果有所指定的话。因此，支持多托管域的网站只需将每个托管域与一个服务器 IP 地址和 MMP 虚拟域相关联就可允许使用短格式的用户 ID。

要定位给定托管域中的用户子树，建议采用该域的 LDAP 域树条目中的 `netDomainBaseDN` 属性。MMP 的 `LdapUrl` 设置不适用于此目的，因为后端邮件库服务器也需要在 LDAP 中查找用户但却不支持虚拟域。

若需启用虚拟域，请编辑 `ImapProxyAService.cfg`、`PopProxyAService.cfg` 或 `SmtpProxyAService.cfg` 等 **instance** 目录中的文件，以使 `VirtualDomainFile` 设置指定虚拟域映射文件的全路径。

虚拟域文件的每个条目具有如下语法：

`vdmap`：*名称 IPaddr*
名称：*参数值*

其中，*名称*仅用于将 IP 地址与配置参数相关联，而且可以是任意选定的名称，*IPaddr* 是以点分断的格式，*参数*和*值*对用以配置虚拟域。设置后，虚拟域配置参数值将取代全局配置参数值。

以下列出的是能够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`
`StoreAdmin and StoreAdminPass`
`SearchFormat`
`TCPAccess`
`TCPAccessAttr`

备注 除非 `LdapURL` 设置正确，否则 `BindDN`、`BindPass`、`LdapCacheSize` 和 `LdapCacheTTL` 等设置将被忽略。

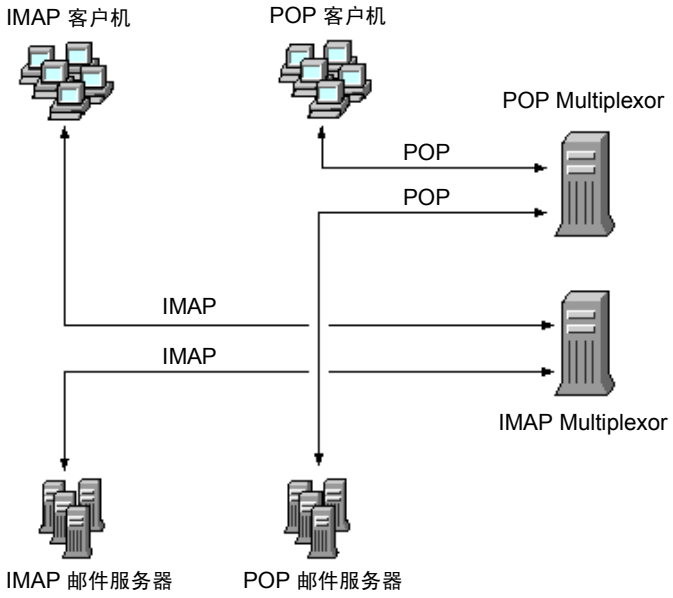
关于这些配置参数的详细信息，请参阅 **iPlanet Messaging Server Reference Manual**。

多重 Messaging Multiplexor 实例

您可在单个服务器上安装 MMP 的多个实例。每一个实例将作为独立的进程运行，可以有不同的配置文件。当不同的服务器 IP 地址或端口需要不同的设置时，多重实例是必不可少的，而那些设置不能被虚拟域改变。 SSL 服务器证书就是这种设置的一个例子。

可以配置一个 MMP 的单实例来同时支持 POP、IMAP 和 SMTP 协议（如图 4-1 所示），或者可以为每个协议分别创建实例，如图 4-2 所示。通过在不同的计算机上分离邮件服务，可以调整每台计算机上的资源以获得最大性能。

图 4-2 各协议分开的 MMP 实例



关于创建 MMP 多重实例的说明，请参阅 **iPlanet Messaging Server Installation Guide**。

关于 SMTP 代理

MMP 包括一个默认为禁用的 SMTP 代理。大多数网站不需要 SMTP 代理，因为互连网邮件标准已经为 SMTP （DNS MX 记录）的水平伸缩性提供了充分的运行机制。

SMTP 代理所提供的安全功能十分有用。首先，SMTP 代理与 POP 代理结合，以在 SMTP 之前实现一些旧 POP 客户机所要求的 POP 认证功能。有关详细信息，请参阅第 325 页 “启用 POP Before SMTP”。

此外，使用 SMTP 代理可使 SSL 加速硬件的投资效益最大化。请参阅第 315 页 “如何用 SMTP 代理优化 SSL 的性能”。

配置 Messaging Multiplexor

配置 Multiplexor 时，必须手工编辑在表 4-1 列出的 Messaging Multiplexor 配置文件中的配置参数。

表 4-1　Messaging Multiplexor 配置文件

文件	说明
PopProxyAService.cfg	配置文件，用于指定 POP 服务使用的配置变量。
PopProxyAService-def.cfg	POP 服务配置模板如果 PopProxyAService.cfg 文件不存在，那么 PopProxyAService-def.cfg 模板被复制以建立一个新的 PopProxyAService.cfg 文件。
ImapProxyAService.cfg	配置文件，用于指定 IMAP 服务使用的配置变量。
ImapProxyAService-def.cfg	IMAP 服务配置模板。如果 ImapProxyAService.cfg 文件不存在，那么 ImapProxyAService-def.cfg 模板被复制以建立一个新的 ImapProxyAService.cfg 文件。
AService.cfg	配置文件，用于指定需启动的服务以及 POP 和 IMAP 服务可共享的一些选项。
AService-def.cfg	配置文件，用于指定需启动的服务以及 POP 和 IMAP 服务可共享的一些选项。如果 AService.cfg 文件不存在，那么 AService-def.cfg 模板被复制以建立一个新的 AService.cfg 文件。
AService.rc	用于启动、停止、重启动和重载 MMP 的脚本。 要启用 MMP 在重启动后的自动启动， AService.rc 脚本可复制到 /etc/init.d 并象征性的链接到适当的 /etc/rc?.d 目录中去。有关初始化和终止脚本的详细信息，请参阅 init.d. 上联机操作说明。
SmtpProxyAService.cfg	用于指定针对 SMTP 代理服务的配置变量的可选配置文件。如果在 SMTP 前启用 POP，则需要该文件；即使不启用 SMTP 前的 POP，该文件也可最大限度地支持 SSL 硬件。有关 SMTP before POP 的详细信息，请参阅第 325 页 “启用 POP Before SMTP”。
SmtpProxyAService-def.cfg	用于指定针对 SMTP 代理服务的配置参数的配置模板。如果 SmtpProxyAService.cfg 文件不存在，那么 SmtpProxyAService-def.cfg 模板被复制以建立一个新的 SmtpProxyAService.cfg 文件。

Messaging Multiplexor 配置文件存储在 *server-root*/mmp-*hostname* 目录下，其中 *server-root* 是安装 Messaging Server 的目录，mmp- *hostname* 是以 MMP 实例命名的子目录。例如，如果在名为 tarpit 的计算机上安装了 MMP，并且接受了默认的安装位置，配置文件则位于 /usr/iplanet/server5/mmp-tarpit。

作为范例，参数 LogDir 和 LogLevel 存在于所有配置文件中。在 ImapProxyAService.cfg 文件中，它们用于指定与 IMAP 相关事件的记录参数；同样，在 PopProxyAService.cfg 文件中，这些参数用于配置与 POP 相关事件的记录参数。在 SmtpProxyAService.cfg 文件中，它们用于指定与 SMTP 代理相关事件的日志记录方式。

而在 AService.cfg 文件中，LogDir 和 LogLevel 则用于记录 MMP 范围内的失败情况，例如无法启动 POP、 IMAP 或 SMTP 服务的情况。

备注 当安装或升级 MMP 时，配置模板文件将被盖写。

有关所有 MMP 配置参数的完整说明，请参阅 **iPlanet Messaging Server Reference Manual**。

启动 Messaging Multiplexor

UNIX 系统

要启动 UNIX 系统中 Messaging Multiplexor 的一个实例，需要运行目录 *server_root*/mmp-*hostname* 中的 AService.rc 脚本：

./AService.rc [*选项*]

AService.rc 脚本的可选参数已在表 4-2 中说明。

表 4-2 AService.rc 脚本的可选参数

选项	说明
start	用于启动 MMP （即使已有一个 MMP 正在运行）。
stop	用于停止最近启动的 MMP。
restart	用于停止最近启动的 MMP，然后再启动一个 MMP。
reload	用于使一个已经运行的 MMP 在不中断任何现用连接的情况下重载其配置文件。

Windows NT 系统

要在 Windows NT 下启动一个 Messaging Multiplexor 实例，转到 Windows NT 控制面板的“服务”，单击“启动”。也可单击“停止”来停止 MMP。服务选项说明，见下面的表 4-3。

表 4-3　Windows NT MMP 服务选项

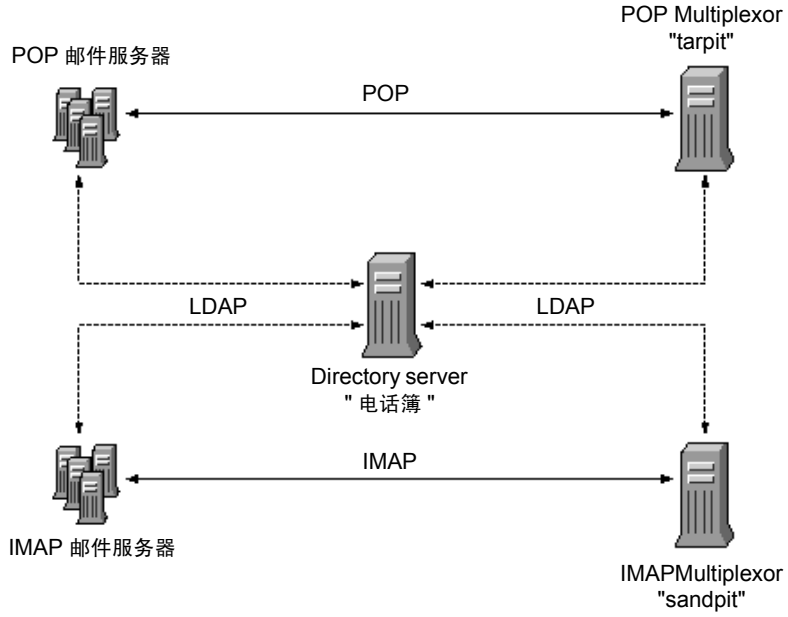
选项	说明
`start`	在控制面板中，启动 MMP（即使已经有一个正在运行），或在命令行执行命令 `AService.exe start`
`stop`	在控制面板，停止最近启动的 MMP，或在命令行执行命令 `AService.exe stop`
`restart`	要重新启动 Windows NT，需停止最近启动的 MMP，然后再启动 MMP。
`reload`	要重载 MMP，转到 mmp-instance 目录，在命令行执行命令 `AService.exe refresh`

拓扑结构范例

虚拟 Siroe 公司的不同的单独计算机上有两个 Messaging Multiplexors，每个都支持多个 Messaging Server， POP 和 IMAP 用户邮箱分布在不同的 Messaging Server 计算机上，每个服务器专用于 POP 或专用于 IMAP（只需把 `ImapProxyAService` 条目从 `ServiceList` 配置中移出，就可限制客户只能访问 POP 服务；同样，只需把 `PopProxyAService` 条目从 `ServiceList` 配置中移出，就可限制客户只能访问 IMAP 服务。）每个 Messaging Multiplexor 也支持 POP 专用或 IMAP 专用。 LDAP 目录服务驻留在一台单独专用机上。

下面的图 4-3 所示为这一拓扑结构的情况。

图 4-3 多 MMP 对多 Messaging Server 的支持



IMAP 配置范例

图 4-3 中的 IMAP Messaging Multiplexor 安装在 `sandpit` 上面，这是一台有两个处理器的计算机。此 Messaging Multiplexor 监听 IMAP 连接的标准接口（143）。Messaging Multiplexor 在主机的 `phonebook` 上与 LDAP 服务器通讯以获得用户邮箱信息，并通过路由选择将连接发送给适当的 IMAP 服务器。它可取代 IMAP 容量字符串，提供虚拟域文件，并支持 SSL 通讯。

下表是其 ImapProxyAService.cfg 配置文件：

```
default:LdapUrl             ldap://phonebook/o=Siroe.com
default:LogDir              /usr/iplanet/server5/mmp-sandpit/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 LANGUAGE XSENDER X-NETSCAPE XSERVERINFO AUTH=PLAIN"
default:SearchFormat        (uid=%s)
default:SSLEnable           yes
default:SSLPorts            993
default:SSLSecmodFile       /usr/iplanet/server5/mmp-sandpit/secmod.db
default:SSLCertFile         /usr/iplanet/server5/mmp-sandpit/cert7.db
default:SSLKeyFile          /usr/iplanet/server5/mmp-sandpit/key3.db
default:SSLKeyPasswdFile    ""
default:SSLCipherSpecs      all
default:SSLCertNicknames    Siroe.com Server-Cert
default:SSLCacheDir         /usr/iplanet/server5/mmp-sandpit
default:SSLBacksidePort     993
default:VirtualDomainFile   /usr/iplanet/server5/mmp-sandpit/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          /usr/iplanet/server5/mmp-sandpit/bgexcl.cfg
default:ConnLimits          0.0.0.0|0.0.0.0:20
default:LdapCacheSize       10000
default:LdapCacheTTL        900
default:HostedDomains       yes
default:DefaultDomain       Siroe.com
```

POP 配置范例

图 4-3 中的 POP Messaging Multiplexor 范例安装在 tarpit 上，这是一台有四个处理器的计算机。此 Messaging Multiplexor 监听 POP 连接的标准接口（110）。Messaging Multiplexor 在主机的 phonebook 上与 LDAP 服务器通讯以获得用户邮箱信息，并通过路由选择将连接发送给适当的 POP 服务器。它还可提供假邮件文件（spoof message file）。

下表是其 PopProxyAService.cfg 配置文件：

```
default:LdapUrl             ldap://phonebook/o=Siroe.com
default:LogDir              /usr/iplanet/server5/mmp-tarpit/log
default:LogLevel            5
default:BindDN              "cn=Directory Manager"
default:BindPass            password
default:BacksidePort        110
default:Timeout             1800
default:Capability          "IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS
CHILDREN LANGUAGE XSENDER X-NETSCAPE XSERVERINFO AUTH=PLAIN"
default:SearchFormat        (uid=%s)
default:SSLEnable           no
default:VirtualDomainFile   /usr/iplanet/server5/mmp-tarpit/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          /usr/iplanet/server5/mmp-tarpit/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
```

关于 Messenger Express Multiplexor

iPlanet Messenger Express Multiplexor 是一种专用服务器，可作为连接到 HTTP 访问服务的单一连接点使用。 Messenger Express 是 iPlanet Messaging Server HTTP 服务的客户机界面。所有用户都连接到这一邮件代理服务器，由其将用户导向各自的适当邮箱。因此，整个邮件服务器阵列将是以单一主机的形象出现在邮件用户面前的。

在 iPlanet Messaging Multiplexor（MMP）连接到 POP 和 IMAP 服务器期间，Messenger Express Multiplexor 与 HTTP 服务器相连接。换句话说，Messenger Express Multiplexor 对于 Messenger Express 的关系正如 MMP 对于 POP 和 IMAP 关系。

和 MMP 一样， Messenger Express Multiplexor 支持下列：

- 与邮件客户程序的未加密和加密 （SSL）通讯。

  有关配置 SSL 的详细信息，请参阅第 12 篇，“配置安全和访问控制”。

- 托管域

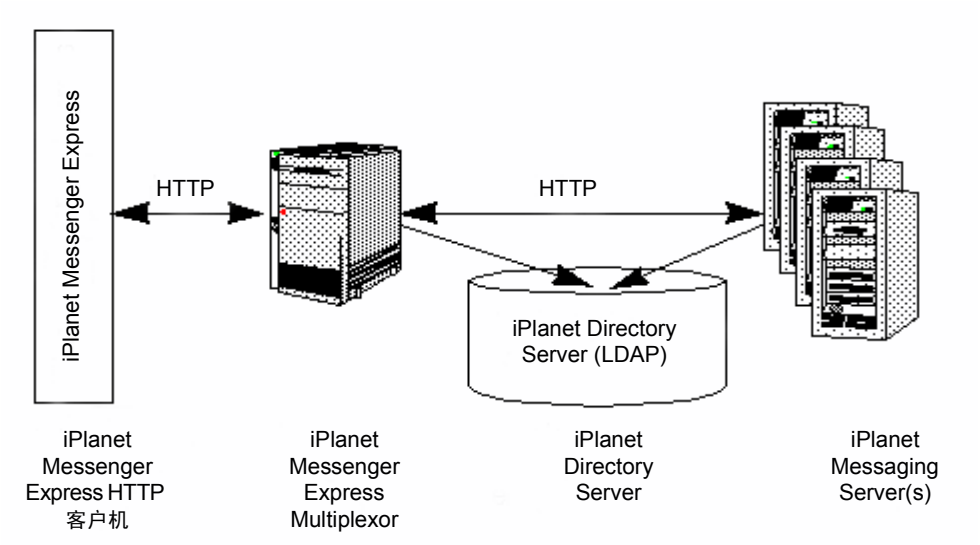
  有关详细信息，请参阅 **iPlanet Messaging Server Provisioning Guide**。

和 MMP 不同的是，Messenger Express Multiplexor 内置于 `mshttpd` 服务器，因此使用同样的日志记录和配置机制。

Messenger Express Multiplexor 的工作原理

Messenger Express Multiplexor 由一个作为 Multiplexor 的代理邮件服务器组成；可用于连接到 iPlanet Messaging Server （Messenger Express）的 HTTP 服务。 Messenger Express Multiplexor 使得邮箱可方便地分布在多个服务器机器上。客户机在登录到 iPlanet Messenger Express 时连接到 Multiplexor，Multiplexor 为用户确定正确的服务器并将之连接到该服务器，然后在客户机和服务器间传输数据。这种能力可使大型安装能够将邮件库分散在多台计算机上（以提高容量），同时又能以单一邮件主机的形象面对用户（以提高效率）和外部客户 （以提高安全性）。第 73 页图 4-4 介绍了在一 iPlanet Messaging Server 安装中 Messenger Express Multiplexor 驻留于何处。

图 4-4 iPlanet Messenger Express Multiplexor 概况



通过接受连接并适当地路由， Messenger Express Multiplexor 充当了 iPlanet Messenger Express 客户机和 iPlanet Messaging Server 之间的界面。与通常的邮件服务器系统一样，每个用户都在特定的邮件服务器上分配有特定的地址和邮箱。但是，所有的 HTTP 连接都通过 Messenger Express Multiplexor 路由。

以下是建立用户连接所涉及的具体步骤：

1. 一个用户的客户机连接到接受初步认证信息的 Messenger Express Multiplexor。
2. Messenger Express Multiplexor 查询 Directory Server 以确定哪个邮件服务器包含该用户的邮箱。
3. Messenger Express Multiplexor 连接到相关联的 Messaging Server，重新认证，然后作为会话期间的连通管道。

设置 Messenger Express Multiplexor

本节将介绍设置和配置 Messenger Express Multiplexor 应遵循的步骤。所涉及的主题包括：

- 在代理计算机上安装 Messaging Server
- 配置 Multiplexor 参数
- 启用 Messenger Express Multiplexor

在代理计算机上安装 Messaging Server

第一步是在代理计算机上安装将成为 Messenger Express Multiplexor 的 Messaging Server。有关具体安装说明，请参见 **iPlanet Messaging Server Installation Guide**。

务必要把 Messaging Server 配置到指向后端邮件服务器的用户和组目录服务器。此目录服务器将用于通过 Messenger Express Multiplexor 将用户认证到 Messaging Server。

配置 Multiplexor 参数

当完成了 Messaging Server 在代理计算机的安装后，即可配置 Messenger Express Multiplexor 参数：

1. 收集必要的后端 Messaging Server 信息。

   运行后端邮件服务器目录中的 `configutil` 命令，以确定本节后面要讲到的参数值。为了保证设置成功，代理计算机（Multiplexor 将在该处启用）的配置必须与后端邮件服务器相匹配。

2. 为 Messenger Express Multiplexor 设置配置参数

   运行代理计算机邮件服务器目录 *server_root*`/bin/msg-`*instance*`/configutil` 中的 `configutil` 命令，以设置配置值。注意这些值应与后端邮件服务器的值匹配。

   有关运行 `configutil` 命令的详细说明，请参见 **iPlanet Messaging Server Reference Manual**。

下列各节将介绍设置 Messenger Express Multiplexor 所必须的 `configutil` 参数：

- LDAP 参数
- dcroot
- 默认域
- 登录分隔符

LDAP 参数

应该确保 Directory Server 参数在启用 Messenger Express Multiplexor 之前正确指定。要确定 LDAP 参数，需运行相应后端 Messaging Server 实例目录中的下列命令：

- `configutil -o local.ugldaphost`

  此参数显示了后端邮件服务器使用的用户和组 LDAP Directory Server。要确保 `ldaphost` 设置为后端邮件服务器使用的同一数值（或包含同样数据的 LDAP 的复本服务器）。

- ```
  configutil -o local.ugldapbinddn
  configutil -o local.ugldapbindcred
  ```

  这些参数显示了用户和组的 Directory Server 管理员的 DN 和口令。`ldapbinddn` 和 `ldapbindcred` 都必须具备和后端邮件服务器相同的规格。

dcroot

应确保 *dcroot* 指定正确。要确定 *dcroot*，运行相应邮件服务器实例目录中的下列命令：

```
configutil -o service.dcroot
```
```

默认域

应确保邮件服务器默认域（*defaultdomain*）的正确性。要确定邮件服务器默认域，运行相应邮件服务器实例目录中的下列 `configutil` 命令：

```
configutil -o service.defaultdomain
```

登录分隔符

确保登录分隔符（*loginseparator*）与后端邮件服务器使用的登录分隔符保持一致。要确定邮件服务器登录分隔符，运行相应邮件服务器实例目录中的 `configutil` 命令：

```
configutil -o service.loginseparator
```

启用 Messenger Express Multiplexor

一旦设置好配置参数，就可以在代理计算机上启用 Messenger Express Multiplexor。要做到这一点，运行代理服务器上的邮件服务器实例目录 *server_root*`/bin/msg-`*instance*`/configutil` 中的下列 `configutil` 命令：

```
configutil -o local.service.http.proxy -v 1
```

其中 `1` 表示启用 Messenger Express Multiplexor （默认值为 `0`）。

当一个非本地用户（其邮件主机不在他们登录的服务器上的用户）登录而且 `local.service.http.proxy` 的值是 `0` 时，用户将被导向他的主机并会看到主机名的改变，因此说明 Multiplexor 未被启用。

如果 `local.service.http.proxy` 的值设置为 `1`， Multiplexor 被启用，主机名不变，并且整个邮件服务器阵列将以单一主机的形象出现在非本地邮件用户面前。

对于本地用户（其邮件主机就在他们登录的服务器上的用户）来说，服务器将使用本地邮件库，而不管参数 `local.service.http.proxy` 为何值。使代理和本地用户在同一邮件服务器上共存是可能的。

有关 `configutil` 命令的详细信息，请参阅 **iPlanet Messaging Server Reference Manual**。

测试所做的设置

在本节，您会学到如何测试您的 Messenger Express Multiplexor 设置以及如何在日志文件中查找消息。假定已配置好并启用了 Messenger Express Multiplexor。

访问 Messenger Express 客户机

在测试安装之前，您应该对 Messenger Express 产品有所了解。此外，还应该已经有一个事先创建好的测试帐户。

要测试 Messenger Express Multiplexor 代理，需遵循如下步骤：

1. 通过 Messenger Express Multiplexor，在浏览器中键入下列地址，以便连接到 Messenger Express：

   `http://` *msgserver_name*。

   例如：

   `http://budgie.sesta.com`

2. 使用预先创建的测试帐户，登录到 Messenger Express。
3. 应该能够成功登录并访问后端邮件服务器中的邮件。
4. 一旦通过 Messenger Express 登录后邮件服务器名称发生改变，那么需确保将 `local.service.http.proxy` 设置为 `1`，并重新启动邮件代理服务器。 Messenger Express Multiplexor 应以单一邮件主机的形象出现在用户面前。

出错讯息

如果在输入用户 id，口令和单击 “连接”时收到出错讯息，则应该检查代理计算机的 HTTP 日志文件。要检看出错讯息，转到 *server_root*`/msg-`*instance*`/log/http/` 目录。多数情况下，出错讯息将包含足够用以诊断问题的信息。若所含信息不足以诊断问题之所在，请与 iPlanet 客户支持中心取得联系。

管理 Messenger Express Multiplexor

本节介绍 Messenger Express Multiplexor 的基本管理能力。

配置与管理 SSL

有关配制和管理 Messenger Express Multiplexor 的 SSL（即安全套接层），请参见第 312 页 “启用 SSL 和选择密码”。

多重代理服务器设置

要创建单一名称寻址的多重 Messenger Express Multiplexor，可使用具有会话时段检测功能（session-aware）的负荷平衡设备。通过此设备，所有请求均可从任意客户机路由到一个唯一的服务器。

管理 Messaging Server 和 Messenger Express Multiplexor 的不同版本

如果 Messenger Express Multiplexor 和后端邮件主机上有 iPlanet Messaging Server 的不同版本，则需更新 Messenger Express 的静态文件以保证服务器间的兼容性。

组成 Messenger Express 界面的静态文件是由 Messenger Express Multiplexor，而非用户邮件主机直接提供服务的。Multiplexor 在 *server_root*`/msg-`*instance*`/html` 目录中寻找这些文件。

若需更新这些文件以确保服务器间的兼容性，需将新版本 Messaging Server 的目录 *server_root*/msg-*instance*/html 中的所有内容（包括组成 Messenger Express 界面的这些静态文件）替换为旧版本 Messaging Server 相同目录中的所有内容。

例如，如果后端邮件服务器使用 iPlanet Messaging Server 5.1，并且已安装了 iPlanet Messaging Server 5.2 作为 Messenger Express Multiplexor，则需把 Messenger Express Multiplexor 中 *server_root*/msg-*instance*/html 目录的所有内容替换为 iPlanet Messaging Server 5.1 后端服务器相同目录中内容。当最终将 iPlanet Messaging Server 5.1 升级为 iPlanet Messaging Server 5.2 后，也可以将 Messenger Express Multiplexor 服务器的 *server_root*/msg-*instance*/html 目录中的这些静态文件更新。

第 5 篇

MTA 概念

本章描述 MTA 的基本概念。本章由以下部分组成：

- MTA 功能
- MTA 体系和邮件流程概述
- Dispatcher
- 重写规则
- 通道
- MTA 目录信息
- 作业控制器

MTA 功能

邮件传送代理，或 *MTA*（第 81 页图 5-2），是 Messaging Server 的一个组件（第 80 页图 5-1），它可执行下列功能：

- **邮件路由** - 接受邮件并将其发送到：A) 另外的 SMTP 主机， B) 一个本地邮件存储库，或 C) 一个程序以便处理 （例如：病毒检查）。
- **邮件阻塞** - 依据指定的来源和 / 或目标的 IP 地址、邮件地址、端口、通道或者标题字符串，拒绝或接受的邮件。
- **地址重写** - 重写来件的 `From:` 或者 `To:` 地址为更适当的格式。
- **邮件处理** - 执行不同类型的邮件处理。例如：
  - 扩展别名
  - 控制 SMTP 命令和协议支持
  - 提供 SASL 支持
  - 当地址数量超过指定限度时暂时停发邮件
  - 将邮件传递到网站提供的程序，例如病毒检查和邮件归档程序
  - 对邮件进行一个部分至一个部分的转换
  - 定制传递状态通知邮件

图 5-1 iPlanet Messaging Server - 简化的组件视图 （Messenger Express 未显示）

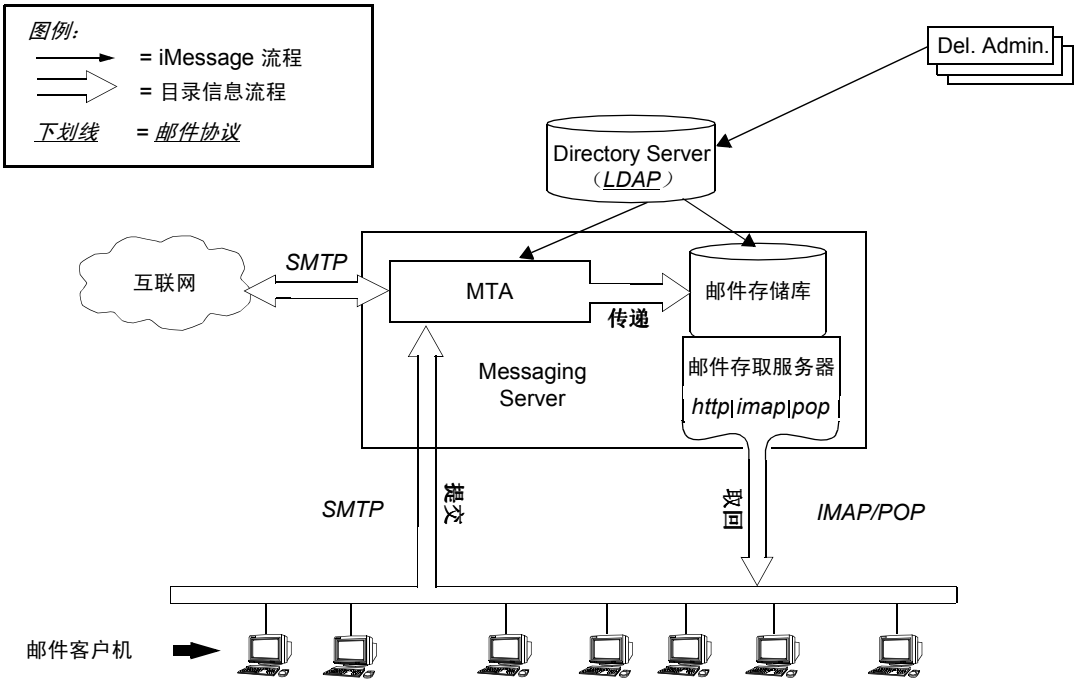
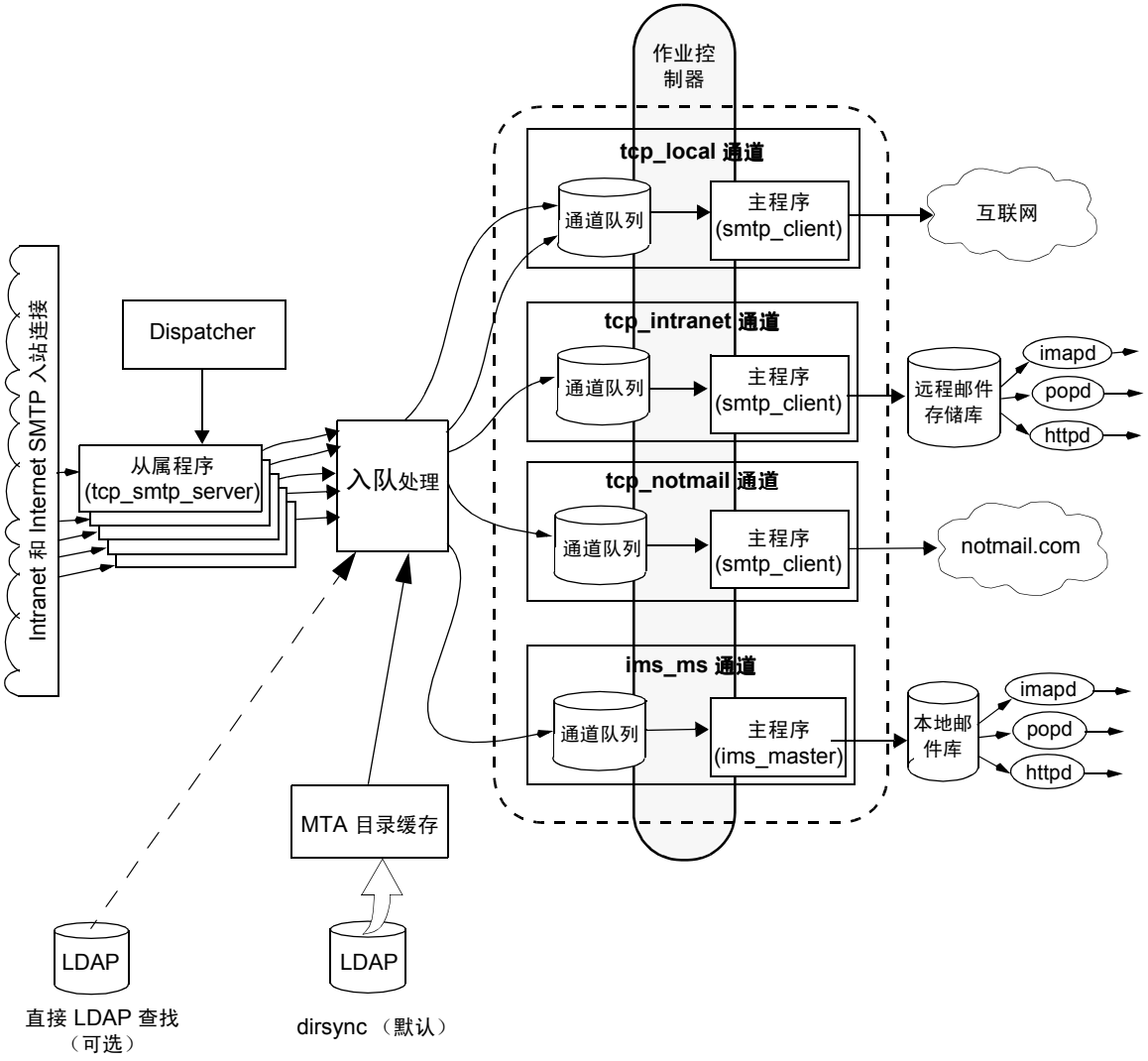


图 5-2 MTA 体系结构


作业控制器
tcp_local 通道
通道队列
主程序 (smtp_client)
互联网
tcp_intranet 通道
通道队列
主程序 (smtp_client)
远程邮件存储库
imapd
popd
httpd
tcp_notmail 通道
通道队列
主程序 (smtp_client)
notmail.com
ims_ms 通道
通道队列
主程序 (ims_master)
本地邮件库
imapd
popd
httpd
Intranet 和 Internet SMTP 入站连接
Dispatcher
从属程序 (tcp_smtp_server)
入队处理
MTA 目录缓存
LDAP
直接 LDAP 查找（可选）
LDAP
dirsync（默认）

MTA 体系和邮件流程概述

本节提供 MTA 体系和邮件流程简短概述 （图 5-2）。

Dispatcher 和 SMTP 服务器 （从属程序）

通过 SMTP 会话，邮件从 Internet 或 Intranet 进入 MTA。当 MTA 收到 SMTP 连接请求时，MTA *Dispatcher*（多线程连接发送代理）执行 *从属*程序（`tcp_smtp_server`）来处理 SMTP 会话。当其它会话请求时，Dispatcher 激活 SMTP 服务器程序处理每个会话。对于每个进入的邮件， Dispatcher 和从属程序一起完成许多不同的功能。三个基本功能是：

- 邮件阻塞 - 拒绝从指定的 IP 地址、 mail 地址、端口、通道、标题字符串等发来的邮件（第 10 篇，“邮件过滤与访问控制”）。
- 地址改写。进入的 `From:` 或者 `To:` 地址可能被重写为不同的格式。
- 通道入队。地址通过重写规则确定邮件应发送到那个通道。

有关详细信息，请参阅第 83 页 “Dispatcher”。

入队

在传递的这一阶段许多任务被激活，但主要的任务是：

- 别名展开。
- 地址通过重写规则确定邮件应在那个通道入队，并重写地址的域部分为合适的格式。
- 通道关键字处理。
- 发送邮件到适当的通道队列。

通道

通道是用于邮件处理的基本 MTA 组件。一个通道代表了与另一系统（如另一个 MTA、另一个通道或本地邮件存储库）的通讯连接。当邮件到达时，不同的邮件按照邮件的来源和目的地的不同，需要不同的路由和处理。例如，对传递到本地邮件存储库的邮件的处理有别于传递到 internet 邮件的处理，而后者又有别于发送到同一邮件系统中的另一个 MTA 的邮件的处理。通道为每个连接所需的处理和路由提供了定制机制。在默认安装中，大多数邮件进入这样一个通道，它可以处理 internet、 intranet 和本地邮件。

特殊的情况下也可创建专用的通道。例如，假定某个 internet 域处理邮件非常慢，导致发往该域的邮件阻塞 MTA。可以建立一个专用通道以提供对那些发往缓慢域的邮件的特殊处理，从而缓解系统中该域的瓶颈问题。

地址中域部分决定了邮件在那个通道入队。阅读域并确定适当通道的机制称为重写规则（参阅第 84 页 “重写规则”）。

通道通常由一个通道队列和一个称为 *主程序*的通道处理程序构成。当从属程序将邮件传递到适当的通道队列后，主程序就开始执行相应的处理并路由。包含有重写规则通道的详细说明和配置在 `imta.cnf` 文件中。下面所示为一个通道进入的例子：

```
tcp_intranet smtp mx single_sys subdirs 20 noreverse maxjobs 7
SMTP_POOL maytlsserver allowswitchchannel saslswitchchannel tcpauth
tcpintranet-daemon
```

第一个词，如此例中的 tcp_intranet，是通道名称。最后一个词称为通道标记。中间的词称为通道关键字，用以指明如何处理邮件。数百个不同的关键字使邮件可得到不同方式处理。在 **iPlanet Messaging Server Reference Manual** 和第 8 篇，“配置通道定义”有通道关键字的完整描述。

邮件传递

邮件经过处理后，主程序沿着邮件的传递路径向下一站发送邮件。这里的 “下一站”可能是既定收件人的信箱，另外的 MTA，甚至另一个通道。图中虽然没有表示出通往另一个通道的转发，但这确是一种常见情况。

Dispatcher

此 Dispatcher 是一个多线程调度代理允许若干多线程服务器进程共享担负 SMTP 连接服务的责任。当使用 Dispatcher 时，可以有几个多线程 SMTP 服务器进程同时运行并连接到同一的端口。此外，每个服务器都可以有一个或多个有效的连接。

Dispatcher 的作用像是配置中所列 TCP 端口的中央接收器。对于每项定义的服务，Dispatcher 可创建一个或多个 SMTP 服务进程以便在连接建立之后处理这些连接。

一般来说，当 Dispatcher 收到一个已定义 TCP 端口的连接时，它会为该端口的服务查找空闲的工作进程存储池，并为新连接选择最佳的候选端口。如果没有适合的候选者，在配置允许的情况下， Dispatcher 可以创建一个新的工作进程以处理此连接以及后续的连接。Dispatcher 也可能创建一个新的工作进程，以等待将来的外来连接。有多个配置选项可以用于设置 Dispatcher 对各种服务的控制，特别是控制工作进程的个数以及每个工作进程处理的连接个数。

要获得更多信息，请参阅第 106 页 “Dispatcher 配置文件”。

服务器进程的创建与终止

Dispatcher 内的自动内务管理功能控制着创建新的服务器进程和终止旧的或空闲的服务器进程。控制 Dispatcher 功能的基本选项是 MIN_PROCS 和 MAX_PROCS。MIN_PROCS 选项可使一定数量的服务器进程处于就绪状态以等待处理外来的连接，从而提供有保证的服务级别。另一方面， MAX_PROCS 选项可用来为指定的服务设置允许几个服务器进程并行工作的上限。

可能出现的情况是，因为服务器进程已在处理它所能承担的最大数量的连接，或因为这个进程已经被安排终止，所以当前运行的服务器进程可能无法接受任何连接。在这种情况下，Dispatcher 会创建额外的进程以帮助处理未来的连接。

MIN_CONNS 和 MAX_CONNS 选项可提供一种有助于在各个服务器进程间分配连接的机制。MIN_CONNS 用以指定将服务器进程标记为 “足够忙”的连接的数量，而 MAX_CONNS 则用以指定服务器进程可被标记为 “最忙”的连接的数量。

一般来说，在当前服务器进程的个数小于 MIN_PROCS 时，或者当所有现有服务器进程都“足够忙”（即每个服务器进程拥有的当前活动的连接个数至少达到 MIN_CONNS）的情况下，Dispatcher 将创建一个新的服务器进程。

如果某服务器进程被意外地取消，例如被 UNIX 系统 `kill` 命令删除，当新的连接到来时，Dispatcher 仍然会创建新的服务器进程。

有关 Dispatcher 配置方面的信息，请参阅第 106 页 “Dispatcher 配置文件”。

启动和停止 Dispatcher

启动 Dispatcher 时，请执行下列命令：

```
imsimta start dispatcher
```

这个命令涵盖和废弃任何其他的 `imsimta start` 命令，即此前被用来启动 Dispatcher 被配置来对之进行管理 MTA 组件的命令。特别需要指出的是，不应再使用 `imsimta start smtp`。任何执行被废弃命令的尝试会导致 MTA 发出警告信息。

若需关闭 Dispatcher，请执行下列命令：

```
imsimta stop dispatcher
```

在 Dispatcher 被关闭的情况下服务器进程会发生什么事情，取决于底层的 TCP/IP 包。如果修改了应用于 Dispatcher 的 MTA 配置或选项，则必须重新启动 Dispatcher，以便使新的配置或选项生效。

重新启动 Dispatcher 时，请执行下列命令：

```
imsimta restart dispatcher
```

重新启动 Dispatcher 具有关闭当前运行的 Dispatcher，然后立即启动一个新的 Dispatcher 的效果。

重写规则

重写规则用于确定下列：

- 如何将一地址中的域部分重写为适当的或相应的格式。
- 地址被重写后，邮件应排入哪个通道的队列。

每个重写规则由一个*模式*和一个*模板*的组成。模式一个字串，用于与地址的域部分匹配。模板则指定若域部分匹配成功须采取的行动。它由两个部分组成：1）一组指示如何重写地址的指令（也就是一个控制字符串）和 2）邮件将发往的通道的名称。地址重写后，邮件排入目标通道队列，以便传递给既定的收件人。

下面是一个重写规则的例子：

```
siroe.com               $U%$D@tcp_siroe-daemon
```

`siroe.com` 是域模式。任何其地址中包含 `siroe.com` 的邮件都将按照模板指令（`$U%$D`）被重写。`$U` 指定重写地址使用相同的用户名。% 指定重写地址使用相同的域分隔符。`$D` 指定重写地址使用与模式中已匹配域名相同的域名。`@tcp_siroe-daemon` 指定邮件与其重写地址一起被发往称为 `tcp_siroe-daemon` 的通道。更多详细信息请参阅第 7 篇，“配置重写规则”。

有关配置重写规则方面的详细信息，请参阅第 91 页 “MTA 配置文件”以及第 7 篇，“配置重写规则”。

通道

通道是处理邮件的基本 MTA 组件。通道表示与另一部计算机系统或一组计算机系统的连接。一个通道与另一个通道之间在实际硬件连接或软件传送方面有很大的差异，或者两方面都有很大差异。

通道具有如下功能：

- 向远程系统发送邮件，在邮件发出后从队列中将其删除。
- 从远程系统接收邮件，并将邮件放置在适当的通道队列中。
- 向本地邮件存储库传递邮件。
- 向处理程序传递邮件以进行特殊的处理。

邮件在进入 MTA 时由通道排入队列，送出时离开队列。邮件通常从一个通道进入，而从另一个通道送出。通道可使邮件离队，然后处理该邮件，或者将该邮件列入另一 MTA 通道的队列。

主程序与从属程序

通常 （但不总是）一个通道与两个程序相关联：主程序与从属程序。从属程序从另一个系统接受邮件并将它们添加到一个通道邮件队列中。主程序将邮件从通道传输到另一个系统。

例如 SMTP 通道，它具有发送邮件的主程序以及接收邮件的从属程序。这两个程序分别为 SMTP 的客户程序与服务器。

主通道程序通常负责由 MTA 启动的外发连接。主通道程序：

- 在本地提出处理请求时开始运行。
- 从通道邮件队列中将邮件出队。
- 如果目标格式与队列中邮件的格式不同，可按需要进行地址、标题及内容转换。
- 启动邮件的网络传输。

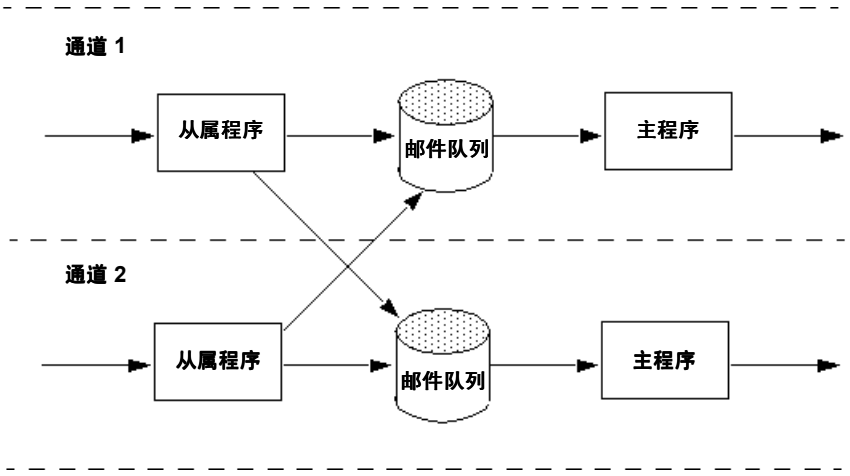
从属通道程序通常接收外来的连接，即 MTA 对外部请求的应答。从属通道程序：

- 在出现外部事件或本地请求时开始运行。
- 将邮件排入通道的队列。目标通道的确定是将信封地址传递给一重写规则而实现的。

例如，图 5-3 中有两个通道程序，Channel 1 和 Channel 2。假定 Channel 1 中的从属程序从远程系统收到一封邮件。从属程序检查地址，根据需要应用重写规则，然后根据重写地址将邮件排入适当的通道邮件队列中。

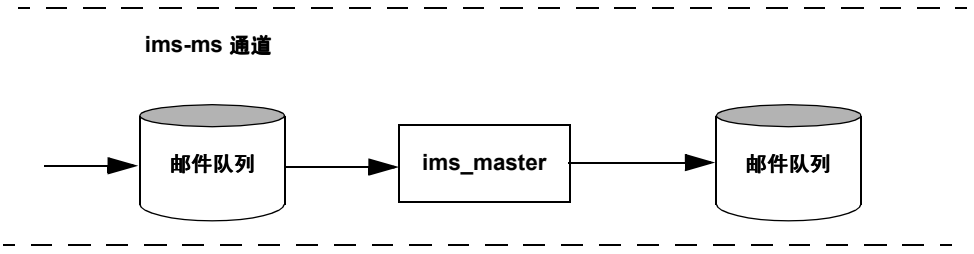
主程序从队列中取出邮件，然后在网络上传输该邮件。注意，主程序只能从自己的通道队列中取出邮件。

图 5-3 主程序与从属程序



虽然典型的通道同时有主程序和从属程序，但有的通道也可能只有从属程序*或*只有主程序。例如，由 Messaging Server 提供的 `ims-ms` 通道就只有一个主程序，因为该通道只负责将邮件取出队列并送往本地邮件存储库，如图 5-4 所示。

图 5-4 ims-ms 通道



通道的邮件队列

所有通道都有相关的邮件队列。当一封邮件进入邮件系统时，从属程序决定该邮件排入哪个邮件队列。排入队列的邮件存储在通道队列目录下的邮件文件中。默认情况下，这些目录存储在下列位置：*/server_instance*`/imta/queue/`*channel*`/*`。

通道定义

通道定义位于 MTA 配置文件 imta.cnf 的下半部分，重写规则的后面 （请参阅第 91 页“MTA 配置文件”）。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定义的开始。

一个通道定义应包括此通道的名字，后面跟着定义通道配置的关键字选项列表，以及一个独特的通道标记，即在重写规则中用来将邮件路由到该通道的标记。通道定义之间用一空行隔开。通道定义内可以有注释，但不能出现空行。

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

通道定义作为一个整体称为通道主表。单独的通道定义也称作通道块。例如，图 5-5 中的通道主表包括三个通道定义或通道块。

图 5-5　　简单配置文件 - 通道定义

```
! 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
```

典型的通道条目看起来像：

```
tcp_intranet smtp mx single_sys subdirs 20 noreverse maxjobs 7
SMTP_POOL maytlsserver allowswitchchannel saslswitchchannel
tcpauth
tcpintranet-daemon
```

第一个词，如此例中的 `tcp_intranet`，是通道名称。最后一个词，如此例中的 `tcpintranet-daemon`，称为*通道标记*。通道标记是被重写规则用来为邮件定向的名称。在通道名称和通道标记之间的那些词称为通道*关键字*，用以描述如何处理邮件。数百个不同的关键字使邮件可得到不同方式处理。在 **iPlanet Messaging Server Reference Manual** 和第 8 篇，“配置通道定义”中有通道关键字的完整清单和描述。

通道主表用于定义 Messaging Server 能够使用的通道以及与每个通道相关联的系统名称。

在 UNIX 系统中，文件中的第一个通道块总是说明本地通道，即 `l`。（一个例外是 `defaults` 通道，它能够出现在本地通道的前面。）本地通道用于做路由决定和传输由 UNIX 邮件程序发送的邮件。

也可以在 MTA 选项文件 `option.dat` 中设置全局通道选项，或者在某个通道选项文件中为一个特殊通道设置选项。有关选项文件的详细信息，请参阅第 107 页 “选项文件”和第 106 页 “TCP/IP（SMTP）通道选项文件”。有关配置通道的详细信息，请参阅第 8 篇，“配置通道定义”。有关建立 MTA 通道的详细信息，请参阅第 91 页 “MTA 配置文件”。

MTA 目录信息

对于每个被处理的邮件，MTA 都需要访问有关用户、用户组及其所支持的域的目录信息。这些信息均保存在 LDAP 目录服务中。MTA 有两种方法访问这样的信息。第一种方法是直接读取 LDAP 目录。这称为*直接 LDAP 模式*，在附录 B，“MTA 直接 LDAP 操作”中有完整的描述。第二种方法，同时也是默认的方法，是通过*目录缓存*访问目录信息。这称为 `dirsync` 模式。

在 `dirsync` 模式中，对 MTA 所使用的用户和用户组的目录信息的访问是通过统称为目录缓存的一系列文件和数据库进行的。数据本身存储在 LDAP 目录，但是实际信息是从缓存中读取的。缓存中的数据被 `dirsync` 程序更新，该程序监视 LDAP 目录的变动并相应地更新有关的文件和数据库。

有关 `dirsync` 操作和配置的细节在第 93 页 “dirsync 配置”中有详细描述。

作业控制器

每当邮件排入通道的队列时，作业控制器可确保有一项传递邮件的作业在运行。这可能涉及到启动新的作业进程、添加线程，或者仅标示出已有一项作业在运行。若因到达在通道或者处理池方面的作业限制而导致作业无法启动，工作控制器将一直等待直到另一个工作结束。当作业限制不再被超越时，作业控制器就启动另一个作业。

这些通道作业在控制器内的处理池中运行。一个处理池可以理解为运行通道作业的 “地方”。处理池提供了一个计算区域，供一组作业进行操作而又不与处理池以外的作业竞争资源。有关处理池的更多信息请参阅第 108 页“作业控制器文件”和第 187 页“通道执行任务的处理池”。

通道的任务限制时由通道关键字 maxjobs 决定的。处理池的任务限制则由处理池选项 JOB_LIMIT 决定。）

Messaging Server 通常尝试立即传递所有邮件。如果一邮件没能在第一次尝试时被传递出去，那么该邮件将被延迟一段由适当的 backoff 关键字所指定的时间。一旦过了由 backoff 关键字指定的时间，被延迟的邮件就可以传递了，并且如有必要会启动一个通道任务来处理该邮件。

作业控制器的正处理邮件和待处理邮件的内存中的数据结构，反映出存储在磁盘中的 MTA 队列区域中的邮件文件的完整集合。但是，如果磁盘中待处理邮件文件增大到超过作业控制器内存数据结构的大小限制时，作业控制器将只在内存中跟踪所有磁盘邮件文件的一个子集。作业控制器只处理在内存中被跟踪的那些邮件。当传递了大量的邮件从而释放了足够的内存之后，作业控制器通过扫描 MTA 队列区域来更新其邮件列表并自动刷新相应的内存存储。然后作业控制器开始处理这些刚从磁盘中检索到的其他邮件文件。作业控制器自动对 MTA 队列区域进行这些扫描。

如果一站点总是面临大量的待处理邮件，恐怕就需要使用 MAX_MESSAGES 选项来调整作业控制器。增大 MAX_MESSAGES 选项的值可使作业控制器使用更多的内存，从而可降低待处理邮件流量溢出作业控制器内存缓存情况的发生次数。这样做将减少作业控制器必须扫描 MTA 队列目录所付出的开销。但是请记住，当作业控制器确实需要重新构建内存缓存时，处理过程将因为缓存的增大而变长。同样需要说明的是，由于每次启动或重新启动作业控制器时都必须扫描 MTA 队列目录，相对于没有待处理邮件，大量的待处理邮件意味着在启动或重新启动作业控制器时将导致更多的额外开销。

作业控制器同样可以运行若干周期性的作业。这样的作业在作业控制器配置中配置，而不是使用更为普通的如 cron 这样的工具，这会使作业调度依赖于作业控制器的启动和运行。对于高实效性设置来说，要考虑到 “故障在线恢复”（failover）。

有关处理池和作业控制器配置的信息，请参阅第 108 页 “作业控制器文件”和第 184 页 “配置邮件处理和传递”。

启动和停止作业控制器

启动作业控制器时，请执行下列命令：

```
imsimta start job_controller
```

关闭作业控制器时，请执行下列命令：

```
imsimta stop job_controller
```

重新启动作业控制器时，请执行下列命令：

```
imsimta restart job_controller
```

重新启动作业控制器具有关闭当前运行的作业控制器、然后立即启动一个新的作业控制器的效果。

第 6 篇

关于 MTA 服务与配置

本章描述一般 MTA 服务和配置。有针对性的或详细解释，请见其它有关章节。本章包括以下各节：

- MTA 配置文件
- `dirsync` 配置
- 映射文件
- 其它 MTA 配置文件
- 别名
- 命令行实用工具
- SMTP 的安全性和访问控制
- 日志文件
- 将内部格式地址转换为公共格式地址
- 控制传递状态通知邮件

MTA 配置文件

MTA 的主配置文件是 `imta.cnf`。在默认设置下，这个文件可在 *instance_root*`/imta/config/imta.cnf` 中找到。该文件包含 MTA 通道定义及通道重写规则。与重写目标地址相关联的通道此时成为目标通道。

本节将就 MTA 配置文件作简要介绍。有关配置重写规则以及构成 MTA 配置文件的通道定义的细节，请参阅第 7 篇，“配置重写规则”和第 8 篇，“配置通道定义”。

通过修改 MTA 配置文件，您可在站点上建立在用通道，并可通过重写规则确立哪个通道负责哪种类型的地址。配置文件可用来建立电子邮件系统的布局，方法是：指定可用的传送方法（通道）和可将地址类型与适当的通道相关联的传送路由 （重写规则）。

配置文件包含两部分：域重写规则和通道定义。域重写规则在文件中最先出现，并与通道定义以一个空行隔开。通道定义统称为通道表。单独的通道定义组成通道块。

下面是 `imta.cnf` 配置文件的例子，说明如何使用重写规则将邮件路由到适当的通道。为了使例子尽可能的简单，在此没有使用域名。重写规则出现在配置文件的上半部分，接下来在配置文件的下半部分是通道定义。

图 6-1 简单的 MTA 配置文件

```
! 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

</usr/iplanet/server5/msg-tango/table/internet.rules (6)
```

下面的列表解释了前面配置文件中的几个关键项目（用黑体数字标注，用括弧括起的部分）：

1. 感叹号（!）表示注释行。感叹号必须出现在第一列。在其他任何地方出现的感叹号解释为*常值*感叹号。
2. 重写规则出现在配置文件的前半部分。在重写规则的行间不能出现空行。允许有注释行（在第一列以感叹号开始）。
3. 出现在文件中的第一个空行意味着重写规则部分的结束和通道块的开始。这些定义统称为*通道驻留表*，用来定义 MTA 可以使用的通道和与每个通道相关联的名称。
4. 第一个要出现的通道块通常是本地块通道，或称为 `l` 通道。此后，空行将各个通道块相互隔开。（例外情况是 `defaults` 通道，它可以出现在 `l` 通道的前面）。
5. 典型的通道定义包括一个通道名（`a_channel`），定义通道配置的一些关键字（`defragment charset7 usascii`）和路由系统（`a-daemon`），也称为*通道标记*。
6. 可以将其他文件的内容包含在配置文件中。如果某行的第一列是一个小于号（<），则该行的其余部分视为文件名；该文件名应当总是具有绝对的和完整的路径。该文件被打开，其内容在那一点处插入到配置文件中。包含文件最高可以嵌套深达 3 层。包含于配置文件中的任何文件必须是世界可读的，正如配置文件是世界可读的一样。

表 6-1 所示为一些示例地址是如何通过前述配置发送的。

表 6-1　地址和与之相关的通道

地址	入队通道
u@a	a_channel
u@b	b_channel
u@c	b_channel
u@d	a_channel

有关 MTA 配置文件的详细说明，请参见第 84 页 “重写规则”、第 87 页 “通道定义”和第 7 篇，“配置重写规则”。

dirsync 配置

默认的 Messaging Server 安装使用 dirsync 运行模式。（另一个选择是使用直接 LDAP 模式，有关说明见附录 B，“MTA 直接 LDAP 操作”。）在 dirsync 模式下，MTA 缓存目录信息并通过访问缓存获得所需数据，而不是每处理一封邮件就查询目录服务。

在目录服务中存储的目录信息是由称作 dirsync 的程序持续更新的。结果是，目录缓存必须定期地，也就是同步地，利用目录服务中的当前目录信息进行更新。同步类型有两种：

- **完整同步** - 用新缓存替换现有的缓存，从目录服务中用当前用户与组条目彻底重建缓存。在这种同步发生后，系统将重新建立 MTA 配置文件，然后自动重新启动 MTA。
- **递增同步** - 用上一次完整同步或递增同步以来创建或修改的用户及组条目更新现有的缓存。 MTA 不重新启动。

在默认设置下， MTA 目录缓存在每日凌晨 02:00:00 进行完整同步，每 10 分钟进行一次递增同步。

表 6-2 所示为全目录同步和部分目录同步时发生的更新情况。

表 6-2　MTA 目录高速缓存更新

MTA 目录高速缓存更新	完整同步	递增同步
添加新用户条目	是	是
更新已修改的用户条目	是	是
* 去除已删除的用户条目	是	否
新成员加入到现有分配列表	是	是
删除的成员已从现有分配列表中去除	是	是

表 6-2　MTA 目录高速缓存更新（接上页）

MTA 目录高速缓存更新	完整同步	递增同步
添加新的分配列表	是	是
* 去除已删除的分配列表	是	否

* 若需递增目录同步考虑到被删除条目，则必须首先将条目的状态标记为已删除。在执行了递增同步后，MTA 认为这些用户或组已不存在。只有在递增同步后才能进行真正的目录条目的移除。

目录同步通常是自动发生的。然而，如有需要，可用 `imsimta dirsync` 命令重新创建或更新 MTA 目录的高速缓存。若需有关 `imsimta dirsync` 命令的更多信息，请参见 **iPlanet Messaging Server Reference Manual**。

目录同步配置参数

表 6-3 列出了目录同步所需的配置参数。

表 6-3　目录同步配置参数

参数	说明
`local.imta.ldsearchtimeout`	当搜索用户与邮件列表信息时，可指定 LDAP 搜索超时。默认设定为无超时。
`local.imta.hostnamealiase`	在检查 LDAP 条目的 `mailhost` 或 `mailRoutingHosts` 属性以确定其是否为本地时，`dirsync` 进程使用 `local.hostname` 参数进行比较。另外，用逗号分隔的主机别名列表可以通过 `local.imta.hostnamealiases` 参数提供。此后，`dirsync` 进程将使用在这两个参数中提供的所有主机名检查条目是否为本地。
`local.imta.mailaliases`	在默认设置下，MTA 认为只有 `mail` 和 `mailAlternateAdress` 的 LDAP 属性为可路由的电子邮件地址。另外，也可通过 `local.imta.mailaliases` 参数提供用逗号分隔的 LDAP 属性列表。这个列表将改写默认属性。例如，MTA 在路由邮件时将考虑下列四个属性： `local.imta.mailaliases=mail,mailAlternateAddress, rfc822mailbox,rfc822mailalias`

表 6-3　目录同步配置参数（接上页）

参数	说明
local.imta.ugfilter	这个参数可用来设置 LDAP 搜索过滤器，即 dirsync 在搜索用户和邮件列表信息时使用的过滤器。 默认过滤器是 （objectClass=inetLocalMailRecipient）。 例如，如果只考虑与 inetLocalMailRecipient AND myispSubscriber 对象类相关的 LDAP 条目，应将这个参数设置为： local.imta.ugfilter=(&(objectClass=inetLocalMailRecipient)(objectClass=myispSubscriber)) 注意：在递增同步的情况下，一个时间戳过滤器会添加到这个过滤器中。因此，您需要将自定义过滤器用 （） 包裹起来。
local.imta.statssamplesize	如果作了设置，这个参数指示 dirsync 在标准输出设备上输出概要信息，包括用户数、从开始以来的累计邮件列表条目数以及以条目 / 秒为单位的平均速率。用户与邮件列表无论是否成功同步均计算在内。
local.imta.reverseenabled	触发生成反转数据库。默认值是 yes。反转数据库的实际使用是由 USE_REVERSE_DATABASE 选项控制的。
local.imta.ssrenabled	触发生成服务器端规则 （SSR）数据库。默认值是 yes。 SSR 数据库的实际使用是由 ssr 通道关键字控制的。
local.imta.vanityenabled	控制是否启用空域 （msgVanityDomain 用户 LDAP 属性）。默认值是 yes。
local.imta.catchallenabled	控制是否启用 catchall 地址 （形如 @domain 的 mail 或 mailAlternateAddress）。默认值是 yes。
local.imta.scope	这个参数可指示 dirsync 应该与哪个条目同步： 仅对其 mailhost 属性为本地主机的用户和邮件列表条目进行缓存处理：value = "local"。 对所有用户和邮件列表条目都进行缓存处理，无论其 mailhost 属性是什么：value = "domains"。这是参数缺失情况下的默认值。 不对任何域、用户或邮件发送列表进行缓存处理：value = "nobody"

映射文件

许多 MTA 组件都使用面向查找表的信息。这种类型的表是用于将一个输入串转换 （也即*映射*）为一个输出串。这样的表，称为*映射表*，通常以两列形式呈现。第一 （左）列提供可能的匹配时需参照的输入串 （模式），第二 （右）列给作为输入串映射结果的输出串 （模板）。

大多数 MTA 数据库 - 包含不同类型的 MTA 数据的数据库，不要与映射表混淆 - 恰恰是这种类型的表的例子。然而， MTA 数据库文件并不提供通配符查找功能，这是由于查找通配符匹配项时要扫描整个数据库，因此这一方法本身的效率极低。

MTA 映射文件支持多重映射表。还提供通配符功能，以及多级和迭代的映射方法。与用数据库相比，这一方法更适合密集计算之环境，在条目数量大的情况下尤其如此。然而，这一维护方面的灵活性实际上可免除使用等效数据库中大多数条目之必要，因此很可能因而降低系统的总体开销。

表 6-4 列出了本文描述的映射表。

表 6-4　iPlanet Messaging Server 映射表

映射表	页	说明
CHARSET-CONVERSION	229	用于指定可以做哪种类型的通道对通道的字符集转换和邮件重格式化。
COMMENT_STRINGS	197	用于修改地址头注释 （括弧括起来的字符串）。
CONVERSIONS	216	用于选择转换通道的邮件流通量。
"domain lookup"	422	用于寻找在直接 LDAP 模式下搜索别名的树基。
FORWARD	118	用于执行转发，类似于使用别名文件或别名数据库所执行的转发。
FROM_ACCESS	236	可根据信封的 “发件人” 地址过滤邮件。如果收件人地址不相关，可使用此表。
INTERNAL_IP	245	用于识别内部系统和子网络。
MAIL_ACCESS	236	用于根据在 SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息阻塞外来的连接。
NOTIFICATION_LANGUAGE	119	用于定制或本地化通知邮件。
ORIG_MAIL_ACCESS	236	用于根据在 ORIG_SEND_ACCESS 和 PORT_ACCESS 表中找到的组合信息阻塞外来的连接。
ORIG_SEND_ACCESS	236	可根据信封的 “发件人” 地址、信封的 “收件人” 地址、源和目标通道用来阻塞外来的连接。
PERSONAL_NAMES	197	用于修改个人姓名 （用尖括弧定界的地址前的字符串）。
PORT_ACCESS	236	可根据 IP 号阻塞外来的连接。
REVERSE	115	用于将地址从内部的形式转换为公共、通告之形式。
SEND_ACCESS	236	可根据信封的 “发件人” 地址、信封的 “收件人” 地址、源和目标通道用来阻塞外来的连接。
X-ATT-NAMES	222	用于从映射表中检索一个参数值。

定位和装载映射文件

映射表保留在 MTA 映射文件中。这是用 MTA tailor 文件中的 IMTA_MAPPING_FILE 选项指定的文件；在默认设置下，该文件为 *server_root*/msg-*instance*/imta/config/mappings。系统将映射文件的内容合成到编译配置。

映射文件应当是世界可读的。若不允许映射文件成为世界可读的文件，则会导致不确定的行为。

映射文件中的文件格式

映射文件是由一系列单独的表组成的。每个表以其表名作为开头。表名的在第一列的字符总是字母。跟在表名后面的是一个必须有的空行，随后是表中的各个条目。条目由零或多个首行缩排的行组成。每个条目行包括两列，是由一个或多个空格或制表符隔开的。任何在条目中的空格都必须用 $ 字符引起来。空行必须在每个映射表名之后和各个映射表之间出现；在一个单独的表的条目间则不能出现空行。注释行用位于第一列的惊叹号 （!）表示。

形成的格式类似于如下：

```
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 的应用程序将字符串 pattern2-2 映射到任何由 template2-2 模板指定的地方。每个模式或模版最多可以包含 252 个字符。映射表中的条目没有数量限制（尽管过多的条目可能消耗大量的 CPU 时间和过多的内存）。长行 （超过 252 个字符者）可以通过使用反斜杠 （\）结尾来续行。在两列间和在第一列前的空白不能省略。

映射文件中不得有重复的映射表名。

在映射文件中包含其它文件

映射文件中可以包含其它文件。可以用如下格式的行做到这一点：

```
<file-spec
```

这样的行有效地将 file-spec 文件的内容替换到映射文件中包含操作出现之处。文件限定应当包括一个完整的文件路径 （目录，等等） 。所有以这种方式包含的文件必须是世界可读的。在这样的被包含的映射文件中也允许有注释。文件包括可嵌套深至 3 层。包含文件与映射文件同时装载 - 它们不是根据需要而装载的，所以在使用包含文件时不涉及性能改进或内存节省问题。

映射操作

在映射文件中的所有映射都是以一致的方法应用的。一个映射与另一个映射的唯一不同是输入字符串源和映射输出的用途。

映射操作总是以一个输入字符串和一个映射表开始。映射表中的条目是按照它们在表中出现的顺序，从顶部到底部一次一个进行扫描的。每个条目的左侧用作模式，并且输入字符串是以大小写不区分的方式与该模式进行比较的。

映射条目模式

模式可包含通配符。特别是，常规的通配符是允许的：星号 （*）与零或更多字符相匹配，每个百分比符号（%）与单个字符相匹配。星号、百分比符号、空格和制表符可通过在其前面加美元符号 （$）而被引起来。引起来的星号或百分比符号丧失其任何特殊的含义。空格或制表符必须引起来以防止它们过早地结束模式或模板。本意的美元符号应当加倍（$$），第一个美元符号用于将第二个引起来。

表 6-5　映射模式通配符

通配符	说明
%	完全匹配一个字符。
*	使用最大或 “贪心的”从左到右匹配方式匹配零个或多个字符。
反匹配	**说明**
$ n*	匹配第 n 个通配符或 glob。
修饰符	**说明**
$_	使用最小或 “惰性”从左到右匹配方式。
$@	关闭相继的通配符或 glob 的 “保存”。
$^	打开相继的通配符或 glob 的 “保存”；此为默认设置。
Glob 通配符	说明

表 6-5　映射模式通配符（接上页）

$A%	匹配一个字母字符， A-Z 或 a-z。
$A*	匹配零个或多个字母字符， A-Z 或 a-z。
$B%	匹配一个二进制数字 （0 或 1）。
$B*	匹配零个或多个二进制数字 （0 或 1）。
$D%	匹配一个十进制数字 0-9。
$D*	匹配零个或多个十进制数字 0-9。
$H%	匹配一个十六进制数字 0-9 或 A-F。
$H*	匹配零个或多个十六进制数字 0-9 或 A-F。
$O%	匹配一个八进制数字 0-7。
$O*	匹配零个或多个八进制数字 0-7。
$S%	匹配一个符号集中的字符，例如 0-9、 A-Z、 a-z、 _、 $。
$S*	匹配零个或多个符号集中的字符，即 0-9、 A-Z、 a-z、 _、 $。
$T%	匹配一个制表符、垂直制表符或空格字符。
$T*	匹配零个或多个制表符、垂直制表符或空格字符。
$X%	与 $H% 同义。
$X*	与 $H* 同义。
$[c]%	匹配字符 c。
$[c]*	匹配任意次出现的字符 c。
$[c_1 c_2 ... c_n]%	匹配恰好一次出现字符 c_1、 c_2 或 c_n。
$[c_1 c_2 ... c_n]*	匹配任意次出现的任意字符 c_1、 c_2 或 c_n。
$[c_1 -c_n]%	匹配从 c_1 到 c_n 范围内的任意一个字符。
$[c_1 -c_n]*	匹配从 c_1 到 c_n 范围内的任意次出现的字符。
$< IPv4>	匹配一个 IPv4 地址，忽略位。
$(IPv4)	匹配一个 IPv4 地址匹配，保持前缀位。
${IPv6}	匹配一个 IPv6 地址。

在 globs 中，即在一个 `$[...]` 构造中，反斜杠字符为字符引号。若要在 glob 中表示一个连字号 –，或右方括弧]，连字号或右方括弧必须前加反斜杠引起来。

在模式中的所有其他字符只代表和匹配其自身。特别是，单引号、双引号字符以及及圆括弧在映射模式和模板中都没有什么特殊含义，它们只是普通的字符。这使书写对应于非法地址和部分地址的条目更简单。

要指定多个修饰符，或指定修饰符和反匹配，语法格式中只使用一个美元符号例如，要反匹配初始通配符，而不保存反匹配自身，应使用 $@0，而不是 $@$0。

请注意 imsimta test -match 实用程序可以用于测试映射模式，尤其是测试通配符在模式中的效果。

星号通配符通过贯穿模式的从左到右的工作方式，使其匹配最大化。例如，当字符串 a/b/c 与模式 */* 进行比较时，左星号与 a/b 相匹配，右星号与剩下 c 匹配。

$_ 修饰符使通配符的匹配为最小化，也就是在贯穿模式的从左到右的工作中，只考虑最少可能的匹配。例如，当字符串 a/b/c 与模式 $_*/$_* 进行比较时，左侧的 $_* 与 a 相匹配，右侧的 $_* 与 b/c 相匹配。

IP 匹配

在 IPv4 前缀匹配的情况下，须指定 IP 地址或子网络，并可选择后跟一个斜杠和一个数字，用来表示进行匹配比较时前缀的有效位数。例如，下列地址与子网络 123.45.67.0 中的任何地址相匹配：

```
$(123.45.67.0/24)
```

在 IPv4 忽略位匹配的情况下，须指定 IP 地址或子网络，并可选择后跟一个斜杠和一个数字，表示进行匹配检查时忽略的位数。例如，下列地址与子网络 123.45.67.0 中的任何地址匹配：

```
$<123.45.67.0/8>
```

下列示例与从 123.45.67.4 到 123.45.67.7 范围内的任何地址相匹配。

```
$<123.45.67.4/2>
```

IPv6 匹配与 IPv6 地址或子网络相匹配。

映射条目模板

如果在给定的条目中模式的比较失败，不会采取行动，继续进行下一个条目的扫描。如果比较成功，条目的右侧被用作一个模板以产生一个输出字符串。该模板有效地促使根据模板给出的指令所构建的输出串来替换输入串。

在模板中的几乎所有字符在输出中都产生其自身。例外之一是美元符号 （$）。

美元符号后跟一美元符号、空格或制表符在输出字符串中产生美元符号、空格或制表符。请注意，所有这些字符必须引起来，以便插入到输出字符串中。

美元符号后跟一数字 *n* 调用一置换；美元符号后跟一字母被称为 “元字符”元字符本身并不出现在模板产生的输出字符串中，但产生一些特殊的置换或处理。参见表 6-6 中的特殊置换和标准处理元字符列表。任何其他元字符是为针对特定映射的应用程序保留的。

请注意，如果元字符 $C，$E，$L 或 $R 中的任意一个在某个匹配模式的模板中出现，会影响映射过程并控制是终止还是继续。也就是说，设置迭代的映射表条目是可能的：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中不包含元字符 $C，$E，$L 或 $R 中的任何一个，则假定为 $E （立即终止映射过程）。

贯穿映射表的迭代检查是有限制的，以防止无限循环。在每次重新启动一检查时，若相关模式的长度与前一次检查时相同或更长，计数器就增 1。如果字符串的长度比前一次短，则计数器重置为零。在计数器已超过 10 后要求再次迭代一映射是不允许的。

表 6-6　映射模板置换和元字符

置换序列	置换
$n	从 0 开始从左向右计数的第 *n* 个通配字段。
$#...#	序列数置换。
$]...[	LDAP 搜索 URL 查找；置换结果。
$|...|	将指定映射应用到提供的串。
${...}	常规数据库置换。
$[...]	调用站点提供的例程，置换结果。
元字符	**说明**
$C	继续开始下一个表条目的映射过程，使用此条目的输出串作为该映射过程的新输入串。
$E	现在就结束映射过程，使用此条目的输出字符串作为映射过程的最终结果。
$L	继续开始下一个表条目的映射过程，使用此条目的输出串作为该映射过程的新输入串；当表中的所有条目用尽后，从第一个表条目开始进行再一次的检查。随后的带有 $C、 $E 或 $R 等元字符的匹配可不受此条件限制。
$R	继续第一个映射表条目开始的映射过程，使用此条目的输出串作为该映射过程的新输入串。
$?x?	映射条目已耗用百分之 x 的时间。
$\	强制随后文本改为小写。
$^	强制随后文本改为大写。
$_	保留随后文本原有的大小写。
$:*x*	只在设置了指定标志时匹配。
$;*x*	只在清除了指定标志时匹配。

通配符字段置换 （$n）

美元符号后跟一数字 n 将被与模式中第 *n* 个通配符相匹配的材料所置换。通配符从 0 开始编号。例如，下列条目将与输入串 PSI%A::B 相匹配并产生作为结果的输出串 b@a.psi.siroe.com：

```
PSI$%*::*     $1@$0.psi.siroe.com
```

输入串 PSI%1234::USER 也将匹配产生 USER@1234.psi.siroe.com 作为输出串。输入串 PSIABC::DEF 将不与此条目中的模式相匹配并将不采取行动，即此条目不产生输出串。

控制文本大小写 （$\， $^， $_）

元字符 $\ 强制随后文本改为小写，$^ 强制随后文本改为大写，而 $_ 使随后文本保留其原有的大小写。例如，这些元字符在使用映射转换大小写有意义的地址时可能很有用。

过程控制 （$C， $L， $R， $E）

$C， $L， $R 和 $E 等元字符影响映射过程，控制是否和何时终止映射过程。元字符：

- $C 的作用是使映射过程在下一个条目继续，使用当前条目的输出串作为该映射过程的新输入串。
- $L 的作用是使映射过程在下一个条目继续，使用当前条目的输出串作为该映射过程的新输入串，而且，如果没有找到匹配的条目，从第一个表条目开始再进行一次检查，带有 $C、 $E 或 $R 等元字符的随后的匹配条目不受此条件限制。
- $R 的作用是使映射过程从映射表的第一个条目继续，使用当前条目的输出串作为该映射过程的新输入串。
- $E 的作用是使映射过程终止；此条目的输出串是最终输出。 $E 是默认设置。

映射表模板是从左到右扫描的。若要为可能 “成功”或 “失败”的条目设置 $C， $L 或 $R 标记 （例如，常规数据库置换或随机值控制条目），需将 $C、 $L 或 $R 元字符放置在条目的可能成功或失败部分的左边，否则，如果如果该条目的其他部分失败，标记是看不见的。

条目随机成功或失败 （$?x?）

在映射表条目中的元字符 $?x? 的作用是使该条目在百分之 *x* 时间的里 “成功”；其余的时间，条目 “失败”并且映射条目输入的输出保持不变作为输出。（请注意，条目失败的效果根据映射的情况，并不一定与在第一位置未匹配的条目相同。）*x* 应当是指定成功百分比的实数。

例如，假设一个 IP 地址为 123.45.6.78 的系统正向您的站点发送稍多一些的 SMTP 邮件，而您希望使其慢下来，则可以按下列方法使用 PORT_ACCESS 映射表。假设您希望只允许其中 25% 的连接尝试通过，而拒绝其他的 75% 的连接尝试。下面的 PORT_ACCESS 映射表使用 $?25? 以使带有 $Y （接受连接）的条目仅在 25% 的时间里成功；在其他 75% 的时间里，该条目失败，在条目中的初始 $C 使得 MTA 从下一个条目继续映射，这就造成连接尝试被拒绝并带有 SMTP 错误和这样的讯息：请稍候再试。

```
PORT_ACCESS

  TCP|*|25|123.45.6.78|*          $C$?25?$Y
  TCP|*|25|123.45.6.78|*          $N45s$ 4.40$ Try$ again$ later
```

序列号置换 （$#...#）

$#...# 置换增加在 MTA 序列文件中的储存的值，并将该值置换到模板中。这可用于希望在映射表输出中有一个唯一限定词的情况下产生唯一的、增加的字符串；例如当使用映射表产生一系列文件名时。

允许的语法包括下列中的任何一个：

```
$#seq-file-spec|radix|width#
```

```
$#seq-file-spec|radix#
```

```
$#seq-file-spec#
```

必须的 *seq-file-spec* 参数是一个已存在的 MTA 序列文件的完整文件指定，其中，可选的 *radix* 和 *width* 参数分别指定输出序列值的基数（数制）和输出数字的位数。默认的基数为 10。在 36 到 36 的范围内的基数都是允许的；例如，基数 36 给出了以数字 0，...，9，A，...，Z 表示的值。在默认设置下，序列值是按照其自然的宽度打印的，但如果指定的宽度要求更多数字位，则输出值的左侧被填补以 0，以获得正确的数字位数。

请注意，如果明确指定了宽度，则基数也必须明确指定。

如前面所解释的，在映射中所参照的 MTA 序列文件必须已经存在。若要创建 MTA 序列文件，请使用如下 UNXI 命令：

```
touch seq-file-spec
```

或

```
cat >seq-file-spec
```

用映射表访问的序列文件必须是世界可读的，以便正常运行。要使用这样的序列数文件，还必须拥有一个 MTA 用户帐户 （在 `imta_tailor` 文件中的配置为 `nobody`）。

LDAP 查询 URL 置换， $]...[

具有 `$]`*ldap-url*`[` 形式的置换是被特别处理的。 *ldap-url* 被翻译为 LDAP 查询 URL，而 LDAP 查询的结果被置换。使用标准的 LDAP URL，省略了主机和端口；而主机和端口则利用 `LDAP_HOST` 和 `LDAP_PORT` 选项进行指定。也就是， LDAP URL 应被指定为：

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

其中显示在上面的方括弧 `[` 和 `]` 表示是 URL 的可选部分。 *dn* 是必需的，它是一个指定搜索基的判别名。 URL 的可选部分 *attributes*， *scope* 和 *filter* 进一步精细描述返回信息。也就是说，*attributes* 指定属性或从与此 LDAP 查询相匹配的 LDAP 目录条目返回的属性。*scope* 可以是 `base` （默认情况）， `one` 或 `sub` 中的任意一个。 *filter* 描述匹配条目的特性。

在 LDAP 查询 URL 中使用时，有某些可用的 LDAP URL 置换序列。

映射表置换 （$|...|）

具有 $| *映射* ;*argument*| 形式的置换是被特别处理的。 MTA 在 MTA 映射文件中查找名为 *映射* 的辅助映射表，并使用 *argument* 作为该命名的辅助映射表的输入。命名的辅助映射表必须存在，并且如果它是成功的，必须在其输出中设置 $Y 标记；如果命名的映射表不存在或不设置 $Y 标记，则该辅助映射表置换失败，而原有的映射条目被认为失败：原有输入串被用作输出串。

请注意，若要在进行映射表置换的映射表条目中使用诸如 $C， $R 或 $L 这样的过程控制元字符，过程控制元字符应被放置在映射表模板中映射表置换的左侧；否则映射表置换“失败”意味着过程控制元字符没有被看见。

常规数据库置换 （${...}）

据有 ${*text*} 形式的置换是被特别处理的。*text* 部分被用来作为访问常规数据库的密钥。此数据库是使用 imsimta crdb 实用程序生成的。如果在数据库中找到 *text*，数据库中的相应的模板将被置换。如果 *text* 与数据库中的任何条目都不匹配，则将输入串毫无改变地用作输出串。

如果常规数据库存在，它应该在世界范围内都是可读的，这样才能确保运转正常。

若要在进行常规数据库置换的映射表条目中使用诸如 $C，$R 或 $L 这样的过程控制元字符，过程控制元字符应被放置在映射表模板中常规数据库置换的左侧；否则常规数据库置换 “失败”意味着过程控制元字符没有被看见。

站点提供的例程置换 （$[...]）

具有 $[*图象*， *routine*， *argument*] 形式的置换是被特别处理的。 image， routine， argument 部分被用来查找并调用客户提供的例程。在 UNIX 运行环境下， MTA 使用 dlopen 和 dlsym 从共享库 *image* 动态装载和调用例程 *routine*。在 Windows NT 运行环境下，MTA 从动态链接库 *image* 调用例程 *routine*。例程 *routine* 于是作为带有下列参数列表的函数而被调用：

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

argument 和 result 分别为 252 字节长的字符串缓冲区。 argument 和 result 参数作为字符串的指针传递（例如，在 C 中，它们的类型应为 char*）。arglength 和 reslength 都是以引用传递的有符号的长整数。作为输入， argument 包含映射表模板中的 *argument* 字符串， arglength 则为该串的长度。作为返回，结果串应被置于 result 中，结果的长度应置于 reslength 中。然后，此结果串替代在映射表模板中的 $[image,routine,argument]。如果映射表置换失败， *routine* 例程返回 0，如果映射表置换成功则返回 -1。如果置换失败，通常将原输入串毫无改变地用作输出串。

如果要在进行站点提供的例程置换的映射表条目中使用诸如 $C， $R 或 $L 这样的过程控制元字符，过程控制元字符应放置在映射表模板中站点提供的例程置换的左侧；否则映射表置换“失败”意味着过程控制元字符没有被看见。

站点提供的例程调用机制使 MTA 的映射处理能以所有各种复杂的方法延伸。例如，在 PORT_ACCESS 或 ORIG_SEND_ACCESS 映射表中，可以调用执行某类装载监控服务，其结果用于决定是否接受连接或邮件。

站点提供的共享库图像 image 应当是世界可读的。

其它 MTA 配置文件

除 imta.cnf 文件外，iPlanet Messaging Server 还提供另外几个配置文件以帮助配置 MTA 服务。这些文件在表 6-7 中简要介绍。

表 6-7　　MTA 配置文件

文件	说明
自动回复选项文件	autoreply 程序所使用的选项。 *instance_root*/imta/config/autoreply_option
别名文件 （必备项）	用于实现在目录中不存在的别名。 *instance_root*/imta/config/aliases
TCP/IP （SMTP）通道选项文件（也称为 SMTP 选项文件）	用于设置具体通道选项。 *instance_root*/imta/config/*channel*_option
转换文件	用于转换通道控制邮件正文部分的转换。 *instance_root*/imta/config/conversions
Dirsync 选项文件 （只在以 dirsync 模式运行时必须）	dirsync 程序使用的选项。 *instance_root*/imta/config/dirsync.opt
Dispatcher 配置文件 （必备项）	Dispatcher 的配置文件。 *instance_root*/imta/config/dispatcher.cnf
作业控制器文件 （必备项）	Job Controller 使用的配置文件。 /*instance_root*/imta/config/job_controller.cnf
MTA 配置文件 （必备项）	用于地址重写、路由选择以及通道定义。 /*instance_root*/imta/config/imta.cnf
映射文件 （必备项）	映射表的资料档案库。 /*instance_root*/imta/config/mappings
选项文件	全局 MTA 选项文件。 /*instance_root*/imta/config/option.dat
Tailor 文件 （必备项）	指定位置和一些调整参数的文件。 /*instance_root*/imta/config/imta_tailor

自动回复选项文件

自动回复选项文件 autoreply_option 可用来设置自动回复 （或休假自动回复）程序的选项。详情请参见 **iPlanet Messaging Server Reference Manual**。

别名文件

别名文件 aliases，可用来设置没有在目录中设置的别名。根地址就是一个很好的例子。如果目录中存在的别名与此文件中设置的别名相同，则文件中的别名将被忽略。有关别名和 aliases 文件的详细信息，请参阅第 113 页 “别名”。

在完成对 aliases 文件的更改后，必须重新启动 MTA。

TCP/IP （SMTP）通道选项文件

TCP/IP 通道选项文件用于控制 TCP/IP 通道的各种特性。通道选项文件必须存储在 MTA 配置目录下，并命名为 *x*_option，这里的 *x* 是通道的名字。
例如，/*ServerInstance*/config/imta/tcp_local_option。有关详细信息，请参阅第 170 页 “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，请参阅 **iPlanet Messaging Server Reference Manual**。

转换文件

转换文件 conversions 用于指定转换通道如何对通过 MTA 的邮件执行转换功能。任何 MTA 通信流的子集都可以选来进行转换，任何程序集、命令过程都可以用来执行转换处理。MTA 将对转换文件进行检查，并为每个正文部分选择一个适当的转换功能。

有关本文件语法的详细信息，请参见第 214 页 “转换通道”。

Dirsync 选项文件

dirsync 选项文件 dirsync.opt 可为 dirsync 程序设置无法通过命令行方式设置的选项。详情请参见第 93 页 “dirsync 配置”和 **iPlanet Messaging Server Reference Manual**。

Dispatcher 配置文件

Dispatcher 配置文件 dispatcher.cnf 指定 Dispatcher 配置信息。在安装时，系统会创建一个默认的配置文件，该文件不作任何变动就可以使用。但是，如果因为安全或性能方面的原因想要修改默认配置文件，可以通过编辑 dispatcher.cnf 文件来实现。（有关的概念性信息请参见第 83 页 “Dispatcher”。）

Dispatcher 配置文件的格式与其它 MTA 配置文件格式相似。各行以如下形式指定选项：

option=value

option 是选项的名称， *value* 是所设置的选项的字符串或整数。如果 *option* 接受了一个整数 *value*，则可用 *b%v* 形式的计数法指定一个基数，其中 *b* 是表示数制的十进制数， *v* 则是用数制 *b* 表示的实际值。用这种方法指定的选项将按照服务项（即按下列选项设置所适用的服务）被分为若干节，使用下列形式的行列：

[SERVICE=*service-name*]

service-name 是某项服务的名称。在每节标志前面出现的所有初始选项定值适用于所有节。

下面是 Dispatcher 配置文件的一个示例（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=server_root/msg-instance/imta/lib/tcp_smtp_server
LOGFILE=server_root/msg-instance/imta/log/tcp_smtp_server.log
```

有关此文件参数的更多信息，参见 **iPlanet Messaging Server Reference Manual**。

映射文件

映射文件 mappings 用于定义 MTA 如何将输入字符串映射为输出字符串。

许多 MTA 组件都使用面向查找表的信息。一般来说，这类表用于将输入的字符串变换（即映射）为输出字符串。这种表称为映射表，一般有两列，第一列（左侧）给出可能的输入字符串，第二列（右侧）给出对应于输入字符串的输出字符串结果。多数 MTA 数据库都是这类映射表的实例。然而，MTA 数据库文件并不提供通配符查找功能，这是由于查找通配符匹配项时要扫描整个数据库，因此这一方法本身的效率极低。

映射文件向 MTA 提供了支持多个映射表的功能。它具有全面的通配符功能和多步映射方法以及交互式的映射方法。与用数据库相比，这一方法更适合密集计算之环境，在条目数量大的情况下尤其如此。然而，这一维护方面的灵活性实际上可免除使用等效数据库中大多数条目之必要，因此很可能因而降低系统的总体开销。

可用 imsimta test -rewrite 命令测试映射表。有关映射文件和 test -mapping 命令语法的更多信息，参见第 95 页 “映射文件”和 **iPlanet Messaging Server Reference Manual**。

选项文件

选项文件 option.dat 指定与特定通道选项相对的全局 MTA 选项。

您可用该选项文件全局性地取代应用于 MTA 的各种参数的默认值。特别是该选项文件可用于确定各种表的容量大小，即系统在读取配置文件和别名文件时须使用的各种表。也可用该选项文件限制 MTA 所接收邮件的大小，指定 MTA 配置所允许的通道个数，设置允许的重写规则个数等等。

有关该选项文件的语法的更多信息，参见 **iPlanet Messaging Server Reference Manual**。

Tailor 文件

Tailor 文件 `imta_tailor` 可用于设置各种 MTA 组件的位置。为使 MTA 正常工作，`imta_tailor` 文件必须永远驻留在 *server-instance*`/imta/config` 目录下。

虽然可以编辑这个文件以反映特定安装的变化，但须特别小心。在对这个文件作了任何改动后，必须重新启动 MTA。最好在 MTA 关闭的情况下进行改动。

备注	如果没有必要，请不要编辑这个文件。

有关该文件的完整信息，参见 **iPlanet Messaging Server Reference Manual**。

作业控制器文件

作业控制器（Job Controller）用于创建并管理通道的邮件传递作业。这些通道作业在控制器内的处理池中运行。存储池可被认为是通道作业运转的“地方”。存储池提供一个计算区域，在那里一组作业可在不与池外作业争夺资源的情况下运转。（有关作业控制器概念和通道关键字配置的信息，参见第 88 页“作业控制器”，第 187 页“通道执行任务的处理池”和第 188 页“服务任务限制”。）

Job Controller 文件 `job_controller.cnf` 用于指定通道处理信息。

- 定义各种存储池
- 在适用的情况下为所有通道指定主程序名和从属程序名

在 `imta.cnf` 文件中，您可用 `pool` 关键字指定一个进程存储池（已在 `job_controller.cnf` 文件中定义）的名字。例如，下面的示例文件 `job_controller.cnf` 中的一段内容定义了存储池 `MY_POOL`：

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

下面这段内容源于指定一通道块中的存储池 `MY_POOL` 的示例文件 `imta.cnf`：

```
channel_x pool MY_POOL
channel_x-daemon
```

如果想要修改与默认存储池配置相关的参数，或想添加额外的存储池，可以通过编辑 `job_controller.cnf` 文件来实现，然后关闭并重新启动作业控制器。

此时，系统将创建一个使用新配置的新作业控制器进程，并用其接收随后的请求。但旧的作业控制器进程仍在继续执行任何已排入队列的请求，直至全部完成时才退出。

在作业控制器配置文件中的第一个存储池用于任何没有指定存储池名称的请求。在 MTA 配置文件 （imta.cnf）中定义的 MTA 通道可以通过使用 pool 通道关键字，后跟存储池名，把其处理请求指向一个具体存储池。这个存储池名必须与作业控制器配置中的存储池名相匹配。如果作业控制器无法识别请求的存储池名，则忽略该请求。

在初始配置中，该配置文件定义了下列存储池：DEFAULT、 LOCAL_POOL、 IMS_POOL 和 SMTP_POOL。

使用示例

典型情况下，若希望把某些通道的处理与其它通道分开，可将额外的存储池定义添加到作业控制器配置中。也可选择使用不同性能的存储池。例如，您可能需要对某些通道允许处理的并发请求的数量进行控制。要实现这一控制，可先创建一个有作业项限制的新存储池。然后，使用 pool 通道关键字将那些通道指向这个新的，更适合的存储池。

除存储池定义外，作业控制器配置文件还可包含 MTA 通道表以及作业控制器在处理每条通道请求时必须使用的命令。这两种类型的请求分别称为 “主”请求和 “从属”请求。在典型情况下，当有邮件储存在通道的一个 MTA 邮件队列中时，就会调用该通道的主程序。主程序可将邮件取出队列。

调用从属程序是为获得一个通道并收集任何该通道入站的邮件。几乎所有 MTA 通道都有主程序，但许多 MTA 通道没有或不需要从属程序。例如，一个通过 TCP/IP 处理 SMTP 的通道并不使用从属程序，这是由于网络服务 （SMTP 服务器）可通过任何 SMTP 服务器的请求接收外来的 SMTP 邮件的。 SMTP 通道的主程序是 MTA 的 SMTP 客户程序。

如果与通道相联系的目标系统无法在同一时刻处理更多的邮件，就需要创建一个新的，作业限制为 1 的存储池类型：

```
[POOL=single_job]
job_limit=1
```

另一方面，如果目标系统具有足够的并行性，则可将作业限制设置为较高的数值。

范例 6-1 所示为一个样例作业控制器配置文件。表 6-8 所示为可用的选项。

范例 6-1 在 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
return_job=server_root/bin/msg/imta/bin/return.sh
return_time=00:30/24:00
purge_job=server_root/bin/msg/imta/bin/purge
purge_argv=-num=5
slave_command=NULL      (2)
max_life_age=3600       (3)
!
!
!Pool definitions
!
[POOL=DEFAULT]          (4)
```

范例 6-1 在 UNIX 中的样例作业控制器配置文件 （接上页）

```
job_limit=10            (5)
!
[POOL=LOCAL_POOL]
job_limit=10
!
[POOL=IMS_POOL]
job_limit=1
!
[POOL=SMTP_POOL]
job_limit=1
!
!Channel definitions
!
!
[CHANNEL=l]              (6)
master_command=server_root/bin/msg/imta/bin/l_master
!
[CHANNEL=ims-ms]
master_command=server_root/bin/msg/imta/bin/ims_master
!
[CHANNEL=tcp_*]          (7)
anon_host=0
master_command=server_root/bin/msg/imta/bin/tcp_smtp_client
```

前面示例中的关键项目 （用数字表示，用括弧括起并使用黑体者）是：

1. 此全局选项定义了 TCP 端口号，作业控制器在此侦听该端口的请求。
2. 为随后的 [CHANNEL] 部分设置默认的 SLAVE_COMMAND。
3. 为随后的 [CHANNEL] 部分设置默认的 MAX_LIFE_AGE。
4. 此 [POOL] 部分定义了一个名为 DEFAULT 的存储池。
5. 将存储池的 JOB_LIMIT 设置为 10。
6. 此 [CHANNEL] 部分应用于名为 l 的通道，即 UNIX 本地通道。此部分需要的唯一定义是 master_command，它是作业控制器发布来运行此通道的。由于在通道名中没有出现通配符，通道必须完全匹配。
7. 此 [CHANNEL] 部分应用于任何名字与 tcp_* 匹配的通道。由于这个通道名中包含一个通配符，所以可与任何名字以 tcp_ 开始的通道相匹配。

添加更多存储池的示例

作业控制器（Job Controller）用于创建并管理通道的邮件传递作业。这些通道作业在控制器内的处理池中运行。一个存储池可认为是一个运转通道作业的 “地方”。存储池提供一个计算区域，在那里一组作业可在不与池外作业争夺资源的情况下运转。请注意，在 job_controller 中对作业限制的设置是逐存储池进行的。所以，例如，如果以 job_limit 为 10 来定义 SMTP_POOL，则在给定的任何时间内，只能运行 10 个 tcp_smtp 客户进程。

有时会有需要创建额外的 tcp_* 通道（比如，用于特别缓慢邮件站点的 tcp 通道）的情况。最好使这些通道在不同的存储池中运行。这样做的原因是，如果创建 10 个不同的 tcp_* 通道并且它们都在 SMTP_POOL 中运行，在给定的时间内每个 tcp_* 通道只可能只有 1 个 tcp_smtp 客户程序在运行 （取决于是否具有发往所有 tcp_* 通道的邮件，并假定 SMTP_POOL 是以 job_limit 为 10 定义的）。假设系统的负荷很重因而所有队列上都有邮件等待从各个 tcp_* 通道发出，则此方法可能没有效果。更可能的情况是，人们想要为额外的 tcp_* 通道定义额外的存储池以避免对插槽的争夺。

例如，假定设置下列 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
```

为了给每个新通道添加 10 个 tcp_smtp_client 进程，应在 job_controller.cnf 文件中添加以下内容：

```
[POOL=yahoo_pool]
job_limit=10

[POOL=aol_pool]
job_limit=10

[POOL=hotmail_pool]
job_limit=10

...

[POOL=sun_pool]
job_limit=10
```

有关存储池的更多信息，请参阅第 187 页“通道执行任务的处理池”。有关作业控制器文件语法的更多信息，请参阅 **iPlanet Messaging Server Reference Manual**。

表 6-8　作业控制器配置文件选项

选项	说明
一般选项	说明
INTERFACE_ADDRESS=*adapter*	指定作业控制器应当对其绑定的 IP 地址界面。指定的值 （适配器）可以是 ANY，ALL、LOCALHOST 或一个 IP 地址。在默认设置下，作业控制器绑定到所有地址（等同于指定 ALL 或 ANY）。指定 INTERFACE_ADDRESS=LOCALHOST 意外着作业控制器只接受来自本地计算机内部的连接。这并不影响正常操作，因为作业控制器不支持计算机间操作。然而，在 HA （高可用性）环境中这样做可能是不适当的，因为 HA 代理可能检查作业控制器是否响应。如果 Messaging Server 正在运行计算机是一 HA 环境，有一个 “内部网络”适配器和一个 “外部网络”适配器，而您不信任防火墙对连接到高端口号的阻塞能力，就应当考虑指定 “外部网络”适配器的 IP 地址。
MAX_MESSAGES= *整数*	作业控制器在一个内存储结构中保留有关邮件的信息。在构建大型待处理邮件的情况下，可能需要限制这个结构的大小。如果待处理的邮件数超过了这个限定参数，有关随后邮件的信息将不在内存中保留。邮件并不会丢失，因为它们总是写在磁盘上，但只有在作业控制器得知邮件数量下降到该数量的一半时，这些邮件才能被考虑传送。此时，作业控制器扫描队列目录以模仿 imsimta cache -sync 命令。 默认值为 100000。
SECRET=*file_spec*	用于保护发送到作业控制器的请求的共享秘密。
SYNCH_TIME=*time_spec*	作业控制器偶尔扫描磁盘上的队列文件，以检查丢失的文件。在默认设置下，在作业控制器开始工作 4 小时后，每 4 小时进行一次。 *time_spec* 的格式是 *HH*:*MM*/*hh*:*mm* 或 /*hh*:*mm*。变量 *hh*.*mm* 使以小时 （*h*）和分钟 （*m*）计的相邻事件之间的时间间隔。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，则在 15:45 起动事件，之后每隔 7 小时 15 分钟再起动一次。
TCP_PORT= *整数*	指定作业控制器应侦听请求信息包的 TCP 端口。除非该默认设置与系统上的另一个 TCP 应用程序冲突，否则不要更改此设置。如果确实要更改此选项，请更改在 MTA tailor 文件中对应的 IMTA_JBC_SERVICE 选项，使其相匹配。MTA tailor 文件位于：*server_root*/msg-*instance*/imta/config/imta_tailor。 TCP_PORT 是全局性应用的，并且如果它在 [CHANNEL] 或 [POOL] 节出现则被忽略。
TIME=*time_spec*	指定在 PERIODIC_JOB 部分中运行的定期性作业的时间和频度。在默认设置下，该值为 /4:00，意思是每隔 4 小时。 *time_spec* 的格式是 *HH*:*MM*/*hh*:*mm* 或 /*hh*:*mm*. *hh*.*mm* 是以小时 （*h*）和分钟 （*m*）计的相邻事件之间的时间间隔。*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，则在 15:45 起动事件，之后每隔 7 小时 15 分钟再起动一次。

表 6-8　作业控制器配置文件选项（接上页）

选项	说明
存储池选项	**说明**
JOB_LIMIT= *整数*	指定存储池可以同时（平行）使用的最大进程数。JOB_LIMIT 分别应用到每个存储池，作业的最大总数是所有存储池 JOB_LIMIT 参数的总和。如果在一个节以外设置，就被没有指定 JOB_LIMIT 的任何 [POOL] 节用作默认值。在 [CHANNEL] 节内此选项被忽略。
通道选项	**说明**
MASTER_COMMAND=*file_spec*	指定由作业控制器创建的 UNIX 系统进程执行的命令的完整路径，该命令运行通道并在该通道上出列出站邮件。如果一个节以外设置，就被没有指定 MASTER_COMMAND 的任何 [CHANNEL] 节用作默认值。在 [POOL] 节内此选项被忽略。
MAX_LIFE_AGE= *整数*	指定通道主作业以秒计的最大生命时间。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，就使用 1800（30 分钟）。
MAX_LIFE_CONNS= *整数*	除了最大生命时间参数外，通道主作业的生命预期值是由它可以向作业控制器询问是否有邮件的次数所限制的。如果通道的此参数没有被指定，就使用全局默认值。如果没有指定默认值，就使用 300。
SLAVE_COMMAND=*file_spec*	指定由作业控制器创建的 UNIX 系统进程执行的命令的完整路径，该命令以运行通道并处理任何入站该通道的邮件。多数 MTA 通道不具有 SLAVE_COMMAND。如果是这种情况，应当指定保留值 NULL 如果在一个节以外设置，就被没有指定 SLAVE_COMMAND 的任何 [CHANNEL] 节用作默认值。在 [POOL] 节内此选项被忽略。

别名

MTA 提供的别名功能可支持与本地系统相关的信箱名，它不一定与实际用户相对应，这就是：*aliases*。别名对构造邮件列表、转发邮件以及为用户名提供替代名很有用处。

备注　本节对在 dirsync 模式下的别名处理进行初步阐述。在直接 LDAP 模式下的别名解析将被描述第 417 页 “使用直接 LDAP 模式解析地址（$V）”。

别名仅适用于下列地址，即与 l 通道或任何以关键字 aliaslocal 标记的通道相匹配的地址。每当 MTA 的邮件提交逻辑遇到与 l 通道或任何以关键字 aliaslocal 标记之通道相匹配的地址时，地址中指定的邮箱（如用户名）会与别名数据库或别名文件中的每个条目进行比较。如果匹配成功，别名地址会替换为转换后的值（即别名指定的值）。一个别名可转换成任意组合和数量的附加别名或实际地址。实际地址自身不必与 l 通道或任何以关键字 aliaslocal 标记的通道相联系，所以别名可以用来向远程系统转发邮件。

由于真正与通道匹配地址只有 Envelope To（信封收件人）地址，所以别名只能应用于 Envelope To 地址。MTA 只有在地址重写完成后才执行别名的转换与扩展。别名产生的转换值被视为全新的地址，并从头进行再次处理。

别名数据库

MTA 使用目录中的信息，并依此创建别名数据库。每当常规别名文件被访问时，别名数据库会被查询一次。但是，系统在使用常规别名文件前首先检查别名数据库。事实上，数据库的作用像一种地址重写器，它会在使用别名文件之前被调用。有关在创建用户条目以及别名数据库中分配列表条目时所用目录属性方面的信息，请参阅 **iPlanet Messaging Server Provisioning Guide**。

备注	数据库本身的格式是专用的。不要直接编辑数据库。对于必需的变动，请在目录中修改。

别名文件

`Aliases` 文件用于设置目录中没有设置的别名。 Postmaster 就是一个很好的例子。如果目录中存在相同别名，则在这个文件中设置的别名将被忽略。为使任何变动生效，必须重新启动 MTA。任何以感叹号开始的行都视作注释而被忽略。空行也被忽略。

备注	Messaging Server 提供其他的地址操作功能，如地址反转数据库和专用映射表。但为了求得最好的性能，在可能的情况下应尽量使用重写工具来处理地址。请参阅第 7 篇，“配置重写规则”。

该文件中的物理行被限制在 1024 个字符以内。可用反斜线 （\）续行符号将一个逻辑行分为多个物理行。

该文件的格式如下：

user`@`*domain*：<*address*>（用于托管域的用户）

user`@`*domain*：<*address*>（用于非托管域中的用户，示例：`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
```

在别名文件中包含其它文件

主 aliases 文件中可以包括其它文件。如下格式的行可指示 MTA 读取 file-spec 文件：

```
<file-spec
```

指定之文件必须为全文件路径，而且此文件必须与主 aliases 文件有相同的保护级别，例如，它必须是全局可读的。

所含文件的内容被插入到 aliases 文件中的引用点。如果把包含文件的引用替换为该文件的实际内容，也能达到相同的效果。所含文件的格式与主 aliases 文件本身的格式相同。实际上，包含文件本身也可包含其它文件。包含文件的嵌套允许达到三层。

命令行实用工具

iPlanet Messaging Server 提供有若干命令行实用工具，可用于为 MTA 执行各种维护、测试与管理任务。例如，您可用 imsimta cnbuild 命令编译 MTA 配置、别名、映射、安全、整个系统的过滤器以及选项文件。您可用 imsimta dirsync 命令重新创建或更新 MTA 目录缓存。有关 MTA 命令行实用程序的完整信息，请参见 **iPlanet Messaging Server Reference Manual**。

SMTP 的安全性和访问控制

有关 SMTP 安全与访问控制的信息，请参阅第 10 篇，“邮件过滤与访问控制”和第 12 篇，“配置安全和访问控制”。

日志文件

所有针对 MTA 的日志文件均保存在 MTA 日志目录 （*server-instance*/log/imta/）中。此目录下有描述经由 MTA 的邮件量的日志文件，以及描述有关特定的主程序或从属程序信息的日志文件。

有关 MTA 日志文件的详细信息，请参阅第 13 篇，“日志记录和日志分析”。

将内部格式地址转换为公共格式地址

使用地址反转数据库和 REVERSE 映射表可以将地址从内部格式转换为公共的、公告的格式。例如，虽然 uid@mailhost.siroe.com 在 siroe.com 域可能是一个有效的地址，而对于外部世界来说，它可能不是一个适当的地址。您可能更喜欢一个诸如 firstname.lastname@siroe.com 这样的公共地址。

备注	Messaging Server 提供其他的地址操作功能，例如 aliases 文件和专用映射表。但为了求得最好的性能，在可能的情况下应尽量使用重写工具来处理地址。请参阅第 7 篇，“配置重写规则”。

在反转数据库中，每个用户的公共地址是由在目录中用户条目的 mail 属性指定的。专用或内部地址是由 mailAlternativeAddress 属性指定的。对于分配表也是如此。

反转数据库包含一个介于任何有效的地址和此公共地址间的映射。每次当 imsimta dirsync 命令运行时，反转数据库被更新和创建。如果已经启用了直接 MTA LDAP 操作（参见附录 B，“MTA 直接 LDAP 操作”），则不使用地址反转数据库。

反转数据库一般位于 MTA 数据库目录中。数据库是一系列文件，其文件名是按在 *server_root*/msg-*instance*/imta/config/imta_tailor 文件中的 IMTA_REVERSE_DATABASE 选项指定的，在默认设置下为文件 *server_root*/msg-*instance*/imta/db/reversedb.*。

如果在数据库中找到一个地址，则数据库的相应右侧被置换为此地址。如果没有找到地址，就会尝试在映射文件中查找一个名为 REVERSE 的映射表。如果该表不存在或表中没有匹配的条目，则不进行置换且重写正常终止。

如果在映射文件中找到了 REVERSE 映射表，而且如果地址与一映射条目相匹配，且该条目指定 $Y，则结果字符串替代该地址。$N 用于放弃映射的结果。如果映射条目除了指定 $Y 外，还指定 $D，则结果串再次运行通过反转数据库；如果产生匹配情况，来自数据库的模板替代映射的结果（以及地址）。一般 REVERSE 映射表条目（即，应用于所有通道的条目）的格式如下所示。请注意，标记既可在新地址的前面，也可以在后面。

```
REVERSE

  OldAddress         $Y[Flags]NewAddress
```

针对特定通道 条目的（即只在通过一特定通道的邮件上才产生的映射）的格式如下所示。请注意，为使特定通道条目工作，必须在 option.dat 中将 use_reverse_database 设置为 13。

```
REVERSE

  source-channel|destination-channel|OldAddress  $Y[Flags]NewAddressS
```

REVERSE 映射表标记如表 6-9 中所示。

表 6-9　REVERSE 映射表标记

标记	说明
$Y	使用输出作为新地址。
$N	地址保持不变。
$D	通过反转数据库运行输出。
$A	添加模式作为反转数据库条目。

表 6-9　REVERSE 映射表标记 （接上页）

标记	说明
$F	添加模式作为正向数据库条目。
标记比较	**说明**
$:B	只匹配标题 （正文）地址。
$:E	只匹配信封地址。
$:F	只匹配向前指引地址。
$:R	只匹配向后指引地址。
$:I	只匹配邮件标识。

设置地址反转控制

reverse， noreverse 通道关键字， MTA 选项 USE_REVERSE_DATABASE 和 REVERSE_ENVELOPE 都是用来控制何时和如何具体应用地址反转。在默认设置下，地址反转操作应用于所有地址，而不仅是向后指引地址。

通过设置 REVERSE_ENVELOPE 系统选项的值 （默认值：1 - 开， 0 - 关）可以启用或禁用地址反转。

目标通道上的 noreverse 指定不将地址反转应用于邮件中的地址。而 reverse 则指定应用地址反转。详情请参见 **iPlanet Messaging Server Reference Manual**。

USE_REVERSE_DATABASE 控制 MTA 是否使用地址反转数据库和 REVERSE 映射作为置换地址源。取值 “0”意味着不对任何通道使用地址反转。取值 “5”（默认）指定在地址被 MTA 地址重写处理重写后，将地址反转应用于所有地址，而不仅仅是向后指引地址。取值 “13”指定在地址被 MTA 地址重写处理重写后，将地址反转应用于带有 reverse 通道关键字的地址，而不仅仅是向后指引地址。地址反转操作的进一步细节可通过设置 USE_REVERSE_DATABASE 选项的二进制位来指定。详情请参见 **iPlanet Messaging Server Reference Manual**。

REVERSE_ENVELOPE 选项控制地址反转是否应用于信封发件人地址以及邮件标题地址。

有关其效果的进一步的信息，参见在 **iPlanet Messaging Server Reference Manual** 中的这些选项和关键字的详细描述。

一般反转映射示例

一般 REVERSE 映射的一个示例如下：假设在 siroe.com 上的内部地址的格式为 user@mailhost.siroe.com。然而，用户名空间的安排使 user@host1.siroe.com 和 user@host2.siroe.com 对于在 siroe.com 上所有主机指定的是同一人。下列的 REVERSE 映射可以结合地址反转数据库使用：

```
REVERSE

  *@*.siroe.com         $0@siroe.com$Y$D
```

在本例中，具有格式 *name*@*anyhost*.siroe.com 的地址将更改为 *name*@siroe.com。$D 元字符使得处理过程将参照地址反转数据库。地址反转数据库应包括如下格式的条目：

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

特定通道反转映射示例

在默认设置下，如果对邮件服务器域设置了可路由范围，则要应用地址反转数据库。特定通道 REVERSE 映射表条目的一个示例如下：

```
REVERSE

  tcp_*|tcp_local|binky@macho.siroe.com    $D$YRebecca.Woods@siroe.com
```

此条目告诉 MTA，对任何带有 tcp_* 源通道和发往 tcp_local 目的地通道的邮件，将其格式为 binky@macho.siroe.com 的地址更改为 Rebecca.Woods@siroe.com

备注 为了启用特定通道映射，必须在 option.dat 中将 USE_REVERSE_DATABASE 选项设置为 13。（默认值 =5）

向前地址映射

地址反转不应用到信封收件人地址。这些地址随着邮件贯穿邮件系统而被不断地重写和修改。路由的完整目标是将信封收件人地址逐步转换为针对特定系统和特定邮箱的格式。地址反转的经典功能对信封收件人地址不适当。

用于信封收件人地址的各种置换机制提供了与反转数据库等同的功能性，但是没有哪种能够提供与反转映射等同的功能性。会出现这样的情况，即对于信封收件人地址，映射功能性是很有用和很需要的。

FORWARD 映射表提供这种缺少的功能性。如果在一个映射文件中 FORWARD 映射表存在，即被应用到每个信封收件人地址上。如果这个映射不存在或在映射匹配中没有条目，则不进行更改。

如果地址与一个映射条目相匹配，映射的结果将被测试。如果此条目指定 $Y，结果字符串替代信封的收件人地址；指定 $N 则放弃该映射结果。

使用转发数据库转发邮件

转发数据库可用于完成类似于使用别名文件或别名数据库所完成的转发功能。但当别名文件或别名数据库可使用时，因为其使用效率更高，因此会比转发数据库优先考虑使用。

使用转发数据库比较合适的情况，一般会发生在因被转发邮件的源的关系而需要完成不同种类转发的情形下。通过 USE_FORWARD_DATABASE 选项，转发数据库转发可以针对特定的源进行。更多信息，请参见 **iPlanet Messaging Server Reference Manual**。

控制传递状态通知邮件

传递状态通知或 *通知邮件* 是 MTA 发给发件人，或（可选）postmaster 的电子邮件状态的消息。 Messaging Server 可用来定制通知邮件的内容和语言还可以为每类传递状态 （如 FAILED，BOUNCED，TIMEDOUT 等等）创建不同的消息。除此之外，还可以为源自特定通道的邮件创建通知邮件。

默认设置下，通知邮件是在 *server_root*/msg-*instance*/imta/config/locale/C/LC_MESSAGES/ 目录下存储的，该目录是由在 /*server_root*/msg-*instance*/imta/config/imta_tailor 文件中的 IMTA_LANG 设置指定的。文件名如下：

return_bounced.txt, return_delivered.txt return_header.opt, return_timedout.txt, return_deferred.txt, return_failed.txt, return_prefix.txt, return_delayed.txt, return_forwarded.txt, return_suffix.txt.

请注意，不要直接更改这些文件，因为当 iPlanet Messaging Server 升级时，这些文件将被覆盖。如果希望修改这些文件并将其作为唯一的通知邮件模板文件 （return_*.txt）的设置使用，请将那些文件复制到一个新的目录下，并在那里进行编辑。然后，在 imta_tailor 文件中设置 IMTA_LANG 选项使之指向包含那些模板的新目录。如果希望通知文件具有多重设置 （如，每种语言一个设置），则需要设置 NOTIFICATION_LANGUAGE 映射表。

构建和修改通知邮件

单个通知邮件是通过对三个文件的设置构建的：
return_prefix.txt + return_*ActionStatus*.txt + return_suffix.txt

若要定制或本地化通知，需要为每个地区和 / 或定制创建一整套 return_*.txt 文件，并在一个单独的目录中存储它。例如，可以在一个目录中存放法语的通知文件，在另一个目录中存放西班牙语文件，而在第三个目录中存放特殊的针对；垃圾邮件的通道的通知。

备注 在本版本中包括了法语、德语和西班牙语的样本文件。这些文件可被修改以适合特定的需要。

通知邮件设置的格式和结构描述如下。

1. return_prefix.txt 提供适当的标题文本及正文的简介材料。US-english 地区的默认文本如下：

   ```
   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 US-ASCII 通知邮件应当适当地修改 charset 参数和 Content-Language 标题值（例如，对于法语本地化文件，该值应当为 ISO-8859-1 和 fr）。%H 是在表 6-10 中定义的标题置换序列。

2. `return_<ActionStatus>.txt` 包含特定状态的文本。*ActionStatus* 指邮件的 MTA 状态类型。例如，`return_failed.txt` 的默认文本如下：

```
Your message cannot be delivered to the following recipients:
%R
```

`return_bounced.txt` 的默认文本是：

```
Your message is being returned. It was forced to return by the
postmaster.

The recipient list for this message was:
%R
```

3. `return_suffix.txt` 包含结束语文本。默认设置下，这个文件是空的。

表 6-10　通知邮件置换序列

置换	定义
%H	扩展为邮件的标题。
%C	扩展为邮件已入队的单位数[1]。
%L	扩展为邮件在返回前已留在队列中的单位数[1]。
%F	扩展为允许一邮件留在队列中的单位数[1]。
%S [%s]	如果前面扩展的数值不等于 1，扩展字母 S 或 s。示例：根据邮件已入队的天数，“%C day%s”可以扩展为 “1 天”或 “2 天”。
%U [%u]	扩展为使用的时间单位[1] Hour [hour] 或 Day [day]。示例：根据邮件已入队的天数或小时数以及 MTA 选项 `RETURN_UNITS` 的值，“%C %U%s”可以扩展为 “2 天”或 “1 小时”。如果已设置 `RETURN_UNITS=1`（小时），并且您的站点正在使用本地化通知邮件，则需编辑 `return_delayed.txt` 和 `return_timedout.txt`，并使用非英语的所有语言的 “小时”一词替代 “day”一词。法语用 heure （s）替代 jour （s）。德语用 Stunde （n）替代 Tag （e）。西班牙语用 hora （s）替代 dia （s）。
%R	扩展为邮件收件人列表。
%%	% （请注意，置换序列的文本扫描是逐字节进行的，不管采用的是何种字符集。如果使用了双字节字符集，请检查 unintended % 标记。）

1. 单位是由在 MTA 选项文件中的 RETURN_UNITS 选项定义的，可以为小时或天 （默认）。

定制和本地化通知邮件

通知邮件可以本地化，这样邮件将以不同的语言返回给不同的用户。例如，法语的通知可被返回到已表示偏好法语的用户。

对通知邮件的本地化或定制包括两个步骤：

1. 创建一系列的本地化 / 定制 return_*.txt 消息文件，并在单独的目录下储存每个系列的文件。请参阅第 119 页 “构建和修改通知邮件”中的详细描述。）
2. 设置一个 NOTIFICATION_LANGUAGE 映射表。

NOTIFICATION_LANGUAGE 映射表 *server_root*/*msg*-instance/imta/config/mappings）指定要使用的本地化或定制的通知邮件文件系列，其依据是*原始邮件*（致使通知发出的那个邮件）的属性（例如：语言，国家，域或地址）。

通过分析原始发件人的邮件以确定状态通知的类型，源通道，偏好的语言，退回地址和第一收件人。根据表的构建方式，一个通知文件系列依据这些属性的一个或多个而被选择出来。

NOTIFICATION_LANGUAGE 映射表的格式是：

```
NOTIFICATION_LANGUAGE

 dsn-type-list|source-channel|preferred-language|return-address|first-recipient \
$Idirectory-spec
```

dsn-type-list 是一个以逗号分隔的传递状态通知类型的列表。如果指定了多种类型，它们必须用逗号隔开且不带空格 （空格表示映射表条目的模式的结束）。类型如下所列：

- failed - （失败）一般永久性失败邮件（例如，无此用户）。使用 return_failed.txt 文件。
- bounced - （退回）与手工 “退回”联合使用的通知邮件。由 postmaster 完成。使用 return_bounced.txt 文件。
- timedout - （超时）MTA 已无法在允许的传递时间内传递该邮件。邮件现在正被退回。使用 return_timedout.txt 文件。
- delayed - （延迟） MTA 已无法传递该邮件，但将继续尝试传递它。使用 return_delayed.txt 文件。
- deferred - （延期）类似于 “delayed”的非传递通知，但没有指出多长时间后 MTA 将继续尝试传递。使用 return_deferred.txt 文件。
- forwarded - （不支持回执）此邮件要求回执，然而邮件已转发到一个不支持回执的系统。使用 return_forwarded.txt 文件。

source-channel （源通道）是生成通知邮件的通道，即消息邮件正在该通道的队列里。例如， ims-ms 为邮件储存库的传递队列， tcp_local 为出站 SMTP 队列，等第。

preferred-language （语言偏好）是在被处理邮件 （为之生成通知的那个邮件）上要使用的语言。此信息首先取自 accept_language 字段。如果该字段不存在，则利用 Preferred-language: 标题字段和 X-Accept-Language: 标题字段。有关标准语言编码值的列表，请参考 *server_root*/bin/msg/install/templates/msg-inst/msg/imta/config/languages.txt 文件。

这个字段，如果不是空的，将是邮件原创者为 Preferred-language: 或 X-Accept-language: 标题行指定的任何内容。因此，此字段中也许会发现无意义的字符。

return-address （退回地址）是原创邮件的信封发件人：*地址*。这就是通知邮件即将发往的信封地址，可能带有使用何种语言的指示信息。

first-recipient （第一收件人）是原始邮件即将发往的信封收件人：地址 （即第一个地址，如果此邮件发往一个以上收件人失败的话）。例如，在通知“您发往 dan@siroe.com 的邮件无法传递”中， dan@siroe.com 是被报告的信封收件人：地址。

directory-spec 是包含 return_*.txt 文件的目录，如果映射表探测匹配成功则使用。请注意， $I 必须放在目录指定之前。

例如，一个在 /lc_messages/table/notify_french/ 目录中储存的法语通知文件 （return_*.txt）和在 /lc_messages/table/notify_spanish/ 目录中储存的西班牙通知文件 return_*.txt 的站点，可以使用如下所示的表。请注意，每个条目必须以一个或多个空格开始，且在条目间可以没有空行。

```
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/
```

备注 默认的 mappings.locale 文件在安装时一起提供，且将包含在 mappings 文件中以启用通知语言映射。若要禁用通知语言映射，请将完成包含的行标记为注释行，如下所示：

```
! <IMTA_TABLE:mappings.locale
```

（请阅读文件中的注释并按照需要进行修改。）

其他通知邮件功能

在前述各节中阐述了设置通知邮件的基本过程。以下的各节阐述其他功能。

阻塞大邮件的内容返回

典型情况下，当一个邮件被退回或被阻塞时，邮件的内容以通知邮件的形式返回到发件人和本地域 postmaster。如果许多很大的邮件完整返回，会造成资源紧张。要阻塞一定大小之上的邮件内容的返回，请在 MTA 选项文件中设置 CONTENT_RETURN_BLOCK_LIMIT 选项。

从包含的通知邮件的标题中移除非 US-ASCII 字符

互联网标题的原格式不允许非 US-ASCII 字符。如果在邮件标题中使用了非 US-ASCII 字符，则使用在 RFC 2047 中描述的 “MIME 标题编码”对其进行编码。这样，在一封电子邮件中的中文 “主题”行实际看起来将像这样：

```
Subject: =?big5?Q?=A4j=AB=AC=A8=B1=AD=B1=B0=D3=F5=A5X=AF=B2?=
```

在显示标题时移除这样的编码是电子邮件客户程序的责任。

因为 %H 模板将标题复制到通知邮件的正文中，编码的标题文本将会正常出现。然而，如果在主题中的字符集 （本例中为 “big5”）与在 return_prefix.txt 中的 Content-Type 标题字符集参数中的字符集相匹配，则 Messaging Server 将移除该编码。如果不相匹配，Messaging Server 将保留原编码不变。

设置通知邮件传递间隔

关键字：notices, nonurgentnotices, normalnotices, urgentnotices

无法传递的邮件在被返回到发件人之前，在一个给定的通道队列中保留指定的一段时间。此外，在 Messaging Server 尝试传递期间，一系列状态 / 警告邮件可以返回到发件人。各个时间总量和邮件间的时间间隔可使用 notices， nonurgentnotices， normalnotices 或 urgentnotices 关键字指定。范例：

```
notices 1 2 3
```

对于所有邮件，瞬时失败通知邮件是在 1 天和 2 天后发送的。如果在 3 天之后邮件还没有被传递，它即被返回到其原创者。

```
urgentnotices 2,4,6,8
```

对于紧急优先级邮件，瞬时失败通知邮件是在 2、4 和 6 天后发送的。如果在 8 天之后邮件还没有被传递，它即被返回到其原创者。

请注意， MTA 选项文件中的 RETURN_UNITS 选项可用将时间单位指定为小时 （1）或者天（0）。默认值为天 （0）。

如果没有指定 notices 关键字，则默认使用本地通道的 notices 的设置，即 1。如果没有对本地通道进行设置，则默认使用 notices 3, 6, 9, 12。

在通知邮件中包含已变更地址

关键字：includefinal, suppressfinal, useintermediate

当 MTA 生成一个通知邮件 （退回消息，传递回执消息等等）时，可能同时有 MTA 可用的一个收件人 “原有”格式的地址和一个该收件人变更后的 “最终”格式的地址。 MTA 总是在通知邮件中包含原有格式 （假定它存在），因为这种格式是通知邮件的收件人 （原邮件的发件人，通知邮件即与之相关）最可能识别的格式。

includefinal 和 suppressfinal 这两个通道关键字控制 MTA 是否也包含最终格式地址。禁止对最终格式地址的包含，对于那些 “隐藏”其内部邮箱名而不为外所见的站点可能有兴趣。这样的站点可能更喜欢在通知邮件中只包括原有的、“外部”格式的地址。includefinal 是默认值，表示包含的最终格式收件人地址。如果来自通知的原有地址格式存在， suppressfinal 致使 MTA 禁止通知邮件中的最终格式地址。

useintermediate 关键字使用一个产生于列表扩展之后但优先于用户名生成的地址中间格式。如果此信息未提供，则使用最终格式。

发送、阻塞和指定发往 postmaster 的通知邮件。

默认设置下，失败和警告通知邮件的一个副本是要发送给 postmaster 的，但在 Errors-to: 标题行或信封发件人：地址是空白的情况下，出错返回和警告将被完全禁止。针对 postmaster 的通知邮件传递，可以通过在以下各节和在表 6-11 中描述的一些通道关键字进行更细微的控制。

返回的失败邮件

关键字：sendpost, nosendpost, copysendpost, errsendpost

通道程序可能因为长时间服务故障或无效地址而无法传递邮件。当发生这样的故障时， MTA 通道程序在邮件中付上无法传递的解释后返回给发件人。可以选择将所有失败邮件的副本发送给本地 postmaster。这对于监控邮件失败很有用，但也可能造成过多的需要 postmaster 处理的邮件流通量。（参阅表 6-11。）

警告讯息

关键字：warnpost, nowarnpost, copywarnpost, errwarnpost

除了返回邮件， MTA 还可以对未传递的邮件发送详细的警告。这通常是由于通知通道关键字的设置而产生的超时，尽管某些情况下通道程序可能在尝试传递失败之后会生成警告讯息。警告讯息包含有对错误内容和传递尝试还将持续多久的说明。大多数情况下还包含有问题邮件的邮件头和前几行。

可以选择将所有警告邮件的副本都发送给本地 postmaster。这对于监控各种队列的状态有一定作用，尽管这样做确实造成大量的需要 postmaster 处理的邮件流通量。关键字 warnpost， copywarnpost， errwarnpost 和 nowarnpost 用于控制向 postmaster 发送警告邮件。（参阅表 6-11。）

空信封退回地址

关键字：returnenvelope

returnenvelope 关键字有一整数值，它被解释为一系列的位标记。第 0 位 （值 = 1）控制由 MTA 生成的返回通知是否被写为空信封地址或本地 postmaster 的地址。设置该位强制使用本地 postmaster 地址，而清除该位则强制使用空地址。

备注	空地址的使用是由 RFC 1123 支配的。然而，有些系统不能适当地处理空信封收件人：地址而可能需要使用此选项。

第 1 位 （值 = 2）控制 MTA 是否用本地 postmaster 地址替代所有空信封地址。此设置用于适应不符合 RFC 821， RFC 822 或 RFC 1123 的不兼容系统。

第 2 位 （值 = 4）禁止语法无效的退回地址。

第 3 位 （值 = 8）与 mailfromdnsverify 关键字相同。

Postmaster 返回邮件的内容

关键字：postheadonly, postheadbody

当通道程序或定期邮件回复工作将邮件返回到 postmaster 和原发件人时，则 postmaster 副本既可以是整个邮件也可以只有标题。 Postmaster 的副本限制为仅有邮件头，增大了用户邮件的私密性级别。但是，这样做并不能确保邮件自身的安全，如果 Postmaster 和系统管理员愿意的话，他们通常可以使用 root 系统特权来阅读邮件的内容。（参阅表 6-11。）

设置逐通道 Postmaster 地址

关键字：aliaspostmaster, returnaddress, noreturnaddress, returnpersonal, noreturnpersonal

默认设置下，当 MTA 构建退回或通知邮件时使用的 postmaster 的退回地址是 postmaster@*local-host*，其中 *local-host* 是正式本地主机名 （在本地通道上的名称），而 postmaster 的个人名称为 “MTA e-Mail Interconnect” 。在选择 postmaster 地址时应小心，不恰当的选择会造成高速的邮件循环和大量的出错邮件。

RETURN_ADDRESS 和 RETURN_PERSONAL 选项可用于为 postmaster 地址和个人姓名设置 MTA 系统默认值。或者，如果需要逐通道控制，可以使用 returnaddress 和 returnpersonal 这两个通道关键字。 returnaddress 和 returnpersonal 各自取得一个需要的参数，分别指定 postmaster 地址和 postmaster 个人姓名。 noreturnaddress 和 noreturnpersonal 为默认设置以强调这些应当使用的值。默认设置是通过 RETURN_ADDRESS 和 RETURN_PERSONAL 选项建立的，如果没有设置这两个选项，则采用常规默认设置值。

如果 aliaspostmaster 关键字放置在某一通道，则任何发往正式通道名上的用户名为 postmaster （小写，大写或大小写混合）的邮件，将被重定向到 postmaster@*local-host*，其中 *local-host* 为正式本地主机名 （在本地通道上的名称）。请注意，互联网标准要求任何接收邮件 DNS 中的域具有一个接收邮件的有效的 postmaster 帐户。所以当希望集中 postmaster 责任，而不是为单独的域设置单独的帐户时，此关键字可能很有用。也就是说，尽管当 MTA 从 postmaster 生成通知邮件时，使用 returnaddress 以控制使用什么退回 postmaster 地址，但 aliaspostmaster 影响到 MTA 对发往 postmaster 的邮件的处理。

表 6-11　发往 postmaster 的通知邮件和发件人关键字

关键字	说明
返回邮件的内容	**指定通知的地址**
notices	指定在发送通知和退回邮件之前可能需经过的时间。
nonurgentnotices	对于具有非紧急优先级的邮件，指定在发送通知和退回邮件之前可能需经过的时间。
normalnotices	对于具有普通优先级的邮件，指定在发送通知和退回邮件之前可能需经过的时间。
urgentnotices	对于具有紧急优先级的邮件，指定在发送通知和退回邮件之前可以耗费的时间量。
退回邮件	**如何处理退回邮件的失败通知。**
sendpost	允许向 Postmaster 发送所有失败邮件的副本。
copysendpost	向 Postmaster 发送失败通知副本，除非失败邮件的发件人地址为空，在这种情况下，Postmaster 获取除了那些实际上是被自身退回或通知的邮件之外的所有失败邮件副本。
errsendpost	仅当不能向发件人返回通知时才向 Postmaster 发送失败通知副本。如果指定了 nosendpost，则不会向 Postmaster 发送失败通知副本。
nosendpost	禁止向 Postmaster 发送所有失败邮件副本。
警告讯息	**如何处理警告讯息。**
warnpost	允许向 Postmaster 发送警告讯息副本。如果没有指定任何关键字，默认的处理是向 Postmaster 发送警告讯息的副本，除非警告信息因使用一个空的 `Warnings-to:` 邮件头或一个空的 `From:` 信封地址而被完全取消。
copywarnpost	向 Postmaster 发送警告讯息副本，除非无法递邮件的发件人地址为空。
errwarnpost	当不能向发件人返回通知时才向 Postmaster 发送警告讯息副本。
nowarnpost	禁止向 Postmaster 发送警告讯息副本。
返回邮件的内容	**指定向 Postmaster 发送整个邮件还是仅发送邮件头。**
postheadonly	仅向 Postmaster 返回邮件头。 Postmaster 的副本限制为仅有邮件头，增大了用户邮件的私密性级别。但是，这并不保证邮件的安全性，因为如果愿意， postmaster 和系统管理员可以使用 `root` 系统特权读取邮件的内容。
postheadbody	既返回邮件头也返回邮件内容。
返回邮件的内容	**指定通知的地址**
includefinal	在传递通知中包含最终格式地址 （收件人地址）。

表 6-11　发往 postmaster 的通知邮件和发件人关键字（接上页）

关键字	说明
returnenvelope	控制空信封退回地址的使用。 returnenvelope 关键字取一整数值，它被解释为一系列位标记。 第 0 位 （值 = 1）控制由 MTA 生成的返回通知是否被写为空信封地址或本地 postmaster 的地址。设置该位强制使用本地 postmaster 地址，而清除该位则强制使用空地址。 第 1 位 （值 = 2）控制 MTA 是否用本地 postmaster 地址替代所有空信封地址。此设置用于适应不符合 RFC 821， RFC 822 或 RFC 1123 的不兼容系统。 第 2 位 （值 = 4）禁止语法无效的退回地址。 Bit 3 （值 = 8）与 mailfromdnsverify 关键字相同。
suppressfinal	在通知邮件中禁止最终格式地址，如果通知邮件中存在原有格式地址。
useintermediate	使用一个产生于列表扩展之后但优先于用户名生成的地址中间格式。如果此信息未提供，则使用最终格式。
返回邮件的内容	**指定通知的地址**
aliaspostmaster	任何发往正式通道名上的用户名为 postmaster 的邮件，将被重定向到 postmaster@local-host 其中 local-host 为正式本地主机名 （在本地通道上的名称）。
returnaddress	指定本地 postmaster 的退回地址。
noreturnaddress	将 RETURN_ADDRESS 选项值用作 postmaster 地址名。
returnpersonal	设置本地 postmaster 的个人姓名。
noreturnpersonal	将 RETURN_PERSONAL 选项值用作 postmaster 的个人姓名。

第 7 篇

配置重写规则

本章描述如何配置 imta.cnf 文件中的重写规则。如果尚未阅读第 6 篇，“关于 MTA 服务与配置”，应先阅读之，然后再回来阅读本章。

本章包括以下各节：

- 重写规则结构
- 重写规则模式和标记
- 重写规则模板
- MTA 将重写规则应用到地址的方法
- 模板置换串和重写规则控制序列
- 处理大量重写规则
- 测试重写规则
- 重写规则示例

Messaging Server 的地址重写工具是处理和修改地址的主机或域部分的主要工具。Messaging Server 还提供了其他的地址处理工具，如别名、地址反转数据库和专用映射表。但为了求得最好的性能，在可能的情况下应尽量使用重写工具来处理地址。

备注 在修改了 imta.cnf 文件中的重写规则后，必需重新启动任何如 SMAP 服务器这样的程序或通道：它们只在用命令 imsimta start 启动时一次性地加载配置数据。如果使用的是已编译的配置，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方面的详细信息，请参阅 **iPlanet Messaging Server Reference Manual**。

重写规则结构

重写规则出现在 MTA 配置文件 `imta.cnf` 的前半部分。配置文件中的每条规则占用一行。规则之间可以有注释行，但不得有空行。重写规则序列以空行结束，其后是通道定义。图 7-1 所示为局部配置文件的重写规则部分。

图 7-1 简单配置文件 - 重写规则

```
! 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
```

重写规则包括两部分：一个模式，后跟一个等值串或*模板*。这两部分必须用空格分开，但其本身不得包含空格。重写规则结构如下：

```
pattern template
```

pattern （模式）

指示要在域名中寻找的串。图 7-1 所示的模式为 `a.com`、`b.org`、`c.edu` 和 `d.com`。

若模式匹配地址的域部分，重写规则即被应用于该地址。必须用空格将模式与模板分开。有关模式语法的详细信息，请参阅第 131 页 “重写规则模式和标记”。

template （模板）

为下列中的之一：

UserTemplate`%`*DomainTemplate*`@`*ChannelTag*`[`*controls*`]`

UserTemplate`@`*ChannelTag*`[`*controls*`]`

UserTemplate`%`*DomainTemplate*`[`*controls*`]`

UserTemplate`@`*DomainTemplate*`@`*ChannelTag*`[`*controls*`]`

UserTemplate`@`*DomainTemplate*`@`*SourceRoute*`@`*ChannelTag*`[`*controls*`]`

UserTemplate *（用户模板）*	指定地址的用户部分如何被重写。置换序列可用来表示原地址的各个部分或数据库查询结果。置换序列被其所表示的内容代替从而构成重写地址。在图 7-1 中，使用的置换序列为 $U。有关详细信息，请参阅第 139 页 “模板置换串和重写规则控制序列”。
DomainTemplate *（域模板）*	指定地址的域部分如何被重写。类似于 *UserTemplate*，*DomainTemplate* 可包含置换序列。
ChannelTag *（通道标记）*	指示发送邮件的通道。（所有通道定义必须包含通道标记和通道名。通道标记通常出现在重写规则以及通道定义中。）
controls （控制）	使用控制可限制一个规则的适用性。一些控制序列必须出现在规则的开头，其他的控制则必须出现在规则的末尾。与控制有关的详细信息，请参阅第 139 页 “模板置换串和重写规则控制序列”。

有关模板语法的详细信息，请参阅第 134 页 “重写规则模板”。

重写规则模式和标记

本节包含下列分节：

- 用于匹配 Percent Hack 的规则
- 用于匹配 Bang-Style （UUCP）地址的规则
- 可匹配任意地址的规则
- 有标记重写规则集

大部分重写规则模式由一个与唯一主机相匹配的特定的主机名，或者一个匹配整个子域中的任意主机 / 域的子域模式所组成。

例如，下面所示的重写规则模式包含一个仅与指定主机相匹配的特定主机名：

```
host.siroe.com
```

下一个重写规则模式包含一个将匹配整个子域中的任意主机或域的子域模式：

```
.siroe.com
```

然而，这一模式并不与主机名 `siroe.com` 精确匹配，要与主机名 `siroe.com` 精确匹配，需要另一个 `siroe.com` 模式。

MTA 首先尝试从特定的主机名重写主机 / 域名，然后逐步归纳使其不那么具体。这意味着较专一的重写规则模式比较一般的重写规则模式优先应用。例如，假定配置文件中有下面所示的重写规则模式：

```
hosta.subnet.siroe.com
.subnet.siroe.com
.siroe.com
```

基于重写规则模式，地址 jdoe@hosta.subnet.siroe.com 将匹配重写规则模式 hosta.subnet.siroe.com ；地址 jdoe@hostb.subnet.siroe.com 将匹配重写规则模式 .subnet.siroe.com ；地址 jdoe@hostc.siroe.com 将匹配重写规则模式 .siroe.com。

特别应指出的是，结合子域重写规则模式来使用重写规则，在 Internet 站点中是相当普遍的。这种站点一般拥有许多内部主机和子网的重写规则，因而将把顶级 Internet 域的重写规则从 internet.rules（*server-instance*/imta/config/internet.rules）文件包含到配置中。

为了确保发送到 Internet 目的地的邮件 （而不是通过更专一的重写规则处理的发至内部主机目的地之邮件）被适当地重写并路由到外发的 TCP/IP 通道，须确保 imta.cnf 文件中包含：

- 与顶级 Internet 域相匹配的重写规则和模式
- 可将与这种模式相匹配的地址重写到外发 TCP/IP 通道的模板

```
!    Ascension Island
.AC                                        $U%$H$D@TCP-DAEMON
. [text
.    removed for
.             brevity]
!    Zimbabwe
.ZW                                        $U%$H$D@TCP-DAEMON
```

IP 域字面值 （常值）遵循类似的层次匹配模式，尽管是从右到左 （而非从左到右）的匹配。例如，下面的模式只匹配、且精确匹配 IP 常值 [1.2.3.4]：

```
[1.2.3.4]
```

下面的模式匹配子网 1.2.3.0 中的任何项：

```
[1.2.3.]
```

除了已经讨论的较常见的主机或子域类型的重写规则模式外，重写规则也可以使用几种特殊的模式，见表 7-1 中的概要，并在下面的段落中讨论。

表 7-1　重写规则特殊模式概要

模式	说明 / 用法
$*	匹配任何地址。如果指定了此规则，则不论其在文件中的位置如何，它都将是第一个被使用的规则。
$%	Percent Hack 规则。匹配任何以 A%B 形式描述的主机 / 域。
$!	Bang-style 规则。匹配任何以 A!B 形式描述的主机 / 域。
[ ]	IP 常值全匹配规则。匹配任何 IP 域常值。
.	匹配任何形式的主机 / 域描述。例如， joe@[129.165.12.11]

除了这些特殊模式外， Messaging Server 还有*标记*的概念可能出现在重写规则模式中。在一个地址有可能被多次重写的情况下需使用这些标记，而且在前一次重写的基础上，随后的重写必须有所区别，这是通过控制用哪个重写规则去匹配地址而实现的。有关详细信息，请参阅第 133 页 “有标记重写规则集”。

用于匹配 Percent Hack 的规则

如果 MTA 试图重写具有 `A%B` 形式的地址并且失败，在完全失败之前会尝试一种额外的规则，即将地址形式处理为 `A%B@localhost`。（有关这些地址形式的详细信息，请参阅第 134 页 “重写规则模板”。）这个额外规则就是 *Percent Hack 规则*。其模式为 `$%`。此模式永不改变。当一个包含 Percent Hack 的本地部分以其他方式（包括如下所述的全匹配规则）重写失败时，此规则才予以启用。

Percent Hack 规则对于赋予 Percent Hack 地址以一些特殊的、内部的含义是十分有用的。

用于匹配 Bang-Style （UUCP）地址的规则

如果 MTA 试图重写具有 `B!A` 形式的地址并且失败，在完全失败之前会尝试一种额外的规则，即将地址形式处理为 `B!A@localhost`。这个额外的规则即 *Bang-style 规则*。其模式是 `$!`。此模式永不改变。当包含一个感叹号的本地部分以其他方式（包括如下所述的默认规则）重写失败时，此规则才予以启用。

Bang-style 规则可强制 UUCP 式样的地址经路由选择发送到一个具有广泛 UUCP 系统和路由能力的系统。

可匹配任意地址的规则

如果其他规则无法匹配并且通道表中无法找到该主机 / 域描述，则特殊的模式 “.”（单句号）将匹配任何主机 / 域描述。换句话说，当其他地址重写方法都失败时，“.” 规则将作为最后的一种手段进行地址重写。

备注 关于置换序列，当全匹配规则匹配成功并且其模板被扩展时， `$H` 扩展为完整的主机名， `$D` 扩展为一个点 “.”。因此， `$D` 在一个全匹配规则模板中的作用是很有限的!

有标记重写规则集

在重写进行过程中，将不同的规则集引入这一过程可能是适当的。您可通过重写规则标记实现这一目的。在配置文件或域数据库中查找之前，当前标记被添加在每个模式的前面。您可通过重写规则模板 （如下所述）中的置换串 `$T` 用任何匹配的重写规则对该标记进行更改。

标记具有记忆性，一旦设置就会继续应用到从单一地址抽取出的所有主机。这意味着，一旦要使用任何标记，就必须非常细心地提供以适当标记值打头的备用规则。实践中很少会出现问题，因为标记通常只应用于非常专门的应用软件。一旦完成地址的重写，标记即被重置为默认标记，即一个空串。

根据约定，所有标记均以竖杠 | 结束。这一字符在一般地址中并不使用，因此可自由地用来分隔标记与模式的其余部分。

重写规则模板

以下各节将较详细地描述重写规则的模板格式。表 7-2 概括了各种模板格式。

表 7-2　重写规则模板格式概要

模板	页面	用法
A%B	134	A 为新用户 / 邮箱名， B 为新主机 / 域描述，再次重写。
A@B	134	视为 A%B@B。
A%B@C	134	A 为新用户 / 邮箱名， B 为新主机 / 域描述，路由到与主机 C 相关联的通道上。
A@B@C	135	视为 A@B@C@C。
A@B@C@D	135	A 为新用户 / 邮箱名， B 为新主机 / 域描述，插入 C 作为一个源路由，路由到与主机 D 相关联的通道上。

常用重写模板：A%B@C 或 A@B

下面的模板是最常见的模板形式。该规则应用于地址的用户部分和地址的域部分。于是使用新地址将邮件路由到一个指定的通道 （由 *ChannelTag* 指示）。

UserTemplate%*DomainTemplate*@*ChannelTag*[*controls*]

下面模板形式在应用上与最常见的模板形式等同。然而，只有当 *DomainTemplate* 和 *ChannelTag* 等同时，此种模板形式才成为可能。

UserTemplate@*ChannelTag*[*controls*]

重复重写模板 A%B

下面模板格式应用于元规则，这需要在应用规则后进行另外的重写。此规则应用后，整个重写过程在作为结果的新地址上重复。（而所有其他的重写规则格式则在规则应用后终止重写过程。）

UserTemplate%*DomainTemplate*[*controls*]

例如，下面的规则具有从地址末端删除所出现在那里可删除域 （.removable domain）。

.removable　　$U%$H

在使用这些重复规则时应格外小心；使用不正确会造成 “规则循环”（rules loop）。出于这一原因，只在确实必要时才应使用 “元规则”。请确保一定要用 `imsimta test -rewrite` 命令测试元规则。有关 `test -rewrite` 命令的详细信息，请参阅 **iPlanet Messaging Server Reference Manual**。

指定路由重写模板， A@B@C@D 或 A@B@C

如下格式的模板与常见模板以同样的方式运行 *UserTemplate*`%`*DomainTemplate*`@`*ChannelTag*（注意在第一分隔符上的区别），不同的是 *ChannelTag* 是作为源路由而被插入到地址中的。邮件然后经路由选择被传送到 *ChannelTag*：

UserTemplate`@`*DomainTemplate*`@`*Source-Route*
`@`*ChannelTag*`[`*controls*`]`

被重写地址变为 `@`*route*`:`*user*`@`*domain*. 下面的模板也有效：

UserTemplate`@`*DomainTemplate*`@`*ChannelTag*`[`*controls*`]`

例如，下面的规则将地址 `jdoe@com1` 重写到源路由地址 `@siroe.com:jdoe@com1`。通道标记变为 `siroe.com`:

```
com1 $U@com1@siroe.com
```

重写规则模板中的大小写敏感性

与重写规则中的模式不同的是，模板中的字符应区分大小写。当使用重写规则来给一个对大小写敏感的邮件系统提供界面时，这是十分必要的。注意，像 $U 和 $D 这样的置换序列在置换从地址中抽取的材料时，保持字符原来的大小写不变。

当需要强制被置换材料只使用特定的字体形式 （大写或小写）时，例如强制 UNIX 系统中的邮箱采用小写字母，可在模板中使用特殊的置换序列以强制被置换材料转换为所希望的字体形式。特别是 $\，它可强制随后的被置换材料转换为小写，$^ 可强制随后的被置换材料转换为大写， $_ 表示保持原来的字体形式不变。

例如，可使用下面的规则强制使地址 `unix.siroe.com` 处的邮箱采用小写字母。

```
unix.siroe.com     $\$U$_%unix.siroe.com
```

MTA 将重写规则应用到地址的方法

下面的步骤描述 MTA 是如何将重写规则应用到给定地址的：

1. MTA 从地址中抽取第一个主机或域描述。

   在这种情况下，一个地址可指定多个主机名或域名。

   `jdoe%hostname@siroe.com.`

2. 在标识出第一个主机名或域名后，MTA 通过搜索以寻找一个其模式匹配该主机名或域名的重写规则。

3. 当找到匹配的重写规则后， MTA 根据规则的模板部分重写该地址。
4. 最后， MTA 将通道标记与关联每个通道的主机名进行比较。

   若匹配成功，MTA 将邮件排在相关通道的队列中；否则，重写过程失败。若匹配通道为本地通道，有可能通过查询别名数据库或别名文件而执行一些另外的地址重写。

这些步骤将在下面段落中详细描述。

备注 使用不属于任何现有通道的通道标记将致使其地址匹配这一规则的邮件被退回。也即，使匹配的邮件不可路由。

第 1 步：抽取第一个主机描述或域描述

重写一地址的过程开始于从地址中抽取第一个主机描述或域描述。（建议不熟悉 RFC822 地址约定的读者阅读该标准以便理解下面的讨论。）扫描主机 / 域规范的顺序如下：

1. 源路由中的主机 （从左向右读）
2. 出现在 “at”（@）符号右边的主机
3. 出现在最后一个单独的百分号 （%）右边的主机
4. 出现在第一个感叹号 （!）左边的主机

如果关键字 `bangoverpercent` 在正进行地址重写的通道上有效，上述顺序的最后两项须对换。也就是说，如果试图为邮件排队的通道本身被 `bangoverpercent` 通道关键字所标记。

一些应首先抽取的地址和主机名的例子，见表 7-3。

表 7-3 抽取的地址和主机名

地址	第一个主机域规范	注释
`user@a`	`a`	“简短”域名。
`user@a.b.c`	`a.b.c`	“全限定”域名 （FQDN）。
`user@[0.1.2.3]`	`[0.1.2.3]`	“域常值”。
`@a:user@b.c.d`	`a`	简短域名的源路由地址，即 “路由”。
`@a.b.c:user@d.e.f`	`a.b.c`	源路由地址，具有全限定的路由部分。
`@[0.1.2.3]:user@d.e.f`	`[0.1.2.3]`	源路由地址，路由部分为一个域常值。
`@a,@b,@c:user@d.e.f`	`a`	源路由地址，具有从 a 到 b 到 c 的路由。
`@a,@[0.1.2.3]:user@b`	`a`	路由部分中含有一个域常值的源路由地址。
`user%A@B`	`B`	这种非标准形式的路由叫做 Percent Hack。

表 7-3　　抽取的地址和主机名（接上页）

地址	第一个主机域规范	注释
user%A	A	
user%A%B	B	
user%%A%B	B	
A!user	A	“Bang-style”寻址；通常用于 UUCP。
A!user@B	B	
A!user%B@C	C	
A!user%B	B	nobangoverpercent 关键字为现用状态，默认状态。
A!user%B	A	bangoverpercent 关键字为现用状态。

RFC 822 没有阐述对地址中的感叹号 （!）和百分号 （%）的解释。若没有 at 符号，百分号通常被解释为与 at 符号 （@）相同，因此这一约定被 Messaging Server MTA 采用。

对重复的百分号的特殊解释用于将百分号作为本地用户名的一部分，这对于处理某些外国邮件系统地址可能有用。对感叹号的解释符合 RFC976 的 Bang-style 地址约定，这使得 Messaging Server MTA 可以使用 UUCP 地址。

上述符号的解释的顺序没有在 RFC 822 或 RFC 976 中说明，因此可使用 bangoverpercent 和 nobangoverpercent 这两个关键字控制通道进行重写时所用的顺序。尽管备用设置在某些情况下很有用，但默认值更为 “标准”。

备注　　在地址中不提倡使用感叹号 （!）或百分号 （%）。

第 2 步：扫描重写规则

一旦第一个主机或域描述从地址中抽取出，MTA 就参照重写规则对其进行处理。将主机 / 域描述与每个规则的模式部分 （即，每个规则的左部）进行比较。这种比较不区分大小写。不区分大小写是由 RFC822 决定的。 MTA 不区分大小写，但尽可能保存字符字体形式的原貌。

若主机或域描述不匹配任何模式，此种情况称为“不匹配任何规则”，主机或域描述的第一部分 （即第一个句号前的部分，通常就是主机名）会被删除并被星号 （*）替代，然后再次试图定位主机或域描述，但只局限于配置文件中的重写规则 （不参照域数据库）。

若失败，第一部分被删除并重复上述处理过程。若还是失败，下一部分被删除 （通常是一子域）并再次尝试重写，先用星号，然后不用星号。所有包含星号的探测只局限于配置文件中的重写规则列表，不检查域数据库。这一过程一直持续，直到找到一个匹配项或检查完整个主机 / 域描述。这一过序的效果就是首先试图匹配最明确的域，然后向外扩展，匹配不那么精确的、较一般的域。

从算法角度来看这样的匹配过序就是：

- 主机 / 域描述用作对照串 spec_1 和 spec_2 的初始值 （例如 spec_1 = spec_2 = a.b.c）。
- 对照串 spec_1 先与配置文件中每一条重写规则的模式部分比较，然后才轮到域数据库，直到找到一个匹配项。若找到匹配项，即退出匹配过程。
- 若未找到匹配项，则将 spec_2 最左边的非星号部分转换为一个星号。例如，如果 spec_2 为 a.b.c 则更改为 *.b.c；若 spec_2 为 *.b.c 则更改为 *.*.c。若找到匹配项，即退出匹配过程。
- 若无匹配项，对照串 spec_1 的第一部分，连同任何前导句号，都将被删除。这里的 spec_1 只有一个部分 （例如 .c 或 c），该串被一单个句号 “.” 所替换。如果产生的字串 spec_1 为非零长度，则返回到第 1 步。若产生的字串为零长度 （例如，前述的 “.”），则查找过程失败，并退出匹配过程。

例如，假设要对地址 dan@sc.cs.siroe.edu 进行重写。这将引起 MTA 按给定顺序查找下面的模式：

```
sc.cs.siroe.edu
*.cs.siroe.edu
.cs.siroe.edu
*.*.siroe.edu
.siroe.edu
*.*.*.edu
.edu
*.*.*.*
.
```

第 3 步：根据模板重写地址

一旦主机或域描述匹配一个重写规则，就可使用规则中的模板部分进行重写。模板指定了三项内容：

1. 地址的新用户名。
2. 地址的新主机或域描述。
3. 标识现有 MTA 通道的通道标识，即通过该通道发送寄往该地址的邮件。

第 4 步：完成重写过程

一旦主机或域描述被重写，则会发生下面几项操作。

- 若通道标记既不与本地通道相关联，又不与标有通道关键字 routelocal 的通道相关联，或者地址中没有另外的主机或域描述，重写描述将替换到地址中以代替为重写而抽取出的原描述，重写过程就此终止。

- 若通道标记匹配本地通道或标有 routelocal 的通道，且地址中有另外的主机或域描述，则放弃重写地址，原（初始）主机或域描述从地址中删除，从地址中抽取新的主机或域描述，整个过程将重复进行。重写过程将继续进行，直到所有的主机或域描述经检查无效或找到一个经由非本地的、未标有 routelocal 通道的路由为止。这种反复机制解释了 MTA 是如何提供对源路由的支持的。事实上，通过这一过程，从地址中删去了经由本地系统和 routelocal 系统的多余的路由。

重写规则失败

如果主机 / 域描述无法匹配任何重写规则而且没有现成的默认规则，MTA 将按字面含义使用描述。例如，原描述既是新描述又是路由系统。如果地址中有一个无意义的主机 / 域描述，邮件将被退回。当路由系统不匹配任何关联某个通道的系统名时，此种情况即被检测出。

重写后语法检查

在重写规则应用于地址后不进行另外的语法检查。这是有意的安排，其目的是用重写规则把一个地址转换成不符合 RFC822 的格式。然而，这也意味着配置文件中的错误可能导致邮件带着不正确或非法的地址离开 MTA。

处理域常值

在重写过程中要对域常值进行特别的处理。如果出现在地址域部分的域常值无法按字面匹配一个重写规则模式，该常值即被解释为用方括弧括起来的、用句号分隔开的一系列字符串。在删除了最右边的串后，再次搜寻。如果仍不成功，删除下一个串，如此循环往复，直到剩下空的括弧为止。如果搜寻空括弧失败，则删除整个域常值，重写过程在域地址的下一节（如果有的话）继续进行。在域常值内部处理中不使用星号；当一个完整的域常值被一个星号所替换时，星号数量与域常值中的元素数量相对应。

与常用域或主机描述一样，域常值也是按最专一到最不专一的顺序进行尝试。其模式匹配成功的第一个规则被用来重写主机或域描述。如果在规则列表中有两个完全相同的模式，则使用先出现的那个。

作为例子，假定要重写 dan@[128.6.3.40] 地址。重写程序先寻找 [128.6.3.40]，然后是 [128.6.3.]、[128.6.]、[128.]、[]、[*.*.*.*]，最后是全匹配规则“.”。

模板置换串和重写规则控制序列

通过在重写地址中插入一个字符串，置换串被用于重写用户名或地址，它的值是由所用的特定置换序列决定。本节包含下列分节：

- 用户名和子地址置换 $U、$0U、$1U
- 主机 / 域和 IP 常值置换串 $D、$H、$nD、$nH、$L
- 常值字符置换串 $$、$%、$@
- LDAP 查询 URL 置换串 $]...[

- 常规数据库置换串 $(...)
- 应用指定映射 ${...}
- 客户提供的例程置换串 $[...]
- 单字段置换串 $&、 $!、 $*、 $#
- 唯一串置换串
- 针对源通道的重写规则 （$M、 $N）
- 针对目标通道的重写规则 （$C、 $Q）
- 针对主机位置的重写 （$A、 $P、 $S、 $X）
- 改变当前标记值 $T
- 控制与重写相关的出错消息 （$?）

例如，在下面的模板中 $U 是一个置换序列。这使得被重写地址的*用户名*部分被置换到模板的输出中。因此，如果 `jdoe@mailhost.siroe.com` 被模板所重写，输出结果应该是 `jdoe@siroe.com`， $U 置换了原地址中用户名部分的 `jdoe`：

```
$U@siroe.com
```

控制序列向给定的重写规则的适用性附加另外的条件。不仅重写规则的模式部分须匹配被检查的主机或域描述，而且被重写的地址的其他方面也必须满足控制序列或序列组所设置的条件。例如，$E 控制序列要求被重写的地址为一信封地址，而 $F 控制序列要求该地址为一个向前指引地址。下面的重写规则只适用于（重写）信封的 To：地址，其形式为 `user@siroe.com`：

```
siroe.com $U@mail.siroe.com$E$F
```

如果域或主机描述匹配了一个重写规则的模式部分，但没有满足规则模板控制序列的所有要求，则重写规则失败，重写程序将继续查找其他适合的规则。

表 7-4 为模板置换串和控制序列的概要。

表 7-4　　模板置换串和控制序列概要

置换序列	置换
`$D`	匹配的域描述部分。
`$H`	主机或域描述的未匹配部分，模式中圆点的左边。
`$L`	域常值的未匹配部分，模式常值中圆点的右边。
`$U`	原地址中的用户名。
$0U	原地址中的本地部分 （用户名），除去任何子地址。
$1U	原地址中的本地部分 （用户名）中的子地址 （如果有的话）。
`$$`	插入一个美元符号常值 （$）。
`$%`	插入一个百分号常值 （%）。

表 7-4　模板置换串和控制序列概要（接上页）

置换序列	置换
$@	插入一个 at 符号常值 （@）。
$\	强制将内容转换为小写字母。
$^	强制将内容转换为大写字母。
$_	使用原字体形式 （大写或小写）。
$W	置换随机的、唯一串。
$]...[	LDAP 搜索 URL 查找。
$(text)	一般数据库置换；如果查找失败则规则失败。
${...}	将指定映射应用到提供的串。
$[...]	调用客户机提供的程序；在结果中置换。
$&*n*	未匹配主机 （或含通配符的主机）的 *nth* 部分，从 0 开始从左至右计数。
$!*n*	未匹配主机 （或含通配符的主机）的 *nth* 部分，从 0 开始从右至左计数。
$**n*	匹配模式的 *nth* 部分，从 0 开始从左至右计数。
$#*n*	匹配模式的 *nth* 部分，从 0 开始从右至左计数。
$*n*D	已匹配的域描述部分，保留自最左边 *nth* 部分 （从 0 开始计数）。
$*n*H	未匹配的主机 / 域描述部分，保留自最左边 nth 部分 （从 0 开始计数）。
控制序列	**对重写规则的影响**
$1M	只有在通道为内部重新处理之通道的情况下适用。
$1N	只有在通道为内部重新处理之通道的情况下适用。
$1~	可对任何未决匹配项进行检查。如果检查失败，则可成功地终止对当前重写规则模板的处理。
$A	如果主机位于 at 符号右边则适用
$B	只适用于标题 / 正文地址
$C *channel*	若发送到 *channel* 则失败
$E	只适用于信封地址
$F	只适用于向前指引的 （例如， TO:）地址
$M *channel*	只适用于 *channel* 正在重写地址的情况
$N *channel*	若 *channel* 正在重写地址则失败
$P	如果主机位于百分号右边则适用
$Q *channel*	适用于发送到 *channel* 的情况
$R	只适用于向后指引的 （例如， From:）地址

表 7-4　模板置换串和控制序列概要（接上页）

置换序列	置换
$S	如果主机来自源路由则适用
$T*newtag*	在将重写规则标记设置为 newtag（新标记）
$V*host*	如果主机名没有在 LDAP 目录中定义（在 DC 树中或作为虚拟域）则失败。如果 LDAP 搜索超时，则直接跟在主机名后面的字符的重写模板之剩余部分将被供选用的 MTA 串 `DOMAIN_FAILURE` 替换。
$X	如果主机位于感叹号左边则适用
$Z*host*	如果主机名在 LDAP 目录中有定义（在 DC 树中或作为虚拟域）则失败。如果 LDAP 搜索超时，则直接跟在主机名后面的字符的重写模板之剩余部分将被供选用的 MTA 串 `DOMAIN_FAILURE` 替换。
$?*errmsg*	若重写失败则返回 *errmsg*，而不是默认的出错信息。出错讯息必须使用 US ASCII。
$*number*?*errmsg*	若重写失败则返回 *errmsg*，而不是默认的出错信息，并将 SMTP 的扩展错误代码设置为 *a.b.c*： • *a* 是 *number*/1000000（第一位数） • *b* 是（*number*/1000）1000 的剩余部分（2 至 4 位数的值） • *c* 是 *number* 1000 的剩余部分（最后三位数的值）。 以下的例子将错误代码设为 3.45.89: `$3045089?the snark is a boojum`

用户名和子地址置换 $U、$0U、$1U

模板中出现的任何 $U 将被用户名（RFC822 的“本地部分”）从原地址中替换掉。注意，形如 a."b" 的用户名将被 "a.b" 所替换，这是因为 RFC2822 已降格使用 RFC822 以前的语法，并以期后一种用法能在将来成为硬性规定。

模板中出现的任何 $0U 将被用户名从原地址中替换掉，并除去任何子地址及子地址指示符（+）。模板中出现的任何 $1U 将被子地址及子地址指示符（如果有的话）从原地址中替换掉。因此应注意， $0U 和 $1U 是用户名的互为补充的两个片断， $0U$1U 等同于简单的 $U。

主机 / 域和 IP 常值置换串 $D、$H、$nD、$nH、$L

任何 $H 将被不与规则匹配的主机或域描述部分所替换。任何 $D 将被与重写规则相匹配的主机或域描述所替换。字符序列 $nH 和 $nD 是保存最左边 nth 部分（从 0 开始计数）的一般的 $H 或 $D 部分的变量。也就是， $nH 和 $nD 忽略了一般为 $H 或 $D 的最左边的 n 个部分（从 1 开始计数），分别置换。特别是， $0H 等同于 $H， $0D 等同于 $D。

例如，假定地址 jdoe@host.siroe.com 匹配下面的重写规则：

```
host.siroe.com     $U%$1D@TCP-DAEMON
```

重写后的地址为 jdoe@siroe.com 并将 TCP-DAEMON 用作出站通道。此处，若为 $D 则在整个域中置换匹配部分，即 host.siroe.com，而 $1D 则只在从第一部分 （即 siroe）开始的那部分中置换匹配部分，因此只在 siroe.com 中置换。

$L 置换一域常值中不与重写规则相匹配的部分。

常值字符置换串 $$、 $%、 $@

字符 $、 % 和 @ 通常为重写规则模板中的元字符。若需插入一个这样的常值字符，须在字符前用美元符号 $ 作标记。也即， $$ 扩展为一个单一的美元符号 $ ； $% 扩展为一个单一的百分号 %（在此情况下百分号不解释为模板域分隔符）； $@ 扩展为一个单一的 at 符号 @（也不解释为域分隔符）。

LDAP 查询 URL 置换串 $]...[

一形如 $]ldap-url[的置换串解释为一个 LDAP 查询 URL，而且 LDAP 查询的结果被置换。标准 LDAP URL 中忽略主机和端口。主机和端口则在 msg.conf 文件中指定（local.ldaphost 和 local.ldapport 属性）。

也即， LDAP URL 应按如下格式指定，其中方括弧 [] 表示 URL 的可选部分。

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

dn 是必需的，它是一个指定搜索基的判别名。URL 中的可选的属性、范围和过滤器等部分进一步定义需返回什么信息。对于重写规则而言，所需的用于指定返回信息的属性是 mailRoutingSystem（或某个类似的属性）。范围可以是 base （默认）、 one 或 sub 中的任意一个。所需过滤器可请求返回这样的对象：其 mailDomain 的值匹配被重写的域。

如果 LDAP 目录规划包含属性 mailRoutingSystem 和 mailDomain，则决定用将一给定类型的地址路由到哪一个系统的可能的重写规则如下所示，其中将 LDAP URL 置换序列 $D 被用来在当前域名中置换到所创建的 LDAP 查询中：

```
.siroe.com \
  $U%$H$D@$]ldap:///o=siroe.com?mailRoutingSystem?sub? \
  (mailDomain=$D)
```

为了便于阅读，用反斜杠字符表示续行，使一个逻辑上的重写规则行呈现在两个物理行中。表 7-5 列出了 LDAP URL 置换序列。

表 7-5　LDAP URL 置换序列

置换序列	说明
$$	常值 $ 字符
$~ *account*	用户帐户主目录
$A	地址
$D	域名
$H	主机名 （全限定域名的第一部分）
$L	去掉任何诸如 ~ 或 _ 这样的特殊前导字符的用户名
$S	子地址
$U	用户名

常规数据库置换串 $(...)

形如 $（text）这样的置换串被特定处理。文本部分被用作访问特殊的常规数据库的密钥。该数据库包括在文件 /imta/config/imta_tailor 中用 IMTA_GENERAL_DATABASE 选项指定的文件，通常就是文件 /imta/db/generaldb.db。

该数据库是用实用工具 imta crdb 生成的。如果在数据库中找到“文本串”，则数据库的相关模板被置换。如果 “文本串”不与数据库中的任何条目匹配，重写过程失败，就好象是重写规则一开始就没有匹配成功。如果置换成功，从数据库抽取出的模板被重新扫描以寻找另外的置换串。但是，来自抽取出的模板中的 $（text）置换被禁止，以防止无限的递归引用。

作为一个例子，假定地址 jdoe@siroe.siroenet 匹配下面的重写规则：

```
.SIROENET $($H)
```

然后，要在常规数据库中查找文本串 siroe，如果找到，查找结果将用于重写规则模板中。假定查找 siroe 的结果是 $u%eng.siroe.com@siroenet。那么模板的输出为 jdoe@eng.siroe.com（也即，用户名 = jdoe, 主机或域描述 = eng.siroe.com），路由系统为 siroenet。

如果常规数据库存在，它应该在世界范围内都是可读的，这样才能确保运转正常。

应用指定映射 ${...}

形如 ${mapping,argument} 的置换串用于从 MTA 映射文件中查找和应用一个映射。mapping 字段用于指定要使用的映射表的名称，而 argument 则用于指定要通过映射的字符串。映射必须存在，而且如果成功必须在输出中设置 $Y 标记。如果不存在或没有设置 $Y，重写将失败。如果成功，映射结果被合并到模板的当前位置处并再次扩展。

这种机制可使 MTA 的重写过程以各种复杂方式进行扩展。例如，用户名的地址部分可有选择地分析并修改，它通常不是 MTA 重写过程所具备的特性。

客户提供的例程置换串 $[...]

形如 $[*image*、*routine*、*argument*] 置换串用于寻找和调用客户提供的例程。在 UNIX 的运行期，MTA 使用 dlopen 和 dlsym 从共享的库映像中动态地装载和调用指定的例程。例程以如下的参数表作为函数被调用：

status := *routine* (*argument*,*arglength*,*result*,*reslength*)

argument 和 *result* 分别为 252 字节长的字符串缓冲区。在 UNIX 中，*argument* 和 *result* 均作为字符串指针被传递，（例如在 C 中，其类型为 char*。）*arglength* 和 *reslength* 是以引用形式传递的有符号长整数。作为输入，*argument* 包含重写规则模板中的参数串，*arglength* 为该参数串的长度。作为返回，结果串应被置于 *result* 中，结果的长度所置于 *reslength* 中。结果串将替换重写规则模板中的“$[*image*,*routine*,*argument*]”。若重写规则失败，例程返回 0，若重写规则成功，则例程返回到 -1。

这种机制可使重写过程以所有类型的复杂方式扩展。例如，可实施对某些类型的名字服务的调用，并将结果用于对地址进行某种方式的修改。目录服务查找向前指引地址（例如，To: 地址），该地址通往主机 siroe.com，可按下面的重写规则执行。在第 147 页“针对方向和位置的重写规则（$B、$E、$F、$R）”中描述的 $F 使得此规则只适用于向前指引地址：

```
siroe.com $F$[LOOKUP_IMAGE,LOOKUP,$U]
```

当一向前指引地址 jdoe@siroe.com 匹配此重写规则时，将使 LOOKUP_IMAGE（UNIX 中的一个共享库）被装载到内存中，并使例程 LOOKUP 以 jdoe 为参数而被调用。例程 LOOKUP 应通过结果参数返回一个不同的地址，例如，John.Doe%eng.siroe.com，并返回值 -1 表示重写规则成功。结果串中的百分号（见第 134 页“重复重写模板 A%B”）使得重写过程以 John.Doe@eng.siroe.com 作为要重写的地址而再次启动。

在 UNIX 系统中，站点提供的共享库映像应该是世界范围内可读的。

单字段置换串 $&、 $!、 $*、 $#

单字段置换串从被重写的主机或域描述之中抽取出一个单一的子域。可供使用的单字段置换串参见表 7-6。

表 7-6　单字段置换串

控制序列	用法
$&n	在主机描述（不匹配或无法匹配某种类型的通配符）中置换 nth 元素，n=0,1,2,..,9。元素被圆点所分隔；左边的第一个元素为 0。如果所要求的元素不存在，重写失败。
$!n	在主机描述（不匹配或无法匹配某种类型的通配符）中置换 nth 元素，n=0,1,2,..,9。元素被圆点所分隔；右边的第一个元素为 0。如果所要求的元素不存在，重写失败。

表 7-6　单字段置换串（接上页）

控制序列	用法
$*n	在域描述（确与模式中的显式文本相匹配的部分）中置换 nth 元素，n=0,1,2,..,9。元素被圆点所分隔；左边的第一个元素为 0。如果所要求的元素不存在，重写失败。
$#n	在域描述（确与模式中的显式文本相匹配的部分）中置换 nth 元素，n=0,1,2,..,9。元素被圆点所分隔；右边的第一个元素为 0。如果所要求的元素不存在，重写失败。

假定地址 `jdoe@eng.siroe.com` 匹配下面的重写规则：

```
*.SIROE.COM      $U%$&0.siroe.com@mailhub.siroe.com
```

来自模板的结果为 `jdoe@eng.siroe.com`，以 `mailhub.siroe.com` 作为路由系统使用。

唯一串置换串

每次使用控制序列 $W 时都插入一个包含大写字母和数字的文本串，此文本串被设计为唯一的和不可重复的。当必须创建无重复地址信息时， $W 是很有用的。

针对源通道的重写规则（$M、 $N）

有可能有这样的重写规则，它只在与指定的源通道相关联时发挥作用。当一个短格式名具有两种含义时这是很有用的：

1. 当它出现在到达一个通道的邮件中时。
2. 当它出现在到达另一个通道的邮件中时。

针对源通道的重写都与使用中的通道程序以及通道关键字 `rules` 和 `norules` 相关联。如果 `norules` 被指定在与执行重写的 MTA 组件相关联的通道上，则不进行针对通道的重写检查。如果 `rules` 被指定在通道上，则强制执行针对通道的规则检查。关键字 `rules` 为默认值

针对源通道的重写不与匹配一给定地址的通道相关联。这只取决于执行重写的 MTA 组件以及该组件的通道表条目。

针对通道的重写检查由出现在规则的模板部分中的控制序列 $N 或 $M 所触发。跟在 $N 或 $M 后面，直到 at 符号（@），百分号（%），或随后的 $N,$M, $Q,$C,$T, 或 $? 之前的字符序列，被解释为通道名。

例如，如果 *channel* 当前没有执行重写，$M*channel* 致使规则失败。如果 *channel* 正执行重写，$N*channel* 致使规则失败。可以指定多重的 $M 和 $N 子句。如果多重 $M 子句中的任何一个匹配成功，则规则成功。如果多重 $N 子句中的任何一个匹配成功，则规则失败。

针对目标通道的重写规则 （$C、 $Q）

有可能有这样的重写规则，它的应用取决于邮件正在其列队中等侯的那个通道。当某台主机有两个名字时这很有用，一个名字为一个主机组所知晓，剩下的一个为另一个主机所知晓。通过使用不同通道向每组主机发送邮件，地址可被重写以与主机相联系，而且所用的名字是每个主机组都知晓的。

针对目标通道的重写与邮件正在其列队中等侯处理的那个通道，以及该通道上的通道关键字 `rules norules` 相关联。如果将 `norules` 指定在目标通道上，不执行针对通道的重写检查。如果将 `rules` 指定在目标通道上，则强制执行针对通道的规则检查。关键字 `rules` 为默认值。

针对目标通道的重写不与给定地址相匹配的通道关联。这主要取决于邮件信封上的 `To:` 地址。当一邮件进入队列时，信封上的 `To:` 地址被首次重写以确定邮件进入哪个通道队列。在重写信封上的 `To:` 地址的过程中，任何 `$C` 和 `$Q` 这样的控制序列均被忽略。在信封上的 `To:` 地址被重写、目标通道被决定之后，控制序列 `$C` 和 `$Q` 才有效，这是由于与该邮件相关的其他地址要被重写。

针对目标通道的重写检查由规则的模板部分中出现的控制序列 `$C` 或 `$Q` 所触发。跟在 `$C` 或 `$Q` 之后，直到 at 字符 (@)，百分号字符 (%)，或另外的 `$N`， `$M`， `$C`， `$Q`, `$T` 或 `$?` 之前的字符序列，被解释为通道名。

例如，如果 *channel* 不是目标通道，则 `$Q`*channel* 致使规则失败。另一个例子，如果 *channel* 是目标通道，则 `$C` *channel* 致使规则失败。可指定多重的 `$Q` 和 `$C` 子句。如果多重 `$Q` 子句中的任何一个匹配成功，则规则成功。如果多重 `$C` 子句中的任何一个匹配成功，则规则失败。

针对方向和位置的重写规则 （$B、 $E、 $F、 $R）

有时需要指定只应用于信封地址，或只应用于标题地址的重写规则。如果被重写的地址不是信封地址，控制序列 `$E` 强制重写失败。如果被重写的地址不是来自邮件标题或正文，控制序列 `$B` 强制重写失败。这些控制序列对重写无其他影响，并可出现在重写规则模板的任何地方。

地址也可按方向分类。向前指引地址是指 `To:`， `Cc:`， `Resent-to:` 或其他指向目标的标题行或信封行。向后指引地址就是 `From:`，`Sender:` 或 `Resent-From:` 之类的指向源的地址。如果地址为向前指引，控制序列 `$F` 子句使重写被应用。如果地址为向后指引，控制序列 `$R` 子句使重写被应用。

针对主机位置的重写 （$A、 $P、 $S、 $X）

环境偶尔也要求对出现于地址中的主机名的位置敏感的重写。地址中的主机名可以几种不同的环境出现：

- 在一源路由中
- 到 at 符号 （@）的右边
- 到本地部分百分号 （%）的右边
- 到本地部分的感叹号的左边

在一般情况下，不管主机名出现在何处，都应以相同的方式处理。在某些情况下可能需要特殊的处理。

有四种控制序列可用于基于地址中主机位置的匹配控制。

- $S 指定规则可匹配一个从源路由抽取出的主机。
- $A 指定规则可匹配在符号 @ 右边的主机。
- $P 指定规则可匹配在符号 % 右边的主机
- $X 指定规则可匹配在感叹号 (!) 左边的主机。

如果主机处于上述以外的位置，规则失败。这些序列可合并为一个单一的重写规则。例如，如果 $S 和 $A 被指定，规则匹配在源路由或 @ 符号右边指定的主机。不指定这些序列中的任何一个等同于指定全部；规则可进行与位置无关的匹配。

改变当前标记值 $T

控制序列 $T 用于改变当前重写规则标记。在配置文件和域数据库中查找之前，重写规则标记被添加到所有重写规则模式的前面。跟在 $T 之后，直到 @，%，$N，$M，$Q，$C，$T 或 $? 之前的文本被取出作为新的标记。

在处理一些特殊地址形式（当遇见一个特定的组件时，地址被整个改变）时标记十分有用。例如，假定当在源路由中的找到特殊的主机名 internet，该名字应从地址中删除，作为结果的地址被强制匹配，而不管 TCP-DAEMON 通道。

这可以通过像下面这样的规则来实现 (localhost 被假定为本地主机的正式名)：

```
internet                $S$U@localhost$Tmtcp-force|

mtcp-force|.            $U%$H@TCP-DAEMON
```

第一个规则将匹配特殊主机名 internet，如果它出现在源路由中。它强制匹配 internet 而不管本地通道，以确保可从地址中将之删除。于是重写标记被设定。重写继续进行，但由于标记的缘故，没有任何正常的规则能够匹配。最后，借助标记尝试默认规则，且该集的第二个规则被激活，不顾任何其他标准地强制匹配地址，而不管 TGP-DAEMON 通道。

控制与重写相关的出错消息 ($?)

当重写和通道匹配失败时，MTA 提供默认的出错消息。改变这些消息的功能在某些情况下是很有用的。例如，如果某人试着向以太网路由器邮箱发送邮件，则像 “Our routers cannot accept mail” 这样的提示可能比通常的提示 “illegal host/domain specified” 包含了更多的信息。

一种特殊的控制序列可用于改变规则失败时会被打印出来的出错消息。序列 $? 用于指定一个出错消息。跟在 $? 之后，直到 at 符号 (@)，百分号 (%)，$N，$M，$Q，$C，$T 或 $? 之前的文本被取出作为出错消息文本，如果重写的结果无法匹配任何通道，该出错消息会被打印出来。出错消息的设置具有记忆性，贯穿整个重写过程均有效。

包含 $? 的规则操作类似于其他规则。一规则只包含 $? 而不包含别的内容，这种特殊情况须特别注意，重写过程在未改变邮箱或地址的主机部分的情况下终止，并且主机是按字面含义在通道表中查找的。这样的查找会如预期的那样失败，并将出错消息作为一个结果返回。

例如，假定 MTA 配置文件的最后一个重写规则如下：

```
. $?Unrecognized address; contact postmaster@siroe.com
```

在这个例子中，任何导致失败的不能识别的主机或域描述在其失败处理过程中都将生成如下的出错消息：`Unrecognized address; contact postmaster@siroe.com`.

处理大量重写规则

MTA 总是从 `imta.cnf` 文件中读入所有的重写规则并其储存在一个散列表中。使用编译的配置文件可免除因每次需要相关信息时就去读配置文件而付出的额外开销；仍旧用一个散列表来储存所有的重写规则。此方案对于小规模或中等规模数量的重写规则是适当的。然而，一些站点需要多达 10,000 个重写规则甚至更多，这将消耗惊人数量的存储空间。

MTA 通过提供一种可选的工具来解决这一问题，该工具可将大量的重写规则存储在一个带辅助索引的数据文件中。每当读常规配置文件时， MTA 都要检查域数据库的存在情况。如果该数据库存在就将之打开，而且每当从配置文件中找到的规则匹配失败时就去参考该数据库。域数据库只有当给定的规则没有在匹配文件中找到时才被检查，因此总能将规则添加到配置文件中以覆盖数据库中的规则。在默认状态下，域数据库用于存储与受托域相关的重写规则。IMTA_DOMAIN_DATABASE 属性被储存在 `imta_tailor` 文件中。默认的数据库位置是 *server-instance*`/imta/db/domaindb.db`。

备注	请不要手工编辑此文件。当受托域在 Directory Server 中创建时， `dirsync` 过程将覆盖任何存在的域数据库，所以任何定制编辑的内容都将丢失。

测试重写规则

您可用 `imsimta test -rewrite` 命令测试重写规则。限定词 `-noimage` 用于在重新编译新配置之前测试对配置文件所做的修改。

使用这一工具重写几个地址时，用限定词 `-debug` 是很有用的。因为它可逐步显示重写地址的过程。例如，键入如下的命令：

```
% imsimta test -rewrite -debug joe@siroe.com
```

有关实用工具 `imsimta test -rewrite` 的详细描述，请参见 **iPlanet Messaging Server Reference Manual**。

重写规则示例

下面例子提供重写规则样本以及如何依据规则重写样本地址

假定系统 SC.CS.SIROE.EDU 的配置文件包含的重写规则如图 7-2 所示。

图 7-2 重写规则示例

```
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 7-7 所示为一些样本地址以及它们是如何依据重写规则被重写和路由的。

表 7-7 样本地址和重写

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

表 7-7　样本地址和重写（接上页）

初始地址	重写为	路由到
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

基本而言，这些重写规则表述的是：如果主机名是我们的短格式名（sc,sc1 或 sc2）中的一个，或者是我们的全名（sc.cs.siroe.edu，等等）中的一个，则将其扩展为全名，并路由给我们。将 cs.cmu.edu 添加到一个只有单部分的短格式名的后面，然后重试。将后面跟有 .cs 的单部分转换为后面跟有 .cs.siroe.edu 的单部分，然后重试。同样，将 cs.siroe 转换为 cs.siroe.edu，然后重试

如果名字为 sd.cs.siroe.edu（可能是我们直接连接的某个系统 ），重写并将之路由到该处。如果主机名是子域 cs.siroe.edu 中的任何其他名字，则路由到 ds.cs.siroe.edu（子域 .cs.siroe.edu 的网关）。如果主机名是子域 siroe.edu 中的任何其他名字，则路由到 cds.adm.siroe.edu（子域 siroe.edu 的网关）。如果主机名是顶层域 .edu 中的任何其他名字，则路由到 gate.adm.siroe.edu（它可能有能力将邮件路由到正确的目标）。如果用的是域常值，也将其发送到 gate.adm.siroe.edu。

大部分重写规则应用（如前面的例子）在任何情况下都不会改变地址的用户名（或邮箱）部分。当 MTA 用作通往不符合 RFC822 的邮件系统的接口时，可使用改变地址的用户名部分的功能。对于这样的邮件系统，有必要将主机或域描述部分填充到地址的用户名部分。如果必须使用此功能，须格外小心。

第 8 篇

配置通道定义

本章说明如何使用 MTA 配置文件 `imta.cnf` 中的通道关键字定义。在阅读本章前，请先阅读第 6 篇，“关于 MTA 服务与配置”以及第 87 页“通道定义”和第 91 页“MTA 配置文件”。本章包括以下各节：

- 按字母顺序列示的通道关键字
- 按功能分类的通道关键字
- 配置通道的默认值
- 配置 SMTP 通道
- 配置邮件处理和传递
- 配置地址处理功能
- 配置邮件头处理功能
- 附件与 MIME 处理
- 邮件大小限制、用户定额和特权
- 在 MTA 队列 中创建文件
- 指定邮箱过滤器文件的位置
- 配置日志记录和调试
- 其它关键字

备注 在修改了 `imta.cnf` 文件中的通道定义后，您必须重新启动任何如 SMTP 服务器这样的程序或通道：它们只在用命令 `imsimta start` 启动时一次性地加载配置数据。如果使用的是已编译的配置，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方面的详细信息，请参阅 **iPlanet Messaging Server Reference Manual**。

按字母顺序列示的通道关键字

下表为字母化的关键字列表。

表 8-1　字母化的通道关键字

关键字	页	关键字	页	关键字	页	关键字	页
733	191	822	191	addreturnpath	196	addrsperfile	206
aliaslocal	198	aliaspostmaster	125	allowetrn	173	allowswitchchannel	181
authrewrite	183	backoff	186	bangoverpercent	193	bangstyle	191
bidirectional	186	blocketrn	173	blocklimit	206	cacheeverything	178
cachefailures	178	cachesuccesses	178	channelfilter	209	charset7	174
charset8	174	charsetesc	174	checkehlo	172	commentinc	197
commentmap	197	commentomit	197	commentstrip	197	commenttotal	197
connectalias	194	connectcanonical	194	copysendpost	124	copywarnpost	124
daemon	182	datefour	201	datetwo	201	dayofweek	202
defaulthost	194	defaultmx	180	defaultnameservers	181	deferred	186
defragment	204	dequeue_removeroute	199	destinationfilter	209	disableetrn	173
domainetrn	173	domainvrfy	174	dropblank	195	ehlo	172
eightbit	174	eightnegotiate	174	eightstrict	174	errsendpost	124
errwarnpost	124	expandchannel	189	expandlimit	189	exproute	193
fileinto	209	filesperjob	188	filter	209	forwardcheckdelete	179
forwardchecknone	179	forwardchecktag	179	header_733	191	header_822	191
header_uucp	191	headerlabelalign	203	headerlinelength	203	headerread	200
headertrim	200	holdexquota	206	holdlimit	189	identnone	179
identnonelimited	179	identnonenumeric	179	identnonesymbolic	179	identtcp	179
identtcplimited	179	identtcpsymbolic	179	ignoreencoding	204	immnonurgent	
improute	193	includefinal	124	indenttcpnumeric	179	inner	200
innertrim	200	interfaceaddress	178	interpretencoding	204	language	204
lastresort	181	linelength	205	linelimit	206	localvrfy	174
logging	208	loopcheck	208	mailfromdnsverify	174	master	186
master_debug	208	maxblocks	205	maxheaderaddrs	202	maxheaderchars	202

表 8-1　字母化的通道关键字（接上页）

关键字	页	关键字	页	关键字	页	关键字	页
maxjobs	188	maxlines	205	maxprocchars	203	maysaslserver	182
maytls	183	maytlsclient	183	maytlsserver	183	missingrecipientpolicy	195
msexchange	183	multiple	206	mustsaslserver	182	musttls	183
musttlsclient	183	musttlsserver	183	mx	180	nameservers	181
noaddreturnpath	196	nobangoverpercent	193	noblocklimit	206	nocache	178
nochannelfilter	209	nodayofweek	202	nodefaulthost	194	nodeferred	186
nodefragment	204	nodestinationfilter	209	nodropblank	195	noehlo	172
noexproute	193	noexquota	206	nofileinto	209	nofilter	209
noheaderread	200	noheadertrim	200	noimproute	193	noinner	200
noinnertrim	200	nolinelimit	206	nologging	208	noloopcheck	208
nomailfromdnsverify	174	nomaster_debug	208	nomsexchange	183	nomx	180
nonrandomemx	180	nonurgentbackoff	186	nonurgentblocklimit	189	nonurgentnotices	123
noreceivedfor	196	noreceivedfrom	196	noremotehost	194	norestricted	196
noreturnaddress	125	noreturnpersonal	125	noreverse	195	normalbackoff	186
normalblocklimit	189	normalnotices	123	norules	199	nosasl	182
nosaslserver	182	nosaslswitchchannel	182	nosendetrn	173	nosendpost	124
noservice	190	noslave_debug	208	nosmtp	172	nosourcefilter	209
noswitchchannel	181	notices	123	notls	183	notlsclient	183
notlsserver	183	novrfy	174	nowarnpost	124	nox_env_to	201
percentonly	193	percents	191	personalinc	197	personalmap	197
personalomit	197	personalstrip	197	pool	187	port	178
postheadbody	125	postheadonly	125	randommx	180	receivedfor	196
receivedfrom	196	remotehost	194	restricted	196	returnaddress	125
returnenvelope	125	returnpersonal	125	reverse	195	routelocal	193
rules	199	rules	199	saslswitchchannel	182	sendetrn	173
sendpost	124	sensitivitycompany-confidential	203	sensitivitynormal	203	sensitivitypersonal	203
sensitivityprivate	203	service	190	sevenbit	174	silentetrn	173
single	206	single_sys	182	slave	186	slave_debug	208
smtp	172	smtp_cr	172	smtp_crlf	172	smtp_crorlf	172

表 8-1　字母化的通道关键字（接上页）

关键字	页	关键字	页	关键字	页	关键字	页
smtp_lf	172	sourceblocklimit	206	sourcecommentinc	197	sourcecommentmap	197
sourcecommentomit	197	sourcecommentstrip	197	sourcecommenttotal	197	sourcefilter	209
sourcepersonalinc	197	sourcepersonalmap	197	sourcepersonalomit	197	sourcepersonalstrip	197
sourceroute	191	streaming	176	subaddressexact	198	subaddressrelaxed	198
subaddresswild	198	subdirs	207	submit	209	suppressfinal	124
switchchannel	181	threaddepth	189	tlsswitchchannel	183	unrestricted	196
urgentbackoff	186	urgentblocklimit	189	urgentnotices	123	useintermediate	124
user	209	uucp	191	viaaliasoptional	199	viaaliasrequired	199
vrfyallow	174	vrfydefault	174	vrfyhide	174	warnpost	124
x_env_to	201						

按功能分类的通道关键字

下表为关键字的分类列表。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）

关键字	页	定义
地址处理		
733	191	在信封中使用 % 路由；与 percents 同义。
822	191	在信封中使用源路由；与 sourceroute 同义。
addreturnpath	196	在该通道排队的邮件上添加 Return-path: 报头。
aliaslocal	198	在别名文件和别名数据库中查找重写的地址。
authrewrite	183	用于在源通道上使 MTA 将认证的始发者信息 （如果有的话）传送到报头中。
bangoverpercent	193	把 A!B%C 分组为 A!(B%C)
bangstyle	191	在信封中使用 UUCP ! 路由；与 uucp 同义。
defaulthost	194	指定一个域名以用于完成地址填写
dequeue_removeroute	199	从信封的 To: 地址中移除源路由。
exproute	193	当地址传送至远程系统时需具有显式路由。

表 8-2　　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
holdlimit	189	当信封收件人地址数量超过此限量时暂不发送邮件。
improute	193	该通道地址的隐式路由
missingrecipientpolicy	195	设置策略，确定如何使缺少任何收件人报头的邮件合法化 （即添加什么样的报头）。
noaddreturnpath	196	排列邮件时，不添加 Return-path: 报头。
nobangoverpercent	193	把 A!B%C 分组为 (A!B)%C
nodefaulthost	194	不指定完成地址填写需使用的域名
noexproute	193	该通道地址无显式路由
noimproute		该通道地址无隐式路由
noreceivedfrom	196	构建 Received: 报头行，但不包括原信封的 From: 地址。
noremotehost	194	使用本地主机的域名作为默认域名，以此完成地址填写
norestricted	196	与 unsrestricted 同义。
noreverse	195	免除对邮件地址进行地址逆向处理
norules	199	不在该通道上强制进行针对具体通道的重写规则检查。
percentonly	193	忽略惊叹号路径。在信封中使用 % 路由。
percents	191	在信封中使用 % 路由；与 733 同义。
remotehost	194	使用远程主机名作为默认域名，以此完成地址填写
restricted	196	通道连接到需要编码的邮件系统。
reverse	195	按照地址反向数据库或反向映射检查的地址
routelocal	193	可使 MTA 在通道上重写地址时以 “短路” 方式中断地址中的任何显式路由。
rules	199	在该通道上强制进行针对具体通道的重写规则检查。
sourceroute	191	与 822 同义。
subaddressexact	198	在匹配条目期间不进行特殊的子地址处理；整个邮箱 （包括子地址）必须与一条目匹配，以使别名被视为与之匹配。
subaddressrelaxed	198	在寻找精确匹配以及与之匹配的格式名称 +* 后， MTA 应只在名称部分的匹配情况再次检查。
subaddresswild	198	在寻找包括整个子地址在内的精确匹配项，MTA 下一步应寻找格式名称 +* 的条目。
unrestricted	196	指示 MTA 不进行 RFC 1137 编码和解码。
uucp	191	在信封中使用 UUCP! 路由；与 bangstyle （惊叹号样式）同义。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
viaaliasoptional	199	不要求与通道匹配的最终收件人地址一定要由一别名生成。
viaaliasrequired	199	与通道匹配的最终收件人地址必须由一别名生成。
附件与 MIME 处理		
defragment	204	而将排列在通道中的部分邮件放置在整理碎片通道队列。
ignoreencoding	204	忽略入站邮件上的 Encoding: 报头。
interpretencoding	204	如果需要，则翻译入站邮件上的 Encoding: 报头。
nodefragment	204	可关闭整理碎片功能。
字符集和八位数据		
charset7	174	与 7 位文本邮件相关的默认字符集
charset8	174	与 8 位文本邮件相关的默认字符集
charsetesc	174	与 7 位文本邮件相关的默认字符集，包括换码字符
eightbit	174	通道支持八位字符。
eightnegotiate	174	通道应尽可能协调八位传输的使用。
eightstrict	174	拒绝包括未经协调的八位数据的邮件。
sevenbit	174	不支持八位字符；八位字符必须编码。
在 MTA 队列区域创建文件		
addrsperfile	206	可与通道队列中的单一邮件文件相关的收件人最大数量限制
expandchannel	189	指定用于执行由于使用 expandlimit 而导致的延迟扩展的通道。
expandlimit	189	当地址数量超过此限制时，对入站邮件进行 “脱机”处理。
multiple	206	不限制邮件文件收件人的数量，但 SMTP 通道将使用默认值 99。
single	206	将为通道上的每个目标地址创建分开的邮件副本。
single_sys	206	为所用的每个目标系统创建邮件的一个单独副本。
subdirs	207	用于指定子目录的数量，以在其上传送通道队列的邮件。
报头		
authrewrite	183	用于在源通道上使 MTA 将认证的始发者信息 （如果有的话）传送到报头中。
commentinc	197	不在邮件标题行中对注释做任何改动。
commentmap	197	通过 COMMENT_STRINGS 映射表运行邮件标题行中的注释串。
commentomit	197	删除邮件标题行中的注释。
commentstrip	197	从邮件标题行的注释字段中删除有问题的字符。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
commenttotal	197	移除所有标题行中的注释 （括号中的资料）， Received: 标题行除外。建议不要使用。
datefour	201	将所有年份字段扩展至四位数。
datetwo	201	移除四位数日期的前两位数。可为需要两位数日期的邮件系统提供兼容性；但决不应用于任何其它目的。
dayofweek	202	保留星期信息并将该信息添加到日期和时间报头 （如果缺失的话）。
defaulthost	194	指定一个域名以用于完成地址填写
dropblank	195	移除入站邮件中的非法空报头。
header_733	191	在邮件头中使用 % 路由。
header_822	191	在邮件头中使用源路由。
headerlabelalign	203	用于控制在该通道上排列的邮件头的成行点；需使用一整数值的变量。
headerlinelength	203	用于控制在该通道上排列的邮件头的长度。
headerread	200	在处理原邮件头之前，将一个选项文件中的报头休整规则 （于排列邮件之时）应用于邮件头 （使用时需格外小心）。
headertrim	200	在处理原邮件头之后，将一个选项文件中的报头休整规则应用于邮件头。
header_uucp	191	在报头中使用！路由
inner	200	分析邮件并重写内部报头。
innertrim	200	将一个选项文件中的报头休整规则应用于内部邮件头 （使用时需小心）。
language	204	用于指定报头的默认语言。
maxheaderaddrs	202	用于控制一行上可以显示多少个地址。
maxheaderchars	202	用于控制一行上可以显示多少个字符。
missingrecipientpolicy	195	设置策略，确定如何使缺少任何收件人报头的邮件合法化 （即添加什么样的报头）。
nodayofweek	202	用于从日期和时间报头中删除星期。可为不能处理此种信息的邮件系统提供兼容性；但决不应用于任何其它目的。
nodefaulthost	194	不指定完成地址填写需使用的域名
nodropblank	195	不移除入站邮件中的非法空报头。
noheaderread	200	不应用选项文件的报头休整规则。
noheadertrim	200	不应用选项文件的报头休整规则。
noinner	200	不重写内部邮件标题行。
noinnertrim	200	不在内部邮件头中应用报头休整功能。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
noreceivedfor	196	构建 Received: 报头行，但不包括任何信封收件人信息。
noreceivedfrom	196	构建 Received: 报头行，但不包括原信封的 From: 地址。
noremotehost	194	使用本地主机的域名作为默认域名，以此完成地址填写
noreverse	195	免除对通道中排列的邮件地址进行地址逆向处理
norules	199	不在该通道上强制进行针对具体通道的重写规则检查。
nox_env_to	201	删除 X-Envelope-to 标题行。
personalinc	197	不在邮件标题行中对人名字段做任何改动。
personalmap	197	通过 PERSONAL_NAMES 映射表运行人名。
personalomit	197	从邮件标题行移除人名字段。
personalstrip	197	移除标题行人名字段中有问题的字符。
receivedfor	196	如果某邮件只定址给一个信封收件人，则用来将该信封的 To: 地址包括在建构的 Received: 标题行中。
receivedfrom	196	如果 MTA 已更改了信封的 From: 地址，则在建构入站邮件的 Received: 标题行时包括原信封的 From: 地址。
remotehost	194	使用远程主机名作为默认域名，以此完成地址填写
restricted	196	通道连接到需要此编码的邮件系统。
reverse	195	按照地址反向数据库或反向映射检查地址
rules	199	在该通道上强制进行针对具体通道的重写规则检查。
sensitivitycompany-confidential	203	Companyconfidential 是所接受邮件的阅读权限上限 （亦称敏感度）。
sensitivitynormal	203	Normal 是所接受邮件的阅读权限上限。
sensitivitypersonal	203	Personal 是所接受邮件的阅读权限上限。
sensitivityprivate	203	Private 是所接受邮件的阅读权限上限。
sourcecommentinc	197	保留入站邮件标题行中的注释。
sourcecommentmap	197	通过源通道运行标题行中的注释字串。
sourcecommentomit	197	从入站邮件的标题行中移除注释，例如， To:、 From: 和 Cc: 报头。
sourcecommentstrip	197	从入站邮件标题行的注释字段中删除有问题的字符。
sourcecommenttotal	197	移除入站邮件中的注释 （括号中的资料）。
sourcepersonalinc	197	不在入站邮件标题行中对人名做任何改动。
sourcepersonalmap	197	通过源通道运行人名。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
sourcepersonalomit	197	从入站邮件标题行中移除人名字段。
sourcepersonalstrip	197	移除入站邮件标题行人名字段中有问题的字符。
unrestricted	196	指示 MTA 不进行 RFC 1137 编码和解码。
x_env_to	201	启用 X-Envelope-to 标题行生成功能。
入站通道的匹配与切换		
allowswitchchannel	181	允许从 switchchannel 通道切换到此通道
nosaslswitchchannel	182	SASL 认证成功时不切换到此通道
noswitchchannel	181	不应在该通道上做收发切换。
switchchannel	181	从服务器通道切换到与原主机相关的通道。
saslswitchchannel	182	在客户程序成功使用 SASL 的情况下，使入站连接切换到指定的通道。
tlsswitchchannel	183	TLS 协调成功时切换到另一通道。
日志记录与调试		
logging	208	在日志记录文件中记录邮件入队和出队信息并启用某通道的日志记录功能。
loopcheck	208	将字串放置在 SMTP EHLO 应答标志区，以便 MTA 检查其自身是否在与之通信。
master_debug	208	在通道的主程序输出中创建调试输出。
nologging	208	不在日志记录文件中记录邮件的入队和出队信息。
noloopcheck	208	不在 SMTP EHLO 应答标志区内放置字串。
nomaster_debug	208	不在通道的主程序输出中创建调试输出。
noslave_debug	208	不生成从属调试输出。
slave_debug	208	生成从属调试输出。
长地址列表或报头		
expandchannel	189	指定用于执行由于使用 expandlimit 而导致的延迟扩展的通道。
expandlimit	189	当地址数量超过此限制时，以 “脱机” 方式处理入站邮件。
holdlimit	189	当地址数量超过此限制时，暂不处理邮件。
maxprocchars	203	可处理和重写的报头之最大长度。
邮箱过滤器		
channelfilter	209	通道过滤器文件的位置；同 destinationfilter。
destinationfilter	209	应用于出站邮件的通道过滤器文件的位置。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
fileinto	209	当应用邮箱过滤器的 fileinto 操作时，用于指定对地址的作用。
filter	209	用于指定用户过滤器文件的位置。
nochannelfilter	209	不在出站邮件上进行通道过滤。亦称 nodestinationfilter。
nodestinationfilter	209	不在出站邮件上进行通道过滤。
nofileinto	209	邮箱过滤器的 fileinto 运算符不起作用。
nofilter	209	不进行用户邮箱过滤。
nosourcefilter	209	不在入站邮件上进行通道过滤。
sourcefilter	209	用于指定入站邮件的通道过滤器文件的位置。
通知与 Postmaster 邮件 （全面的通知操作程序，请见 119 页）		
aliaspostmaster	125	将在正式通道名上定址到用户名 postmaster 的邮件重定向到 postmaster@local-host，其中的 local-host 是本地主机名（即本地通道名）。
copysendpost	124	向 Postmaster 发送失败通知副本，除非出问题的邮件原发者的地址是空的。
copywarnpost	124	向 Postmaster 发送警告讯息副本，除非无法传递邮件的发件人地址是空的。
errsendpost	124	仅当不能向发件人返回通知时才向 Postmaster 发送失败通知副本。
errwarnpost	124	当不能向发件人返回通知时才向 Postmaster 发送警告讯息副本。
includefinal	124	在传递通知中包括收件人地址的最终格式。
nonurgentnotices	123	对于具有非紧急优先级的邮件，指定在发送通知和退回邮件之前可以耗费的时间量。
noreturnaddress	125	用 RETURN_ADDRESS 选项值作为 postmaster 的地址名。
noreturnpersonal	125	用 RETURN_PERSONAL 选项值作为 postmaster 的人名。
normalnotices	123	对于具有普通优先级的邮件，指定在发送通知和退回邮件之前可以耗费的时间量。
nosendpost	124	禁止向 Postmaster 发送所有失败邮件副本。
notices	123	指定在发送通知和退回邮件之前可以耗费的时间量。
nowarnpost	124	禁止向 Postmaster 发送警告讯息副本。
postheadbody	125	既返回邮件头也返回邮件内容。
postheadonly	125	仅向 Postmaster 返回邮件头。
returnaddress	125	用于指定本地 postmaster 的返回地址。
returnenvelope	125	控制使用空白的信封返回地址。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
returnpersonal	125	设置本地 postmaster 的人名。
sendpost	124	允许向 Postmaster 发送所有失败邮件的副本。
suppressfinal	124	如果有原地址格式，则在通知邮件中抑制使用最终的地址格式。
urgentnotices	123	对于具有紧急优先级的邮件，指定在发送通知和退回邮件之前可以耗费的时间量。
useintermediate	124	使用在列表扩展之后产生的 （但在生成用户邮箱名之前形成的）中间格式地址。
warnpost	124	允许向 Postmaster 发送警告讯息副本。
处理提交的控制和作业项 （细分的功能单位，请见第 184 页表 8-7）		
backoff	186	传递不成功之邮件的重新传递频率。可用以下关键字替换：normalbackoff， nonurgentbackoff， urgentbackoff。
bidirectional	186	由主程序和从属程序为之提供服务的通道。
deferred	186	承认并执行 Deferred-delivery: 标题行。
expandchannel	189	指定用于执行由于使用 expandlimit 而导致的延迟扩展的通道。
expandlimit	189	当地址数量超过此限制时，对入站邮件进行 “脱机”处理。
filesperjob	188	单次作业所能处理的队列条目的数量。
immnonurgent		在提交紧急、普通和非紧急邮件后立即启动传递。
master	186	由主程序 （master）为之提供服务的通道。
maxjobs	188	通道中能够同时运行的最大任务数量。
nodeferred	186	指定 Deferred-delivery: 标题行不予以执行。
nonurgentbackoff	186	尝试传递非紧急邮件的频率。
nonurgentblocklimit	189	将大小大于此值的邮件的优先级强制定义为低于非紧急优先级 （第二等优先级），这意味着此邮件将一直等待下一个任务周期，以得到更进一步的处理。
normalbackoff	186	尝试重新传递正常邮件的频率。
normalblocklimit	189	将大小大于此值的邮件强制定义为非紧急优先级。
noservice	190	对进入此通道的邮件所进行的服务转换必须 CHARSET-CONVERSION 启用。
pool	187	用于为某通道指定一个池。后面必须跟有池的名称，当前通道中的传递任务都应合并到这个池中。
service	190	不论 CHARSET-CONVERSION 条目为何，都无条件地启用服务转换功能。
slave	186	由主程序 （slave）为之提供服务的通道。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
threaddepth	189	使用多线程 SMTP 客户机触发新线程的邮件数量。
urgentbackoff	186	尝试重新传递紧急邮件的频率。
urgentblocklimit	189	将大小大于此值的邮件强制定义为普通优先级。
user	209	在传递通道上使用，以此指示在哪个用户名下运行。
阅读权限		
sensitivitycompany-confidential	203	接受之邮件的阅读权限上限。
sensitivitynormal	203	Normal 是所接受邮件的阅读权限上限。
sensitivitypersonal	203	Personal 是所接受邮件的阅读权限上限。
sensitivityprivate	203	Private 是所接受邮件的阅读权限上限。
邮件大小限制、用户定额和特权		
blocklimit	206	每封邮件允许的最大 MTA 信息块数量。
holdexquota	206	暂不传递超定额用户的邮件。
holdlimit	189	当地址数量超过此限制时，暂不传递入站邮件。
linelength	205	以通道为基础限制邮件行长度的最大允许值。
linelimit	206	每封邮件允许的最多行数量。
maxblocks	205	用于指定邮件中允许的最大信息块数量。
maxlines	205	用于指定邮件中允许的最多行数量。
noblocklimit	206	不限制每封邮件允许的 MTA 信息块数量。
noexquota	206	对于超定额的用户，发送给其的任何邮件都将返回至发件人。
nolinelimit	206	不限制每封邮件允许的行数量。
nonurgentblocklimit	189	将大小大于此值的邮件的优先级强制定义为低于非紧急优先级 （第二等优先级），这意味着此邮件将一直等待下一个任务周期，以得到更进一步的处理。
normalblocklimit	189	将大小大于此值的邮件强制定义为非紧急优先级。
sourceblocklimit	206	每封入站邮件允许的最大 MTA 信息块数量。
urgentblocklimit	189	将大小大于此值的邮件强制定义为普通优先级。
SMTP 认证、 SASL 和 TLS （细分的功能单位，请见 182）		
authrewrite	183	用于在源通道上使 MTA 将认证的始发者信息 （如果有的话）传送到报头中。
maysaslserver	182	允许客户程序尝试使用 SASL 认证。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
maytls	183	使 MTA 给外来连接提供 TLS 并在外发连接上尝试 TLS。
maytlsclient	183	如果发送到某支持 TLS 的 SMTP 服务器， MTA SMTP 客户程序将在发送出站邮件时尝试使用 TLS。
maytlsserver	183	MTA SMTP 服务器将通告其对 STARTTLS 扩展程序的支持，并于接收邮件之时允许使用 TLS。
msexchange	183	用于在 TCP/IP 通道上通知 MTA 这是一个可与 Microsoft Exchange 网关和客户机通信的通道。
mustsaslserver	182	除非远程客户机能成功地认证，否则 SMTP 服务器将不接受邮件。
musttls	183	强制在出站和入站连接中使用 TLS。
musttlsclient	183	MTA SMTP 客户机将在发送出站邮件时强制使用 TLS （MTA 将发出 STARTTLS 命令，而且该命令必须成功执行）。
musttlsserver	183	MTA SMTP 服务器将通告其对 STARTTLS 扩展程序的支持，并于接收入站邮件之时强制使用 TLS。
nomsexchange	183	默认值。
nosasl	182	不允许或不尝试 SASL 认证。
nosaslserver	182	不允许 SASL 认证。
notls	183	不允许或不尝试 TLS 认证。
notlsclient	183	MTA SMTP 客户机将不在出站连接上尝试使用 TLS （系统将在出站连接期间不执行 STARTTLS 命令）。
notlsserver	183	MTA SMTP 服务器将不允许在入站连接上使用 TLS （SMTP 服务器将不通告有 STARTTLS 扩展程序，同时也不接受这一命令）。
saslswitchchannel	182	在客户机成功使用 SASL 的情况下，使外来连接切换到指定的通道。
tlsswitchchannel	183	在客户机成功使用 TLS 的情况下，使外来连接切换到指定的通道。这需要一个值，用以说明切换到哪个通道。
SMTP 命令和协议 （细分的功能单位，请见第 170 页表 8-4）		
allowetrn	173	执行 ETRN 命令。
blocketrn	173	不执行 ETRN 命令。
checkehlo	172	检查 SMTP 响应标志区以决定是使用 EHLO 还是 HELO。
disableetrn	173	关闭对 ETRN SMTP 命令的支持功能。
domainetrn	173	仅执行有指定域的 ETRN 命令。
domainvrfy	174	用完整地址发布 VRFY 命令。
ehlo	172	在初始连接上使用 SMTP EHLO 命令。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
eightbit	174	通道支持八位字符。
eightnegotiate	174	通道应尽可能协调八位传输的使用。
eightstrict	174	拒绝包括未经协调的八位数据的邮件。
localvrfy	174	用本地地址发布 VRFY 命令。
mailfromdnsverify	174	检验用于 MAIL FROM: 命令的域在 DNS 中是否存在。
noehlo	172	不使用 EHLO 命令。
nomailfromdnsverify	174	对用于 MAIL FROM: 命令的域在 DNS 中是否存在不进行检验。
nosendetrn	173	不发送 ETRN 命令。
nosmtp	172	不支持 SMTP 协议。这是默认值。
novrfy	174	不发布 VRFY 命令。
sendetrn	173	发送 ETRN 命令。
sevenbit	174	不支持八位字符；八位字符必须编码。
silentetrn	173	执行 ETRN 命令，但不回送通道信息。
smtp	172	支持 SMTP 协议。关键字 smtp 对所有 SMTP 通道都是必须的。（此关键字等同于 smtp_crorlf。）
smtp_cr	172	接受以回车 （CR）结束，后面不跟换行符 （LF）的行。
smtp_crlf	172	接受的行必须以回车 （CR）换行 （LF）序列结束。
smtp_crorlf	172	所接受的行可以以回车 （CR）、换行 （LF）或一个完整的 CRLF 序列结束。
smtp_lf	172	接受以换行 （LF）结束，前面没有 CR 的行。
streaming	176	用于控制在与一通道相关的协议中使用的协议流等级。
vrfyallow	174	提供对 VRFY 命令的信息响应。
vrfydefault	174	依据通道的 HIDE_VERIFY 选项的设置，提供对 VRFY 命令的默认响应。
vrfyhide	174	提供对 SMTP VRFY 命令的模糊响应。
TCP/IP 连接与 DNS 查找支持功能 （细分的功能单位，请见第 176 页表 8-5）		
cacheeverything	178	高速缓存所有连接信息。
cachefailures	178	仅高速缓存连接失败信息。
cachesuccesses	178	仅高速缓存连接成功信息。
connectalias	194	传递给收件人地址中列出的任何主机。

表 8-2　按功能分类的通道关键字（默认字体为粗体）（接上页）

关键字	页	定义
connectcanonical	194	连接到系统的主机别名，即 MTA 将与之连接者。
daemon	182	无论信封地址是什么都连接到一个特定的主机系统。
defaultmx	180	通道决定是否从网络进行 MX 查找。
defaultnameservers	181	参考 TCP/IP 栈的名字服务器选择。
forwardcheckdelete	179	如果已执行反向的 DNS 查找，下一步将在返回的名字上执行正向查找以检查返回的 IP 号是否与原始的相匹配，如果不匹配，则删除这个名字并使用 IP 地址。
forwardchecknone	179	在 DNS 反向查找后不执行正向查找。
forwardchecktag	179	如果反向的 DNS 查找已被执行，下一步在返回的名字上执行正向查找以检查返回的 IP 号是否与原始的匹配，如果不匹配，将名字标记上 *。
identnone	179	不执行 IDENT 查找；执行 IP 到主机名的转换；在 Received: 邮件头中同时包含主机名和 IP 地址。
identnonelimited	179	不执行 IDENT 查找；执行 IP 到主机名的转换，但在通道切换过程中不使用主机名；在 Received: 邮件头中同时包含主机名和 IP 地址。
identnonenumeric	179	不执行 IDENT 查找或 IP 地址到主机名的转换。
identnonesymbolic	179	不执行 IDENT 查找，执行 IP 到主机名的转换，在 Received: 邮件头中仅包含主机名。
identtcp	179	执行在外来 SMTP 连接上的 IDENT 查找和 IP 地址到主机名的转换，在 Received: 邮件头中同时包含主机名和 IP 地址。
identtcplimited	179	执行在外来 SMTP 连接上的 IDENT 查找和 IP 地址到主机名的转换，但在通道切换过程中不使用主机名。在 Received: 邮件头中同时包含主机名和 IP 地址。
indenttcpnumeric	179	在外来 SMTP 连接上执行 IDENT 查找，但不执行 IP 地址到主机名的转换。
identtcpsymbolic	179	执行在外来 SMTP 连接上的 IDENT 查找和 IP 地址到主机名的转换，在 Received: 邮件头中仅包含主机名。
interfaceaddress	178	绑定到指定的 TCP/IP 接口地址。
lastresort	181	指定最后使用的主机
mailfromdnsverify	174	检验用于 MAIL FROM: 命令的域在 DNS 中是否存在。
mx	180	TCP/IP 网络和软件支持 MX 记录查找。
nameservers	181	指定需参考的名字服务器列表而不参考 TCP/IP 栈自身对名字服务器的选择； nameservers 要求一个用空格隔开的名字服务器的 IP 地址的列表。
nocache	178	不高速缓存任何连接信息。
nomailfromdnsverify	174	对用于 MAIL FROM: 命令的域在 DNS 中是否存在不进行检验。

表 8-2　按功能分类的通道关键字 （默认字体为粗体）（接上页）

关键字	页	定义
nomx	180	TCP/IP 网络不支持 MX 查找。
nonrandomemx	180	进行 MX 查找，不以相等的优先级随机排列返回项。
port	178	指定 SMTP 连接的默认端口号。标准端口是 25。
randommx	180	进行 MX 查找，以相等的优先级随机排列返回项。
single	182	指定应在通道上为每个目标地址创建邮件的一个独立副本。
single_sys	182	为每个使用的目标系统创建邮件的一个单独副本。
threaddepth	189	使用多线程 SMTP 客户触发新线程的邮件数量。
其它		
submit	209	用于把某通道标记为 “仅限提交”通道。
user	209	在传递通道上使用，以此指示在哪个用户名下运行。

配置通道的默认值

所有或几乎所有的通道的许多配置都重复使用各种通道关键字。维护这样的配置既繁杂也容易出错。为简化某些配置，可以指定那些关键字默认用于各种通道。

例如，下面这一配置文件中的文本行表明，其后的所有通道块将继承该行中指定的关键字：

```
defaults keyword1 keyword2 keyword3 ...
```

此 defaults 行可被理解为一个特殊的通道块，它可改变关键字默认值而无需实际地指定一个通道。此 defaults 行也不需要任何其他的通道块信息行 （如果指定了，将忽略不计）。

对可以指定 defaults 的行，一般没有数量上的限制，多个默认行的效果是累积性的，最近遇到 （从上至下读）的行优先。

可能需要在配置文件的某个点之后 (例如，一外部文件的通道块独立部分开始处）无条件地消除任何 defaults 行的影响。 **nodefaults** 行正是为此目的而提供的。例如，将下行插入到配置文件时，这不仅将废止由此前任何默认通道建立的所有设置，而且可使配置返回到如同没有指定任何默认值的应用状态：

```
nodefaults
```

与常规通道块相同的是，必须用空行将每个 defaults 或 nodefaults 通道块与其他的通道块分割开。defaults 和 nodefaults 通道块为配置文件中仅有的能出现在本地通道之前的通道块。但与任何其他通道块相同，它们必须出现在最后的重写规则之后。

配置 SMTP 通道

根据安装的类型，Messaging Server 在安装时可提供几种 SMTP 通道（见下表）。这些通道可在 TCP/IP 之上执行 SMTP。多线程的 TCP SMTP 通道包括一个在 Dispatcher 控制下运行的多线程 SMTP 服务器。外发的 SMTP 邮件由通道程序 `tcp_smtp_client` 处理，并在需要时在 Job Controller 的控制下运行。

表 8-3　SMTP 通道

通道	定义
`tcp_local`	从远程 SMTP 主机接收入站邮件。根据是否使用智能主机 / 防火墙配置，可以直接发送出站邮件到远程 SMTP 主机或发送出站邮件到智能主机 / 防火墙系统。
`tcp_intranet`	在 intranet 内部接收和发送邮件。
`tcp_auth`	用作 tcp_local 的切换通道，授权的用户可切换到 tcp_auth 通道，以此躲避 “转接 - 阻止” 之限制。
`tcp_submit`	可在保留提交端口 587 上接受提交的邮件，通常为来自用户代理程序的邮件 （见 RFC 2476）。
`tcp_tas`	IA 特殊通道，通常为提供 “一体化通信” 业务的网站使用。

您可按本节的说明，通过添加或移除通道关键字之方法修改这些通道的定义或创建新通道。此外，还可用一选项文件控制 TCP/IP 通道的各种特性。这种选项文件必须存储在 MTA 配置目录下 （*ServerRoot*`/msg-`*instance*`/imta/config`），并命名为 *x_option*，其中 *x* 是通道的名字。有关详细信息，请见 **iPlanet Messaging Server Reference Manual**。

本节分为以下分节：

- 配置 SMTP 通道选项
- SMTP 命令和协议支持
- TCP/IP 连接和 DNS 查找支持
- SMTP 认证、 SASL 和 TLS
- 使用邮件头中 SMTP AUTH 的认证地址
- 使用邮件头中 SMTP AUTH 的认证地址
- 指定 Microsoft Exchange 网关通道
- 传输层安全

配置 SMTP 通道选项

TCP/IP 通道选项文件用于控制 TCP/IP 通道的各种特性。通道选项文件必须存储在 MTA 配置目录下，并命名为 *x*_option，这里的 *x* 是通道的名字。例如，/*ServerInstance*/imta/config/tcp_local_option。

选项文件由一个或多个关键字及其相关值组成。例如，在选项文件中包含 DISABLE_EXPAND 关键字并且将它的值设置为 1，即可禁用服务器上的邮件发送列表之扩展功能。

其它选项文件关键字可用来：

- 设置每封邮件允许的收件人数量的限制 （ALLOW_RECIPIENTS_PER_TRANSACTION）
- 设置每个连接允许的邮件数量的限制 （ALLOW_TRANSACTIONS_PER_SESSION）
- 详细调整记录到 MTA 日志文件中的信息类型 （LOG_CONNECTION，LOG_TRANPORTINFO）
- 指定客户机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及其语法方面的信息，请参阅 **iPlanet Messaging Server Reference Manual**。

SMTP 命令和协议支持

可以指定 SMTP 通道是否支持某种 SMTP 命令，例如 EHLO、ETRN 和 VRFY。也可以指定该通道是否支持 DNS 域验证，哪些字符作为行结束符等等。本节描述以下内容：

- 通道的 AICI 协议选择和行结束符
- EHLO 命令支持
- ETRN 命令支持
- VRFY 命令支持
- DNS 域检验
- 字符集标注和八位数据
- 协议流

表 8-4 总结了在此部分中说明的关键字。

表 8-4　SMTP 命令和协议关键字

通道关键字	说明
协议选择和行结束符	指定通道是否支持 SMTP 协议并指定被采用为行结束符的字符序列。
smtp	支持 SMTP 协议。关键字 smtp 对所有 SMTP 通道都是必须的。（此关键字等同于 smtp_crorlf。）

表 8-4　SMTP 命令和协议关键字（接上页）

通道关键字	说明
nosmtp	不支持 SMTP 协议。这是默认值。
smtp_cr	接受以回车 （CR）结束，后面不跟换行符 （LF）的行。
smtp_crlf	接受的行必须以回车 （CR）换行 （LF）序列结束。
smtp_lf	接受以换行 （LF）结束，前面没有 CR 的行。
smtp_crorlf	所接受的行可以以回车 （CR）、换行 （LF）或一个完整的 CRLF 序列结束。
EHLO 关键字	**指定通道如何处理 EHLO 命令**
ehlo	在初始连接上使用 SMTP EHLO 命令。
checkehlo	检查 SMTP 响应标志区以决定是使用 EHLO 还是 HELO。
noehlo	不使用 EHLO 命令。
ETRN 关键字	**指定通道如何处理 ETRN 命令 （请求队列处理）**
allowetrn	执行 ETRN 命令。
blocketrn	不执行 ETRN 命令。
domainetrn	仅执行有指定域的 ETRN 命令。
silentetrn	执行 ETRN 命令，但不回送通道信息。
sendetrn	发送 ETRN 命令。
nosendetrn	不发送 ETRN 命令。
VRFY keywords	**指定通道如何处理 VRFY 命令**
domainvrfy	用完整地址发布 VRFY 命令。
localvrfy	用本地地址发布 VRFY 命令。
novrfy	不发布 VRFY 命令。
vrfyallow	提供对 VRFY 命令的信息响应。
vrfydefault	依据通道的 HIDE_VERIFY 选项设置，提供对 VRFY 命令的默认响应。
vrfyhide	提供对 SMTP VRFY 命令的模糊响应。
DNS 域检验	**指定通道是否执行 DNS 域验证**
mailfromdnsverify	检验用于 MAIL FROM: 命令的域在 DNS 中是否存在。
nomailfromdnsverify	对用于 MAIL FROM: 命令的域在 DNS 中是否存在不进行检验。
字符集和八位数据	**指定通道如何处理八位数据** **备注：虽然这些关键字常常用在 SMTP 通道上，但它们与任何类型的通道都有潜在的关系。**

表 8-4　SMTP 命令和协议关键字（接上页）

通道关键字	说明
charset7	与 7 位文本邮件相关的默认字符集
charset8	与 8 位文本邮件相关的默认字符集
charsetesc	与 7 位文本邮件相关的默认字符集，包括换码字符
eightbit	通道支持八位字符。
eightnegotiate	通道应尽可能协调八位传输的使用。
eightstrict	通道应拒绝那些包括未经协调的八位数据的邮件。
sevenbit	通道不支持八位字符；八位字符必须编码。
协议流	**指定通道使用的协议流等级**
streaming	用于控制在与一通道相关的协议中使用的协议流等级。

通道的 AICI 协议选择和行结束符

关键字：smtp, nosmtp, smtp_crlf, smtp_cr, smtp_crorlf, smtp_lf

关键字 smtp 和 nosmtp 指定通道是否支持 SMTP 协议。关键字 smtp 或其某一变体对所有 SMTP 通道都是必须的。

关键字 smtp_crlf、smtp_cr、smtp_crorlf 和 smtp_lf 可在 SMTP 通道上使用，用以指定 MTA 将之作为行结束符接受的字符序列。关键字 smtp_crlf 意味着行必须以回车（CR）换行 （LF）序列结束。关键字 smtp_lf 或 smtp 意味着所接受的是前面没有 CR 的 LF。最后， smtp_cr 意味着所接受的是后面没有 LF 的 CR。这些选项仅影响外来资料的处理。

由于 SMTP 标准要求以 CRLF 作为行结束符， MTA 总是产生这个标准 CRLF 序列。各种 smtp 关键字因而仅用于控制 MTA 以决定是否接受其它非标准行结束符。例如，如果希望 MTA 仅接受严格合法的 SMTP 邮件并拒绝任何具有非标准行结束符的邮件，则可指定 stmp_crlf。

EHLO 命令支持

关键字：ehlo, noehlo, checkehlo

SMTP 协议已被扩展 （RFC 1869）以允许附加命令的协调。这可通过使用新的 EHLO 命令完成，用以代替 RFC 821 中的 HELO 命令。扩展的 SMTP 服务器通过提供所支持的扩展列表来响应 EHLO。未扩展的服务器将返回一个不可知命令错误，而客户机则发送旧的 HELO 命令。

这种退却策略通常在扩展和未扩展的服务器上都能使用。然而问题会出现在根据 RFC 821 不实施 SMTP 的服务器上。特别的，一些不符合标准的服务器在收到一个不可知的命令时会切断当前连接。

SMTP 客户机实施这样一种策略，即当任何服务器在收到 EHLO 后切断连接时，尝试重新连接和使用 HELO。然而，如果远程服务器在收到 EHLO 时不仅切断了连接而且进入有问题的状态，这种策略将不会起作用。

通道关键字 ehlo、noehlo 和 checkehlo 正是为处理这种情况而提供的。关键字 ehlo 可指示 MTA 对所有初始连接请求使用 EHLO 命令。关键字 noehlo 可禁用所有 EHLO 命令。关键字 checkehlo 可用于检测远程 SMTP 服务器返回的响应标志区中的字符串 “ESMTP” 。如果发现该字符串，则使用 EHLO，如果未发现，则使用 HELO。默认操作设置是对所有初始连接请求使用 EHLO，除非标志区行包括字符串“fire away”，在这种情况下须使用 HELO，请注意没有关键字对应于这种默认行为，它位于来自关键字 ehlo 和 checkehlo 的行为之间。

ETRN 命令支持

关键字： allowetrn, blocketrn, disableetrn, domainetrn, silentetrn, sendetrn, nosendetrn, novrfy

定义于 RFC 1985 中的 ETRN 命令提供了对 SMTP 服务的扩展，因而一 SMTP 客户通过与服务器的相互作用使服务器有机会启动对其队列的处理，以使其中的邮件去往给定的主机。

使用 ETRN 时，SMTP 客户机可请求远程 SMTP 服务器启动对发送到此 SMTP 客户机的邮件队列的处理。这样， ETRN 提供了一种实现为来到自身系统的邮件而 “轮询” 远程 SMTP 系统的方法。这对于相互间只具瞬态连接的系统很有用，例如，作为只具拨号连接上网的其它网站的第二邮件交换 （MX）主机而建立的站点。通过启用此命令，您可允许远程服务器 （可能是拨号服务器）请求传递其邮件。

在 SMTP ETRN 命令行上，SMTP 客户机可指定邮件到达系统的名称（通常是 SMTP 客户系统自己的名称）。如果远程 SMTP 服务器支持 ETRN 命令，则可触发执行一分开的进程，以与具该名称的系统连接并为此系统发送任何等待传递的邮件。

响应 ETRN 命令

当发送邮件的 SMTP 客户机发布 ETRN 命令时，关键字 allowetrn、blocketrn、domainetrn 和 silentetrn 可控制 MTA 响应，以请求 MTA 尝试传递 MTA 队列中的邮件。

默认状态下， MTA 将尝试执行所有 ETRN 命令，即启用关键字 allowetrn。可以通过在通道定义中包含关键字 blocketrn 以指定 MTA 不执行 ETRN 命令。

您可指定 MTA 执行所有 ETRN 命令，但不回送域所匹配的通道名，并且 MTA 将尝试包含关键字 silentetrn 的运行。关键字 domainetrn 可指定 MTA 仅执行对域有指定的 ETRN 命令，同时也可使 MTA 不回送域所匹配的通道名以及 MTA 将尝试运行者。

disableetrn 可用来全面禁用对 ETRN 命令的支持；SMTP 服务器并不把 ETRN 作为支持的命令而加以通告。

发送 ETRN 命令

通道关键字 sendetrn 和 nosendetrn 可控制 MTA 是否在 SMTP 连接开始时发送 ETRN 命令。默认的关键字是 nosendetrn，意指 MTA 将不发送 ETRN 命令。关键字 sendetrn 可通告 MTA 发送一 ETRN 命令，如果远程 SMTP 服务器支持 ETRN 的话。关键字 sendetrn 后面应跟随正在请求其邮件接收传递尝试的系统名。

VRFY 命令支持

关键字：domainvrfy, localvrfy, vrfyallow, vrfydefault, vrfyhide

VRFY 命令可使 SMTP 客户机能够向 SMTP 服务器发送一请求，以检验特定用户名的邮件是否驻留在该服务器上。 VRFY 命令在 RFC 821 中定义。

服务器发送的响应可表明用户是否为本地用户，邮件是否将被转发等等。值为 250 的响应表明用户名是本地的，值为 251 的响应表明用户名不是本地的，但服务器能够转发此邮件。服务器的响应包含邮箱名。

发送 VRFY 命令

在正常情况下，不应该将 VRFY 命令作为 SMTP 对话的一部分而发布。SMTP RCPT TO 命令应与 VRFY 执行同样的功能并返回一个适当的错误。然而，存在这样的服务器，它们能够接受 RCPT TO 中的任何地址 （并随后将其退回），同样是这些服务器还执行作为 VRFY 命令的一部分的更广泛的检查。

默认状态下， MTA 不发送 VRFY 命令 （即启用 novrfy 关键字）。

如果必要，可通过在通道定义中包含关键字 domainvrfy 或 localvrfy 的方法配置 MTA，以使其发布 SMTP VRFY 命令。关键字 domainvrfy 可使 VRFY 命令在发布时以完整地址（user@host）作为其参数。关键字 localvrfy 可使 MTA 发布 VRFY 命令时仅包括地址的本地部分 （user）。

响应 VRFY 命令

关键字 vrfyallow、 vrfydefault 和 vrfyhide 可在发送邮件的 SMTP 客户程序发出 SMTP VRFY 命令时控制 SMTP 服务器的响应。

关键字 vrfyallow 可指示 MTA 发布一个详细的、包含丰富参考信息的响应。vrfydefault 可指示 MTA 提供一个详细的、包含丰富参考信息的响应，除非通道选项 HIDE_VERIFY=1 已被指定。关键字 vrfyhide 可指示 MTA 仅发布一个含糊的、不明确的响应。这些关键字允许针对每个通道的 VRFY 响应控制，这与 HIDE_VERIFY 选项相反，后者通常应用于所有外来的通过相同的 SMTP 服务器处理的 TCP/IP 通道。

DNS 域检验

关键字：mailfromdnsverify, nomailfromdnsverify

如果在外来 TCP/IP 通道上设置 mailfromdnsverify，则可使 MTA 验证在 DNS 中存在的条目，即与其相关的域用在 SMTP MAIL FROM 命令上，而且若无此条目就拒收邮件。默认关键字 nomailfromdnsverify 意味着不执行这种验证。请注意在返回地址域上执行 DNS 检查会导致拒收一些原本希望有效的邮件。（例如，来自合法的站点而仅仅没有登记域名的邮件，或在 DNS 中有错误信息时的邮件），这与宽容面对接收的邮件和通过对 Internet 主机的要求（见 RFC 1123）得到电子邮件的精神是相违背的。然而，一些站点会希望在具有假地址 （来自不存在的域）的大宗商业电子邮件 （UBE）被发送的情况下执行这种检查。

字符集标注和八位数据

关键字：charset7, charset8, charsetesc, sevenbit, eightbit, eightnegotiate, eightstrict

字符集标注

MIME 规范提供的机制可用来在纯文本邮件中标注字符集。具体而言，也就是可将 charset= 参数指定为 Content-type：标题行的一部分。MIME 规范中定义了各种字符集名称，其中包括 US-ASCII（默认值）、ISO-8859-1、ISO-8859-2 以及后来定义的许多字符集名称。

有些现有的系统和用户代理程序没有提供生成这些字符集标注的机制；其结果是，某些纯文本邮件将可能无法被适当标注。通道关键字 charset7、charset8 和 charsetesc 提供了一种针对每个通道的机制，对于缺少字符集标注的邮件头，可用来指定插入的字符集名。每个关键字需要一个可给出字符集名的参数。系统不检查这些名称的有效性。但要注意，只能针对 MTA 表目录中的字符集定义文件 charsets.txt 中指定的字符集进行字符集转换。应尽可能地使用这个文件中定义的名字。

charset7 字符集名仅在邮件包含七位字符时使用； charset8 字符集名则在邮件包含八位数据时使用； charsetesc 在邮件仅包含七位数据且恰巧也包含换码符时使用。如果没有指定适当的关键字，则不会有字符集名被插入到 Content-type：标题行。

许注意的一点是，charset8 关键字还可用来控制邮件头中八位字符的 MIME 编码（此中的八位数据是绝对的非法）。如果没有指定 charset8 值， MTA 通常只以 MIME 对在邮件头中遇到的任何 （非法）八位数据进行编码，并将之标注为 UNKNOWN charset。

这些字符集说明不会覆盖现存的标注，也就是说，如果一邮件已具有字符集标注或属于文本类型以外的类型，这些说明将不起作用。通常较为适宜的做法是以下列方式标注 MTA 本地通道：

```
l ... charset7 US-ASCII charset8 ISO-8859-1 ...
hostname
```

如果邮件中没有内容类型报头，则添加之。该关键字还可添加 MIME 版本：的报头，如果缺失的话。

关键字 charsetesc 对使用包含换码字符的日文或韩文字符集接收未标注邮件的通道非常有用。

八位数据

一些传输方式限制使用序数值大于 127 （十进制）的字符。特别需要注意的是，一些 SMTP 服务器会去除高位，从而使使用八位字符的邮件出现乱码。

Messaging Server 提供的工具可自动给这种邮件编码，这样麻烦的八位字符就不会直接出现在邮件中了。通过指定关键字 sevenbit，编码可应用于入队到指定通道的所有邮件。如果无此限制存在，通道应标记为 eightbit。

SMTP 协议是不允许有八位数据的，除非远程 SMTP 服务器明确其能支持允许有八位数据的 SMTP 扩展程序。有些传输方式 （如扩展 SMTP）可能确实支持某种形式的协商途径，从而确定是否能够传输八位字符。因此，建议用户使用关键字 eightnegotiate，以此指示通道在协商失败时给邮件编码。这对所有通道都是默认的，不支持协商的通道只会认为该传输方式能够处理八位数据。

关键字 eightstrict 可通告 Messaging Server 拒收任何包含未协调的八位数据的入站邮件。

协议流

关键字：`streaming`

有些邮件协议可以支持流操作。这意味着 MTA 能同时发出一个以上的操作并等待每个操作的回复的成批到达。关键字 `streaming` 可控制在与一通道相关的协议中使用的协议流等级。此关键字需要一个整数参数，该参数如何解释取决于所使用的协议。

在正常情况下，协议流支持的可用范围需通过 SMTP 流水线扩展程序进行协商。这样，该关键字就决不应在正常情况下使用。

有效的流值为 0 到 3。0 值说明没有流操作，1 表示对 RCPT TO 命令组进行流操作，2 表示对 MAIL FROM/RCPT TO 进行流操作，3 表示对 HELO/MAIL FROM/RCPT TO 或 RSET/MAIL FROM/RCPT TO 进行流操作。默认值为零。

TCP/IP 连接和 DNS 查找支持

您可指定有关服务器如何处理 TCP/IP 连接和地址查找的信息。本节说明以下内容：

- TCP/IP 端口号和接口地址
- 高速缓存通道连接信息
- 反向 DNS 查找
- IDENT 查找
- TCP/IP MX 记录支持
- 名字服务器查找
- 最后使用的主机
- 来件的备用通道 （转换通道）
- 目标主机选择

表 8-5 列出了在本节描述的关于 TCP/IP 连接和 DNS 查找的关键字。

表 8-5　　TCP/IP 连接和 DNS 查找关键字

通道关键字	说明
端口选择和接口地址	**指定 SMTP 连接的默认端口号和接口地址。**
`port`	指定 SMTP 连接的默认端口号。标准端口是 25。
`interfaceaddress`	连通到指定的 TCP/IP 接口地址。
高速缓存关键字	**指定如何高速缓存连接信息。**
`cacheeverything`	高速缓存所有连接信息。
`cachefailures`	仅高速缓存连接失败信息。

表 8-5　TCP/IP 连接和 DNS 查找关键字（接上页）

通道关键字	说明
cachesuccesses	仅高速缓存连接成功信息。
nocache	不高速缓存任何连接信息。
反向 DNS 查找	**指定如何在外来 SMTP 连接上处理反向 DNS 查找。**
forwardcheckdelete	如果已执行了反向的 DNS 查找，下一步将在返回的名字上执行正向查找以检查返回的 IP 值是否与原始的相匹配，如果不匹配，则删除这个名字并使用 IP 地址。
forwardchecknone	在 DNS 反向查找后不执行正向查找。
forwardchecktag	如果反向的 DNS 查找已被执行，下一步在返回的名字上执行正向查找以检查返回的 IP 值是否与原始的匹配，如果不匹配，将名字标记上 *。
IDENT 查找 /DNS 反向查找	**指定如何在外来 SMTP 连接上处理 IDENT 查找和 DNS 反向查找**
identnone	不执行 IDENT 查找，执行 IP 到主机名的转换，在 Received: 邮件头中同时包含主机名和 IP 地址。
identnonelimited	不执行 IDENT 查找，执行 IP 到主机名的转换，但在通道切换过程中不使用主机名，在 Received: 邮件头中同时包含主机名和 IP 地址。
identnonenumeric	不执行 IDENT 查找或 IP 地址到主机名的转换。
identnonesymbolic	不执行 IDENT 查找，执行 IP 到主机名的转换，在 Received: 邮件头中仅包含主机名。
identtcp	执行在外来 SMTP 连接上的 IDENT 查找和 IP 地址到主机名的转换，在 Received: 邮件头中同时包含主机名和 IP 地址。
identtcplimited	执行在外来 SMTP 连接上的 IDENT 查找和 IP 地址到主机名的转换，但在通道切换过程中不使用主机名。在 Received: 邮件头中同时包含主机名和 IP 地址。
indenttcpnumeric	在外来 SMTP 连接上执行 IDENT 查找，但不执行 IP 地址到主机名的转换。
identtcpsymbolic	执行在外来 SMTP 连接上的 IDENT 查找和 IP 地址到主机名的转换，在 Received: 邮件头中仅包含主机名。
MX 记录支持和 TCP/IP 名字服务器	**指定通道是否以及如何支持 MX 记录查找**
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	通道决定是否从网络进行 MX 查找。
randommx	进行 MX 查找，以相等的优先级随机排列返回项。
nonrandomemx	进行 MX 查找，不以相等的优先级随机排列返回项。

表 8-5　TCP/IP 连接和 DNS 查找关键字（接上页）

通道关键字	说明
nameservers	指定参考的名字服务器列表而非参考 TCP/IP 栈自身对名字服务器的选择， nameservers 要求一个用空格隔开的名字服务器的 IP 地址的列表。
defaultnameservers	参考 TCP/IP 栈的名字服务器选择。
lastresort	指定最后使用的主机
切换关键字	**选择入站邮件备用通道的控制功能**
allowswitchchannel	允许从 switchchannel 通道切换到此通道。
noswitchchannel	逗留在服务器通道，不切换到与源主机相关的通道，不允许被切换。
switchchannel	从服务器通道切换到与原主机相关的通道。
tlsswitchchannel	TLS 协调成功时切换到另一通道。
saslswitchchannel	当 SASL 认证成功时切换到另一通道。
目标主机选择和邮件副本的存储	**指定一目标主机系统以及邮件副本如何存储。**
daemon	无论信封地址是什么都连接到一个特定的主机系统。
single	指定应在通道上为每个目标地址创建邮件的一个独立副本。
single_sys	为每个使用的目标系统创建邮件的一个单独副本。

TCP/IP 端口号和接口地址

关键字：port, interfaceaddress

当发送邮件时 TCP/IP 通道上的 SMTP 通常连接到端口 25。关键字 port 可用于指示 TCP/IP 通道上的 SMTP 连接到一个非标准端口。请注意此关键字是对 Dispatcher 选项 PORT（它控制 MTA 以决定为接受 SMTP 连接须监听哪些端口）的补充。

关键字 interfaceaddress 控制一 TCP/IP 通道为出站连接作为源地址而连通的地址，也就是说，在多接口地址的系统中，此关键字决定了哪个地址将在 MTA 发送外发 SMTP 邮件时作为源 IP 地址使用。请注意此关键字是对 Dispatcher 选项 INTERFACE_ADDRESS（它控制 TCP/IP 通道以决定为接受外来连接和邮件须监听哪个接口地址）的补充。

高速缓存通道连接信息

关键字：cacheeverything, nocache, cachefailures, cachesuccesses

使用 SMTP 协议的通道维护着一个包含先前连接尝试的历史记录的缓存。此缓存用于避免多次重复连接不可存取的主机，从而避免浪费许多时间并耽搁其它邮件。缓存是针对每个进程的，它仅在出站 SMTP 传递通道的一次运行期间存在。

高速缓存通常即记录连接成功也记录连接失败。（成功的连接尝试被记录下来以弥补以后的失败 - 曾经连接成功但本次连接失败的主机在进行下次连接尝试前的延迟不会像没有尝试过连接或先前连接失败的主机那样长。）

然而，MTA 使用的缓存策略不是对所有情况都必定适当。因此提供了若干通道关键字用以调整 MTA 缓存。

关键字 cacheeverything 启用所有形式的缓存并且是默认的。关键字 nocache 禁用所有缓存。

关键字 cachefailures 启用连接失败 （而非连接成功）的缓存 - 这在一定程度上促使比 cacheeverything 更严格的重新连接。最后，cachesuccesses 仅缓存成功连接。最后这个关键字与 SMTP 通道的 nocache 关键字等效。

反向 DNS 查找

关键字：forwardchecknone, forwardchecktag, forwardcheckdelete

通道关键字 forwardchecknone、 forwardchecktag 和 forwardcheckdelete 能够改变反向 DNS 查找的效果。这些关键字能够控制 MTA 以决定是否对用 DNS 反向查找所找到的 IP 名进行正向查找，如果这种正向查找被请求，则指定如果 IP 名的正向查找与连接的原 IP 值不匹配时 MTA 如何做。

forwardchecknone 是默认关键字，意味着不进行任何正向查找。关键字 forwardchecktag 告诉 MTA 在每个反向查找后进行正向查找，而且如果用正向查找得到的数字与原始连接值不匹配，则将 IP 名标记上星号（*）。关键字 forwardcheckdelete 告诉 MTA 在每个反向查找后进行正向查找，如果名字的正向查找与原始连接的 IP 地址不匹配，则忽略（删除）反向查找返回的名字，在这种情况下， MTA 使用原 IP 地址取而代之。

备注	正向查找与原 IP 地址不匹配的情况在许多站点是正常的，在这些站点里，更为 “普遍”的 IP 名被用于多个不同的 IP 地址。

IDENT 查找

关键字： identnone, identnonelimited, identtnonnumeric, identnonesymbolic, identtcp, identtcpnumeric, identtcpsymbolic, identtcplimited

关键字 IDENT 可通过 IDENT 协议控制 MTA 对连接和查找的处理方式。有关 IDENT 协议的说明，请见 RFC 1413。

关键字 identtcp、identtcpsymbolic 和 identtcpnumeric 可指示 MTA 使用 IDENT 协议执行连接和查找。按下列方式将从 IDENT 协议获得的信息 （通常就是进行 SMTP 连接的用户的标识）插入到邮件的 Received: 邮件头：

- identtcp 插入与外来 IP 值对应的主机名，也就是从 DNS 反向查找中找到的内容以及 IP 值本身。

- identtcpsymbolic 插入与外来 IP 值相应的主机名，也就是从 DNS 反向查找中找到的内容，但 IP 值本身不包含在 Received: 邮件头中。
- identtcpnumeric 插入实际的外来 IP 值，不针对该 IP 值执行 DNS 反向查找。

备注 远程系统必须为使用 identtcp、 identtcpsymbolic 或 identtcpnumeric 所导致的 IDENT 查找运行一个 IDENT 服务器。

要知道， IDENT 查询尝试有可能招致性能受损。路由器会像 “黑洞”那样吞食掉大量针对不可识别的端口的连接尝试。如果这种情况发生在 IDENT 查询中，则在连接超时前 MTA 根本侦听不到反馈 （由 TCP/IP 栈控制的超时，通常为 1 至 2 分钟）。

另一影响性能的因素发生在 identtcp、 indenttcplimited 或 identtcpsymbolic 与 identtcpnumeric 进行比较的时候。使用 identtcp、 identtcplimited 或 identtcpsymbolic 调用 DNS 反向查找，会导致某些额外开销，以获得对用户更为友好的主机名。

关键字 identnone 禁用 IDENT 查找，但执行指定 IP 地址到主机名的转换，而且 IP 值和主机名都包含在邮件的 Received: 邮件头中。这是默认值。

关键字 identnonesymbolic 禁用 IDENT 查找，但执行 IP 到主机名的转换，仅主机名包含在邮件的 Received: 邮件头中。

关键字 identnonenumeric 禁用此 IDENT 查找，并禁止通常的从 IP 地址到主机名的 DNS 反向查找转换，并以 Received: 邮件头中较少的用户友好信息为代价而使性能得到改善。

在 IDENT 查找，反向 DNS 查找，和显示于 Received: 邮件头中的信息等方面，关键字 identtcplimited 和 identnonelimited 分别与 identtcp 和 identnone 具有同样的效果。它们的不同之处在于：使用 identtcplimited 或 identnonelimited， IP 常值地址总是作为任何由 switchchannel 引起的通道切换的基础，而不管 DNS 反向查找是否成功地确定了一个主机名。

TCP/IP MX 记录支持

关键字：mx, nomx, defaultmx, randommx, nonrandommx

一些 TCP/IP 网络支持 MX （邮件转发）记录的使用而另一些则不支持。如果 MTA 系统所连接的网络不提供对 MX 记录支持， TCP/IP 通道程序可配置成不使用 MX 记录。关键字 mx、 nomx、 defaultmx、 randommx、 nonrandommx 控制着对 MX 记录支持。

关键字 randommx 指定应进行 MX 查找并且相等优先级的 MX 记录值应按随机顺序处理。关键字 nonrandommx 指定应进行 MX 查找并且相等优先级的 MX 记录值应按接收顺序处理。

关键字 mx 目前等同于 nonrandommx，在以后的版本中可能改为与 randommx 等同。关键字 nomx 禁用 MX 查找。关键字 defaultmx 指定：如果网络支持 MX 记录则应使用 mx。在支持任何形式的 MX 查找的通道上，关键字 defaultmx 是默认的。

名字服务器查找

关键字：nameservers, defaultnameservers

当执行名字服务器查找时，可用通道关键字 nameservers 指定要参考的名字服务器列表，而非参考 TCP/IP 栈自身对名字服务器的选择。关键字 nameservers 需要一个用空格隔开的名字服务器的 IP 地址的列表，如下例所示：

```
nameservers 1.2.3.1 1.2.3.2
```

默认关键字 defaultnameservers 意味着使用 TCP/IP 栈自身对名字服务器的选择。

为防止在 UNIX 上进行名字服务器查找，可以修改文件 nsswitch.conf。在 NT 上可以修改 TCP/IP 配置。

最后使用的主机

关键字：lastresort

关键字 lastresort 用于指定在所有其它连接尝试都失败时须连接的主机。实际上起着一个最后使用的 MX 记录的作用。这仅在 SMTP 通道上有用处。

该关键字一个单一参数，用以指定 “最后使用的主机”的名称。例如：

```
tcp_local single_sys smtp mx lastresort mailhub.siroe.com
TCP-DAEMON
```

来件的备用通道 （转换通道）

关键字：switchchannel、 allowswitchchannel、 noswitchchannel。另请见 saslswitchchannel 182 和 tlsswitchchannel 183

以下关键字可用来控制来件的备用通道选择：switchchannel, allowswitchchannel, noswitchchannel

当 MTA 从远程系统接受一外来连接时，必须选择一个与其相联系的通道。通常此决定基于所使用的传输方式；例如，外来的 SMTP over TCP/IP 连接自动与通道 tcp_local 相联系。

然而，当具有不同特征的多个外发通道以相同的传输用于处理不同系统时，此约定被打破。在这种情况下，外来连接和外发连接不与相同的通道相联系，其结果是对应的通道特征不与远程系统相联系。

关键字 switchchannel 提供了解决这一难题的办法。如果 switchchannel 被指定在服务器所使用的初始通道上，连接的 （原）主机的 IP 地址将与通道表进行匹配，如果匹配成功源通道会因此而改变。如果没有找到匹配的 IP 地址或与初始的默认外来通道相匹配，MTA 可以尝试使用通过 DNS 反向查找得到的主机名来进行匹配。源通道可以改变为具有 switchchannel 或 allowswitchchannel （默认）标记的任何一个通道。关键字 noswitchchannel 指定没有通道会与此通道相互切换。

除了针对与一服务器相联系的通道外，针对其他任何对象指定 switchchannel 都不会起作用。目前，switchchannel 仅影响 SMTP 通道，但实际上没有其它通道使用 switchchannel 是合理的。

目标主机选择

关键字：daemon, single, single_sys

对 daemon 关键字的解释和使用取决于其所应用的通道类型。

关键字 daemon 用于 SMTP 通道以控制目标主机的选择。

通常，通道要与被处理邮件的信封地址上列出的任何主机连接。关键字 daemon 用于指示通道不考虑信封地址，取而代之的是连接到一特定的远程系统，一般为防火墙或邮件集线器系统。实际的远程系统名应直接出现在 daemon 关键字之后，如下例所示：

```
tcp_firewall smtp mx daemon firewall.acme.com
TCP-DAEMON
```

如果关键字 daemon 后面的参数不是一个全限定域名，此参数将被忽略并且通道将连接到通道的正式主机。当指定防火墙或网关系统名为正式主机名时，关键字 daemon 的参数通常被指定为路由器，如下例所示：

```
tcp_firewall smtp mx daemon router
firewall.acme.com
TCP-DAEMON
```

其它重要的关键字有 single 和 single_sys。关键字 single 指定应为每个目标地址在通道上创建一个单独的邮件副本。关键字 single_sys 为每个所使用的目标系统创建一个单一的邮件副本。请注意，对于邮件入队于其中的每个通道，至少为每个邮件创建一个副本，而不考虑所使用的关键字。

SMTP 认证、 SASL 和 TLS

关键字：maysaslserver, mustsaslserver, nosasl, nosaslserver, saslswitchchannel, nosaslswitchchannel)

您可控制 Messaging Server 是否支持使用 SASL （简单认证和安全层）来认证 SMTP 服务器。 SASL 在 RFC 2222 中定义。有关 SASL、 SMTP 认证和安全的详细信息，请参阅第 12 篇，“配置安全和访问控制”。

通道关键字 maysaslserver、mustsaslserver、nosasl、nosaslserver、itchchannel 和 saslswitchchannel 都可由 SMTP 通道 （例如 TCP/IP 通道）用来配置 SMTP 协议期间的 SASL （SMTP AUTH）之使用。

默认关键字是 notls，这意味着不允许有或尝试 SASL 认证。它包含 nosaslserver，这意味着不允许有 SASL 认证。如果指定了 maysaslserver，则会使 SMTP 服务器允许客户机尝试使用 SASL 认证。如果指定了 mustsaslserver，则会使 SMTP 服务器坚持要客户机使用 SASL 认证；在远程客户机没有成功地验证之前， SMTP 服务器不接受邮件。

在客户成功使用 SASL 的情况下，使用 saslswitchchannel 可使外来连接切换到指定的通道。这需要一个值，用以说明切换到哪个通道。

使用邮件头中 SMTP AUTH 的认证地址

关键字：authrewrite

authrewrite 通道关键字可用于在源通道上使 MTA 将认证的始发者信息（如果有的话）传送到邮件头中。使用的信息通常为 SMTP AUTH，但也可通过 FROM_ACCESS 映射替换之。根据表 8-6，关键字 authrewrite 需有一整数值。

表 8-6　authrewrite 整数值

数值	用法
1	如果已有 Resent-from: 或 Resent-sender:，则添加一个 Sender: 邮件头或 Resent-sender: 邮件头，以包含 AUTH 原发件人。
2	添加一个包含 AUTH 原发件人的 Sender: 邮件头。

指定 Microsoft Exchange 网关通道

关键字：msexchange, nomsexchange

通道关键字 msexchange 可用于在 TCP/IP 通道上通知 MTA 这是一个可与 Microsoft Exchange 网关和客户机通信的通道。当放置在启用了 SASL 的入站 TCP/IP 通道上时（通过 maysaslserver 或 mustsaslserver 关键字启用），它会使 MTA 的 SMTP 服务器通告 AUTH 使用“不正确的”格式（此乃基于原来的 ESMTP AUTH 规范，而不是较新的修正过的 AUTH 规范，前者实际上不能与正确的 ESMTP 用法兼容）。例如，有些 Microsoft Exchange 客户程序并不能识别正确的 AUTH 格式，而只能识别不正确的 AUTH 格式。

通道关键字 msexchange 还可通告（识别）无效的 TLS 命令。

nomsexchange 是默认值。

传输层安全

关键字：maytls, maytlsclient, maytlsserver, musttls, musttlsclient, musttlsserver, notls, notlsclient, notlsserver, tlsswitchchannel

通道关键字 maytls、maytlsclient、maytlsserver、musttls、musttlsclient、musttlsserver、notls、notlsclient、notlsserver 和 tlsswitchchannel 用于配置在 SMTP 协议有效期间如 TCP/IP 通道这样的基于 SMTP 的通道对 TLS 的使用。

默认关键字是 notls，意味着 TLS 不被允许或尝试。它包含关键字 notlsclient，其意味着 MTA SMTP 客户不会在外发连接上尝试 TLS 使用（在外发连接中不发布 STARTTLS 命令），还包含关键字 notlsserver，其意味着 MTA SMTP 服务器不会在外来连接上允许 TLS 使用（STARTTLS 扩展没有被 SMTP 服务器公布，其命令本身也未采用）。

指定 maytls 使 MTA 给外来连接提供 TLS 并在外发连接上尝试 TLS。它包含关键字 maytlsclient，其意味着如果发送邮件到一个支持 TLS 的 SMTP 服务器，MTA SMTP 客户在发送时将尝试 TLS 使用，还包含关键字 maytlsserver，其意味着 MTA SMTP 服务器将公布对 STARTTLS 扩展的支持并在接收邮件时允许使用 TLS。

指定 musttls 使 MTA 在外发和外来连接上坚持 TLS 使用；不会与协调 TLS 使用失败的远程系统交换电子邮件。它包含关键字 musttlsclient，其意味着 MTA SMTP 客户在发送外发邮件时坚持 TLS 使用并且不会发送到没有成功协调 TLS 使用的 SMTP 服务器（MTA 将发布 STARTTLS 命令且此命令必须成功）。它也包含关键字 musttlsserver，其意味着 MTA SMTP 服务器将公布对 STARTTLS 扩展的支持并当接收外来邮件时坚持使用 TLS，而且将不从没有成功协调 TLS 使用的客户处接收邮件。

关键字 tlsswitchchannel 用于在一客户成功协调 TSL 的情况下使外来连接切换到指定的通道。它需要一个值用以说明切换到哪个通道。

配置邮件处理和传递

可配置服务器以确定何时尝试基于特定标准的邮件传递。还可指定任务处理的参数，如服务任务的处理限制或何时生成新的 SMTP 通道线程。本节描述以下内容：

- 设置通道的方向性
- 执行延迟传递日期
- 指定无法传递邮件的重新传递频率
- 通道执行任务的处理池
- 服务任务限制
- 基于大小的邮件优先级
- SMTP 通道线程
- 多地址扩展
- 启用服务转换功能

有关邮件处理和传递方面的概念性信息，请参见第 88 页 “作业控制器”和第 108 页 “作业控制器文件”。

表 8-7 总结了在此部分中说明的关键字。

表 8-7　　邮件处理和传递所用的关键字

关键字	定义
Immediate Delivery	定义邮件立即传递规范。
immnonurgent	在提交紧急、普通和非紧急邮件后启动立即传递。
Deferred Delivery	定义延迟任务的传递规范。
backoff	指定尝试传递延迟邮件的频率。可用以下关键字替换：normalbackoff、nonurgentbackoff、urgentbackoff。
deferred	承认并执行 Deferred-delivery: 标题行。
nodeferred	默认值。指定 Deferred-delivery: 标题行不予以执行。

表 8-7　邮件处理和传递所用的关键字（接上页）

关键字	定义
nonurgentbackoff	尝试传递非紧急邮件的频率。
normalbackoff	尝试重新传递正常邮件的频率。
urgentbackoff	尝试重新传递紧急邮件的频率。
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	将大小大于此值的邮件的优先级强制定义为低于非紧急优先级（第二等优先级），这意味着此邮件将一直等待下一个任务周期，以得到更进一步的处理。
normalblocklimit	将大小大于此值的邮件强制定义为非紧急优先级。
urgentblocklimit	将大小大于此值的邮件强制定义为普通优先级。
通道执行任务的处理存储池	**指定存储池，用于处理不同紧急程度的邮件以及延迟任务。**
pool	指定通道运行于其中的存储池。
after	指定通道运行之前的延迟时间。
服务任务限制	**指定服务任务数量和每个任务处理的最大邮件文件数量。**
maxjobs	指定通道中能够同时运行的最大任务数量。
filesperjob	指定单个任务所能处理的队列条目的数量。
SMTP 通道线程	
threaddepth	使用多线程 SMTP 客户触发新线程的邮件数量。
多地址扩展	**定义多收件人邮件的处理**
expandlimit	当地址数量超过此限制时，对入站邮件进行 “脱机” 处理。
expandchannel	指定用于执行由于使用 expandlimit 而导致的延迟扩展的通道。
holdlimit	当地址数量超过此限制时，保存来件暂不处理。
无法传递邮件通知	**指定何时发送无法传递邮件通知。**
notices	指定在发送通知和退回邮件之前可以耗费的时间量。
nonurgentnotices	对于具有非紧急优先级的邮件，指定在发送通知和退回邮件之前可以耗费的时间量。
normalnotices	对于具有普通优先级的邮件，指定在发送通知和退回邮件之前可以耗费的时间量。
urgentnotices	对于具有紧急优先级的邮件，指定在发送通知和退回邮件之前可以耗费的时间量。

设置通道的方向性

关键字：master, slave, bidirectional

可用三个关键字指定某通道是用主程序提供服务（master）还是用从属程序（slave）提供服务，或由两个程序（bidirectional）同时提供服务。如果没有指定任何关键字，则为 bidirectional。这些关键字可在邮件于通道中排队期间决定 MTA 是否启动传递操作。

这些关键字的使用反映了相关通道程序的某些基本特点。针对 MTA 支持的各种通道的说明，可表明这些关键字应在何时何处使用。

执行延迟传递日期

关键字：deferred, nodeferred

通道关键字 deferred 可识别并执行 Deferred-delivery: 标题行。标有 deferred 传递日期（将来日期）的邮件将保留在通道队列中，直到其过期退回或到了延迟传递日期时为止。有关 Deferred-delivery: 标题行的格式和使用方面的详细信息，请参见 RFC 1327。

关键字 nodeferred 为默认值。需说明的一点是，虽然 RFC 1327 有规定一定要支持延迟邮件处理功能，但执行时实际上是让用户把邮件系统作为其磁盘配额的扩展而使用。

指定无法传递邮件的重新传递频率

关键字：backoff, nonurgentbackoff, normalbackoff, urgentbackoff, notices

系统设置是：对于有传递失败情况的邮件，重新传递的频率取决于邮件的优先级别。以下是尝试传递之间的默认时间间隔（分）。优先级别后面的第一个数表示初次传递失败后第一次尝试重新传递的分钟数：

urgent: 30, 60, 60, 120, 120, 120, 240
normal: 60, 120, 120, 240, 240, 240, 480
nonurgent: 120, 240, 240, 480, 480, 480, 960

如果是紧急邮件，则在初次传递失败 30 分钟后尝试重新传递，第一次重新传递 60 分钟后尝试重新传递，第二次重新传递 60 分钟后尝试重新传递，第三次重新传递 120 分钟后尝试重新传递，等等。指定的最后尝试后的重新传递，以相同的时间间隔重复。因此，如果是紧急邮件，则每隔 240 分钟重新传递一次。

传递尝试之持续时间由下列关键字指定：notices、nonurgentnotices、normalnotices 或 urgentnotices。如果无法传递，系统将生成一则*无法传递之通知*，并将邮件退回给发件人。（有关 notices 关键字的详细说明，请见第 123 页 “设置通知邮件传递间隔”。）

您可通过 “backoff”关键字为不同优先等级的邮件指定自定义的重新传递时间间隔。nonurgentbackoff 用于指定非紧急邮件的重新传递时间间隔。normalbackoff 用于指定正常邮件的重新传递时间间隔。urgentbackoff 用于指定紧急邮件的重新传递时间间隔。如果没有指定这些关键字， backoff 指定的时间间隔则适用于所有邮件，不论优先等级为何。

以下为示例：

```
urgentbackoff "pt30m" "pt1h" "pt2h" "pt3h" "pt4h" "pt5h" "pt8h"
"pt16h"
```

此例中，紧急邮件是在初次传递失败后 30 分钟时尝试重新传递的，随后的重新传递尝试如下：第一次后的一个小时 （即初次传递失败后的 1 小时 30 分）、第二次后的两个小时、第三次后的三个小时、第四次后的四个小时、第五次后的五个小时、第六次后的八个小时、第七次后的十六个小时。再往后的重新传递尝试将为每 16 小时一次，直至关键字 `notices` 指定的时限到期为止。如果无法传递，系统将生成一则“无法传递”之通知，并将邮件退回给发件人。有关时间间隔的语法，请见 ISO 8601P，使用方法说明，请见 **iPlanet Messaging Server Reference Manual**。

在下一个示例中：

```
normalbackoff "pt30m" "pt1h" "pt8h" "p1d" "p2d" "p1w"
```

一正常邮件是在初次传递失败后 30 分钟时尝试重新传递的，随后的重新传递尝试如下：第一次后的一个小时、第二次后的八个小时、第三次后的一天、第四次后的两天、第五次后的一星期，然后每星期尝试一次，直至关键字 `notices` 指定的时限到期为止。如果无法传递，系统将生成一则 “无法传递”之通知，并将邮件退回给发件人。

在最后的示例中：

```
backoff "pt30m" "pt120m" "pt16h" "pt36h" "p3d"
```

对于所有无法传递的邮件，不论优先级如何，都将在初次传递失败后 30 分钟时尝试重新传递，并在第一次后的两个小时重试，第二次后的十六个小时重试，第三次后的三十六小时重试，第四次后的三天重试，然后每三天重试一次，直至关键字 `notices` 指定的时限到期为止；除非您用 `nonurgentbackoff`、`normalbackoff` 或 `urgentbackoff` 关键字替换之。如果无法传递，系统将生成一则 “无法传递”之通知，并将邮件退回给发件人。

通道执行任务的处理池

关键字：`pool`

您可通过配置使不同的通道在同一存储池中运行，以便共享资源。还可能需要配置其他通道使之运行于专用于某特定通道的存储池中。在每一个存储池中，根据邮件的优先级自动将其存储到不同的处理队列中。存储池中高优先级的邮件在低优先级邮件之前得到处理。（请参见第 189 页 “基于大小的邮件优先级”。）

通过使用关键字 `pool`，您可在创建任务项的处理池中，以通道对通道为基础选择处理池。关键字 `pool` 之后必须有当前通道传递任务应使用的存储池的名称。存储池名称不得超过 12 个字符。

有关 Job Controller 的工作原理和配置信息，请参见第 108 页 “作业控制器文件”、第 88 页 “作业控制器”和第 188 页 “服务任务限制”。）

服务任务限制

关键字：maxjobs,filesperjob

每当邮件排入通道的队列时，作业控制器可确保有一项传递邮件的作业在运行。这可能涉及到启动新的作业进程、添加线程，或者仅标示出已有一项作业在运行。但是，一个单独服务任务不能够充分保证即时传递所有邮件。有关 Job Controller 的工作原理和配置信息，请参见第 108 页“作业控制器文件”、第 187 页“通道执行任务的处理池”和第 88 页“作业控制器”。）

对于某给定安装而言，为传递邮件而启动的最大进程数和线程数量应有一个合适的值。最大数量取决于诸如处理器个数、磁盘速度和连接的特性等因素。在 MTA 配置中，可以进行如下的控制：

- 为一给定通道的运行可启动进程的最大数量 （通道关键字 maxjobs）
- 为一组通道可启动进程的最大数量 （任务控制器配置文件的存储池相关部分的 JOB_LIMIT 参数）
- 在一新线程或进程启动之前接收的入队邮件个数 （通道关键字 threaddepth）
- 对于某些通道，在给定的传递程序之中可运行线程的最大数量 （通道选项文件中的 max_client_threads 参数）。

为一给定通道的运行可启动进程的最大数量应是下面两个值中的较小者：为通道设置的 maxjobs 和为通道运行所用存储池设置的 JOB_LIMIT。

假设某邮件需要处理。通常，任务控制器按如下所述那样启动新进程：

- 如果没有为一通道运行的进程并且还没有达到存储池的任务限制，任务控制器启动一新进程。
- 如果通道程序是单线程的或已达到线程限制，待处理邮件的增长超过线程数的倍数 （由 threaddepth 指定）时且通道和存储池任务限制都未达到，那么任务控制器启动一新进程。
- 如果通道程序是多线程的并且还没有达到线程限制，且待处理邮件的增长超过 threaddepth 的倍数时，启动一新线程。

特别是对于 SMTP 通道，当邮件排入不同主机的队列中时即启动新线程或新进程。因此，对于 SMTP 通道，任务控制器是按如下所述方式启动新进程的。假定有一邮件需要处理：

- 如果没有为 SMTP 通道运行的进程并且没有达到存储池限制时，任务控制器启动新进程。
- 如果已经达到线程限制（MAX_CLIENT_THREADS），排入主机队列的一邮件没有得到服务，并且通道限制（maxjobs）和存储池任务限制（JOB_LIMIT）都没有达到时，则启动一新进程。
- 如果还没有达到线程限制，排入主机队列的一邮件还没有得到服务时，启动一新线程。
- 如果还没有达到线程限制，并且由于邮件排入队列使主机待处理邮件增长超过 threaddepth 的倍数时，启动一新进程。

还可参阅第 189 页 “SMTP 通道线程”。

关键字 filesperjob 可用于使 MTA 创建额外的服务任务。此关键字以一单个正整数为参数，用于指定在创建多于一个的服务任务来处理队列条目之前，必须有多少个队列条目（也就是文件）被发送到相关的通道之中。如果给出的参数值小于或等于零，则被解释为只请求一个队列服务任务。没有指定关键字等同于将关键字的值指定为零。应充分重视此关键字的效果；计算出的数值越大，可实际创建的服务任务的个数就越多。

关键字 filesperjob 用给定值去除实际队列条目（即文件）的个数。注意，源于一给定邮件的队列条目的个数受很多因素的影响，包括（但不限于）关键字 single 和 single_sys 的使用以及邮件列表中邮件头修改操作的规定等。

关键字 maxjobs 设置能够同时运行的服务任务个数总和的上限。该关键字后必须跟有一个整数值，如果计算出的服务任务个数大于此值，则实际仅创建 maxjobs 个任务。如果没有指定 maxjobs，此值的默认值为为 100。通常 maxjobs 设置为小于或等于能同时运行在通道所使用的任何服务存储池或存储池组中的任务合计数。

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 基于大小降低邮件的优先级。这些关键字影响处理邮件时任务控制器所应用的优先级。

SMTP 通道线程

关键字： threaddepth,

多线程 SMTP 客户程序把发送到不同目的地的邮件分发到不同线程中。关键字 threaddepth 可用于指示多线程 SMTP 客户程序在任意一线程中只处理规定数目的邮件，甚至对于所有发向同一目的地的邮件（正常情况下在一个线程中处理）也使用额外的线程。

若与通道相连接的 SMTP 服务器能处理多个并发连接，使用 threaddepth 可能对在一守护程序路由器 TCP/IP 通道 - 一种与单个指定 SMTP 服务器连接的 TCP/IP 通道 - 上实现多线程特别有用。

每当通道待处理邮件的增长超过 threaddepth 的倍数时，任务控制器试图增加专用于处理该通道队列中的邮件的进程总数。对于多线程通道，任务控制器建议任何处理该通道邮件的进程启动新线程，或当所有任务都有该通道所允许的最大线程数（tcp_* 通道选项中的 MAX_CLIENT_THREADS）时启动新进程。对于单线程通道将启动新进程。注意，当达到通道限任务制（maxjobs）或存储池任务限制（JOB_LIMIT）时，任务控制器将不再启动新任务。

多地址扩展

关键字：expandlimit, expandchannel, holdlimit

大多数通道在传输每一个入站邮件时都支持指定多个收件人地址。在单个邮件中指定多个收件人地址有可能导致邮件传输处理的延迟（联机延迟）。如果延迟时间太长，可能会发生网络超时，这又可能导致反复尝试邮件提交和其他的问题。

MTA 提供了一个特别的功能，当为单个邮件指定了超过给定数目的地址时，将该邮件强制为延迟（离线）处理。延迟处理能够降低大量的联机延迟。注意，额外的开销也只是被延迟了，而没有完全避免。

该功能需要在一定的组合下才能激活，例如，一般为 reprocessing 通道和 expandlimit 关键字。关键字 expandlimit 取一个整数参数，以指定在延迟处理之前可接受多少来自通道的邮件中的地址。如果没有指定 expandlimit 关键字，默认值为无限大。一 0 值强制延迟处理所有来自通道的地址。

务必不要为本地通道或 reprocessing 通道自身指定关键字 expandlimit，这样指定的后果是无法预测的。

实际用来执行延迟处理的通道可以使用关键字 expandchannel 指定，默认状态下使用 reprocessing 通道，如果没有指定 expandchannel，那么使用另外某些重处理通道或处理通道可能对特定目的来讲是有用的。如果通过 expandchannel 指定了处理延迟的通道，该通道应该是重处理通道或处理通道，指定其他类型的通道可能导致无法预测的结果。

reprocessing 通道或任何用于执行延迟处理的通道，必须添加到 MTA 配置文件中以便 expandlimit 关键字能发挥作用。如果配置是由 MTA 配置实用程序构建，那么一个重处理通道应该已经存在。

格外大的收件人地址列表经常是充斥大宗商业电子邮件的征兆。关键字 holdlimit 通知 MTA 当来自通道的邮件导致超过指定数量的收件人时，将其标记为 .HELD 邮件并且排入到 reprocess 通道 （或任何通过 expandchannel 关键字指定的通道）中。这些文件将滞留在 reprocess 队列中不予处理，等待 MTA Postmaster 的人工干预。

启用服务转换功能

关键字：service, noservice

不论 CHARSET-CONVERSION 条目为何，关键字 service 都无条件地启用服务转换功能。如果设定了 noservice 关键字，则进入此通道的邮件服务转换就必须通过 CHARSET-CONVERSION 启用。

配置地址处理功能

本节说明处理地址所需使用的关键字。这一部分由下列分节组成：

- 启用服务转换功能
- 地址类型和约定
- 解释使用 ! 和 % 的地址
- 在地址中添加路由信息
- 禁用显式路由地址重写
- 邮件出队时的地址重写

- 指定更正不完全地址时应使用的主机名
- 使收件人标题行的邮件合法化
- 去除非法的空白收件人报头
- 启用针对具体通道的反向数据库的使用
- 启用受限邮箱编码
- 生成 Return-path: 标题行
- 从信封的 To: 和 From: 地址构建 Received: 标题行
- 处理地址 标题行中的注释
- 处理地址标题行中的人名
- 指定别名文件和别名数据库探查项
- 子地址的处理
- 启用具体通道的重写规则检查
- 移除源路由
- 指定必须来自别名的地址

地址类型和约定

关键字：`822`, `733`, `uucp`, `header_822`, `header_733`, `header_uucp`

这组关键字用于对通道支持的地址类型进行控制。类型有传输层使用的地址 （邮件信封）和邮件头使用的地址之别。

822 （sourceroute）

源路由信封地址。该通道全面支持 RFC 822 格式的信封寻址约定，其中包括源路由。关键字 `sourceroute` 也可作为 822 的同义词使用。如果没有指定其它信封地址类型关键字，则为默认关键字。

733 （percents）

百分号信封地址。除了源路由外，该通道全面支持 RFC 822 格式的信封寻址；源路由则应用百分号约定重写。关键字 `percents` 也可作为 733 的同义词使用。

备注	在 SMTP 通道上使用 733 地址约定可致使这些常规被携带到 SMTP 信封中的传输层地址中。这种情况是违反 RFC 821 规定的。所以只有在确信必要时，才使用 733 地址约定。

uucp （bangstyle）

Bang-style （惊叹号式）信封地址。这种通道在信封中采用与 RFC 976 bang-style 地址约定相符的地址（例如，此乃 UUCP 通道）。关键字 `bangstyle` 也可作为 uucp 的同义词使用。

header_822

源路由邮件头地址。该通道全面支持 RFC 822 格式的邮件头寻址约定，其中包括源路由。如果没有指定其它邮件头地址类型关键字，则为默认关键字。

header_733

百分号邮件头地址。除了源路由外，该通道全面支持 RFC 822 格式的邮件头寻址；源路由则应用百分号约定重写。

备注	在邮件头中使用 733 地址约定可能会违反 RFC 822 和 RFC 976 之规定。所以，请只在确信该通道所连接的系统不能处理源路由地址时，才使用该关键字。

header_uucp

UUCP 或 bang-style 邮件头地址。建议不要使用该关键字。因为这种用法违反 RFC 976 规约。

解释使用！和 % 的地址

关键字：`bangoverpercent`,`nobangoverpercent`,`percentonly`

地址须永远依照 RFC 822 和 RFC 976 进行解释。然而，对于没有包括在这些标准内的某些复合地址，在处理上还是有些含糊。特别是具有 `A!B%C` 格式的地址，既可解释为：

- `A` 为路由主机； `C` 为最终目的地主机

  或

- `C` 为路由主机； `A` 为最终目的地主机

虽然 RFC 976 暗示邮件程序可以使用后者之约定解释地址，但并未说明是否要求如此。有些情况下，前面的第一种解释可能更适用。

关键字 `bangoverpercent` 可强制使用第一种 `A!(B%C)` 解释。关键字 `nobangoverpercent` 则强制使用后面的 `(A!B)%C` 解释。 `nobangoverpercent` 是默认设置。

备注	该关键字对 `A!B@C` 格式的地址处理没有影响。因为这些地址永远被当作 `(A!B)@C` 进行处理。这种处理是 RFC 822 和 RFC 976 的共同要求。

关键字 `percentonly` 可忽略 bang 路由。当设定了这个关键字时，百分号则被解释为路由。

在地址中添加路由信息

关键字：exproute, noexproute, improute, noimproute

MTA 处理地址时采用的寻址模型假定：所有系统都知道所有其它系统的地址，并知道如何获取这些地址。不幸的是，这种理想的处理方法并非适用于所有情况，如：当某一通道所连接到的一个或多个系统不为世界其它地区所知时，则无法处理 （例如，专用 TCP/IP 网上的内部机器）。该通道上的系统地址对于网站外的远程系统而言可能是非法的。如果您想回复这些地址，其中必须含源路由信息，以此通告远程系统使用本地机器路由邮件。如此，本地的机器才能 （自动）将邮件传递到这些机器。

关键字 exproute （“explicit routing”之缩写）用于通告 MTA 相关的通道 （在其地址被传送到远程系统时）需要显式路由。如果某通道上指定了该关键字，MTA 就会在所有与该通道匹配的邮件头地址和所有信封 From：地址中添加含本地系统名称 （或本地系统目前使用之别名）的信息。默认关键字 noexproute，则可指定不在其中添加路由信息。

选项 EXPROUTE_FORWARD 可用来将 exproute 之操作限制为 “反向指向地址” （backward-pointing addresse）。当 MTA 通过某通道与之连接的系统不能自身执行正确的路由时，则会出现另一种情形。在这种情况中，与其它通道相关的所有地址都需有明确的路由，特别是当邮件中使用了这些地址，而发送通道与不能执行路由的系统相连接的时候，尤其如此。

隐式路由和关键字 improute 可用来为这种情况解围。 MTA 知道所有与其它通道匹配的地址，在其被用于发送至标有 improute 的通道时需要进行路由选择。默认关键字 noimproute 用于指定不在通过特定通道外发的邮件地址中添加路由信息。选项 IMPROUTE_FORWARD 可用来将 improute 之操作限制为 “反向指向地址”。

关键字 exproute 和 improute 应尽量少使用。因为着两个关键字会使地址变长，使之更复杂，而且可能会逾越其它系统使用的智能路由方案。显式和隐式路由不应与指定的路由相混淆。指定路由用于将重写规则中的路由信息插入到地址。这乃是通过特殊的 A@B@C 重写规则模板启用的。

当指定路由被启用时，它将应用于所有地址，邮件头和信封无一例外。指定路由是由特定重写规则启用的，因此通常独立于目前在用的通道。而显式和隐式路由则是在每条通道的基础上加以控制，所插入的路由地址也总是本地系统的地址。

禁用显式路由地址重写

关键字： routelocal

通道关键字 routelocal 可使 MTA 在通道上重写地址时以 “短路”方式中断地址中的任何显式路由。显式路由 （使用 !、 %，或 @ 字符）现已得以简化。

若在“内部”通道（如内部 TCP/IP 通道）上使用该关键字，则可用较简单的方式配置 SMTP 转节阻塞功能。

请注意，此关键字不要应在要求有显式 % 或其它路由的通道上使用。

邮件出队时的地址重写

关键字：connectalias, connectcanonical

MTA 通常在将邮件排列到其通道队列时对地址进行重写。而邮件出队时则没有任何重写操作。这就可能会在主机名称更换时，而通道队列还有仍送往旧名称的邮件时，带来潜在的问题。

关键字 connectalias 可指示 MTA 将邮件发送至收件人地址中列出的任何主机。这是默认关键字。关键字 connectcanonical 可指示 MTA 连接到应该与之连接的那个系统的主机别名。

指定更正不完全地址时应使用的主机名

关键字：remotehost, noremotehost, defaulthost, nodefaulthost

MTA 常常会收到一些因邮件程序和 SMTP 客户程序配置不当或不符合标准而在其中没有域名的地址。在出现这种情况时，MTA 会在允许其通过之前，尝试使这种地址合法。其具体做法是：MTA 将在地址中附加一个域名 （例如，将 @siroe.com 附加到 mrochek）。

对于缺失域名的信封 To: 地址，永远假定应附加本地主机名称。然而对于其它地址（如 From: 地址），在使用 MTA SMTP 服务器的情况下，则至少有两个可选择的域名，即本地 MTA 主机名和客户 SMTP 报告的远程主机名。或在某些情况下，可能还有第三个可用的选择，即在通过该通道入站的邮件上添加一个特定的域名。由于前两个选择的操作都会在一定频率上出现，所以看上去似乎都是正确的。在处理配置不当的 SMTP 客户程序时，最好使用远程主机的域名。而在处理轻型远程邮件客户程序 （如使用 SMTP 传递邮件的 POP 或 IMAP 客户程序），则最好使用本地主机的域名。或如果是 POP 或 IMAP 等轻型远程邮件客户程序，则客户程序应该有其各自的特定域名，即非本地主机域名者。在此种情况下，最好添加特定的其它域名。 MTA 能做到的是允许按通道进行选择。

通道关键字 noremotehost 可指定系统使用本地知己名。关键字 noremotehost 为默认值。

通道关键字 defaulthost 用于指定需添加在入站基本用户 id 中的特定主机名。其后必须跟有主机名，用以完成进入该通道的地址 （在信封 From: 和邮件头中）。（如果是提交通道，defaulthost 关键字的第一个参数也会影响基本信封 To: 地址。）供选用的第二个域名（至少有一个英文句号者）可被指定用来完成信封 To: 的地址。而 nodefaulthost 是默认值。

正如前面“来件的备用通道（转换通道）”所描述的那样，关键字 switchchannel 可用来将入站 SMTP 连接与某一特定通道相关联。这一工具可用来在某一通道上把远程邮件客户程序分成组，以便给予适当的处理。另一种方法是：统一部署符合标准的远程邮件客户程序 （即使在使用多种不兼容的客户程序情况下），而不是试图在您的 MTA 主机上更正网络上的问题；相比之下，前者更为简单。

使收件人标题行的邮件合法化

关键字：missingrecipientpolicy

RFC 822 要求（因特网）邮件必须含收件人标题行，即 To:、Cc: 或 Bcc: 标题行。没有此类标题行的邮件是非法的。但是，有些老掉牙的用户代理程序和邮件程序（例如许多旧版本的 sendmail 程序）仍会吐出一些非法邮件。

关键字 missingrecipientpolicy 可用一整数值指定使用这种邮件的方法；如果没有明确的关键字在用，默认值则为 0，其意思是将信封 To: 的地址放入 To: 邮件头中。

表 8-8　missingrecipientpolicy 的值

值	操作
0	将信封上的 To: 收件人放入 To: 标题行。
1	在不做任何改变的情况下传送非法邮件。
2	将信封上的 To: 收件人放入 To: 标题行。
3	将所有信封 To: 收件人放入一个 Bcc: 标题行中。
4	生成一个组结构（例如：;） To: 标题行，未指定 To: 收件人者。
5	生成一空白的 Bcc: 标题行。
6	拒收邮件。

请注意，选项 MISSING_RECIPIENT_POLICY 可用于设置这种行为的 MTA 系统默认值。初始的 Messaging Server 配置应将 MISSING_RECIPIENT_POLICY 设置为 1。

去除非法的空白收件人报头

关键字：dropblank, nodropblank

在 RFC 822（因特网）邮件中，任何 To:、Resent-To:、Cc: 或 Resent-Cc: 报头或邮件头都需含至少一个地址，这种报头不能为空值。尽管如此，有的邮件程序还是会发放出此类非法报头或邮件头。通道关键字 dropblank 如果被指定于某源通道，则可使 MTA 从入站邮件中去除任何此种非法的空白报头。

启用针对具体通道的反向数据库的使用

关键字：reverse, noreverse

关键字 reverse 可指示 MTA 按照地址反向数据库或 REVERSE 映射（如果二者之一有一个存在的话）检查并可能修改排列在通道中的邮件的地址。关键字 noreverse 则可免除对排列在通道中的邮件的地址进行地址反向处理。关键字 reverse 为默认值。有关详细说明，请参见第 115 页 “将内部格式地址转换为公共格式地址”。

启用受限邮箱编码

关键字：restricted, unrestricted

有些邮件系统难于处理 RFC 822 允许的全长地址时。比较常见的例子是基于 sendmail 的邮件程序，特别是当其配置文件设置有误的情况下，尤其如此。引用的本地部分（或邮箱规范）是常见的麻烦来源：

```
"smith, ned"@siroe.com
```

这一问题变得如此严重，以至 RFC 1137 不得不制订相应的方法以迂回方式解决这一问题。基本方法是从地址中移除引用，然后通过翻译将需引用的字符映射成为 atom（组合单位）允许的字符（有关此处使用的 atom 一词的定义，请见 RFC 822）。例如，全面的地址可能变成：

```
smith#m#_ned@siroe.com
```

通道关键字 restricted 可告知 MTA 与该通道连接的邮件系统需要这种编码。当邮件写入通道时，MTA 便可在报头和信封地址两处，对引用的本地部分进行编码处理。通道上的入站地址可自动解码。关键字 unrestricted 可指示 MTA 不进行 RFC 1137 编码和解码。关键字 unrestricted 是默认设置。

备注 对于不能接受引用的本地部分的系统，当有通道与之连接时，则应使用关键字 restricted。但不应该应用于可实际生成援引本地地址部分的通道。（这种情况假定凡能生成这种地址的通道，也能处理这种这种地址。）

生成 Return-path: 标题行

关键字：addreturnpath, noaddreturnpath

在通常情况下，添加 Return-path: 标题行是执行最终传递通道的作业项。但对某些通道而言（如 ims-ms 通道），由 MTA 添加 Return-path: 报头的效率比允许通道添加之作业法更好。关键字 addreturnpath 可使 MTA 在邮件于该通道入队时添加 Return-path: 报头。

从信封的 To: 和 From: 地址构建 Received: 标题行

关键字：receivedfor, noreceivedfor, receivedfrom, noreceivedfrom

关键字 receivedfor 可指示 MTA：如果某邮件只定址给一个信封收件人，则将该信封的 To: 地址包括在构建的 Received: 标题行中。关键字 receivedfor 为默认值。关键字 noreceivedfor 将指示 MTA 构建 Received: 标题行，但不包括任何信封地址信息。

关键字 receivedfrom 用于指示 MTA：如果 MTA 由于某种邮件发送列表的扩展（举例）而更改了信封 From: 地址，则在构建入站邮件的 Received: 标题行时包括原信封的 From: 地址。receivedfrom 是默认设置。关键字 noreceivedfor 将指示 MTA 构建 Received: 标题行，但不包括原信封的 From: 地址。

处理地址 标题行中的注释

关键字：commentinc, commentmap commentomit, commentstrip, commenttotal, sourcecommentinc, sourcecommentmap, sourcecommentomit, sourcecommentstrip, sourcecommenttotal

MTA 只在必要时解释标题行的内容。然而，所有含地址的注册标题行必须在分析后重写，并去除短格式地址，或将其转换为合法地址。在此过程中，系统将在重新构建标题行时抽取并可能修改或排除注释 （即括号中的字串）。

对这一系统行为的控制，可通过使用关键字 commentinc、commentmap、commentomit、commentstrip 和 commenttotal 加以实现。关键字 commentinc 将指示 MTA 保留标题行中的注释。这是默认值。关键字 commentomit 将指示 MTA 从寻址报头中移除任何注释，例如：To:、 From: 或 Cc: 标题行。

关键字 commenttotal 将指示 MTA 从所有标题行中移除任何注释，但 Received: 标题行除外；这个关键字通常用处不大，也不建议用户使用。关键字 commentstrip 可指示 MTA 从所有注释字段中去除任何非基本单元之字符。关键字 commentmap 可通过 COMMENT_STRINGS 映射表运行注释字串。

在源通道上时，对这种系统行为的控制可通过下列关键字的使用加以实现：sourcecommentinc、 sourcecommentmap、 sourcecommentomit、sourcecommentstrip 和 sourcecommenttotal。关键字 sourcecommentinc 将指示 MTA 保留标题行中的注释。这是默认值。关键字 sourcecommentomit 用于指示 MTA 从寻址报头中（例如，To:、From: 和 Cc: 报头）移除任何注释。关键字 sourcecommenttotal 用于指示 MTA 从所有标题行中移除任何注释，但 Received: 报头除外；因为这个关键字通常用处不大，也不建议用户使用。最后，关键字 sourcecommentstrip 用于指示 MTA 从所有注释字段中去除任何非基本单元之字符。关键字 sourcecommentmap 可通过源通道运行注释字串。

这些关键字可应用于任何通道。

COMMENT_STRINGS 映射表的语法如下：

(*comment_text*) | *address*

如果该条目模板设定有 $Y 标志，原注释则由特定的文本 （应包括括号）予以替换。

处理地址标题行中的人名

关键字：personalinc, personalmap, personalomit, personalstrip, sourcepersonalinc, sourcepersonalmap, sourcepersonalomit, sourcepersonalstrip

在重写过程中，所有含地址的注册标题行必须在分析后重写，并去除短格式地址，或将其转换为合法地址。在此过程中，系统将在重新构建标题行时抽取并可能修改或排除人名 （即用尖括号分割的地址前面的字串）。

对这一系统行为的控制，可通过使用关键字 personalinc、personalmap、personalomit 和 personalstrip 加以实现。关键字 personalinc 可指示 MTA 保留报头中的人名。这是默认值。关键字 personalomit 用于指示 MTA 移除所有人名。关键字 personalstrip 用于指示 MTA 从所有人名字段中去除任何非基本单元之字符。关键字 personalmap 用于指示 MTA 通过 PERSONAL_NAMES 映射表运行人名。

在源通道上时，对这种系统行为的控制可通过下列关键字的使用加以实现：sourcepersonalinc、 sourcepersonalmap、 sourcepersonalomit 或 sourcepersonalstrip。关键字 sourcepersonalinc 可指示 MTA 保留报头中的人名。这是默认值。关键字 sourcepersonalomit 用于指示 MTA 移除所有人名。最后，关键字 sourcepersonalstrip 用于指示 MTA 从所有人名字段中去除任何非基本单元之字符。关键字 sourcepersonalmap 用于指示 MTA 通过源通道运行人名。

这些关键字可应用于任何通道。

PERSONAL_NAMES 映射表探查句的语法为：

personal_name | *address*

如果模板设定有 $Y 标志，原来的人名则以特定文本替换。

指定别名文件和别名数据库探查项

关键字：aliaslocal

在一般情况下，只有被重写到本地通道 （即 UNIX 上的通道 1）的地址可在别名文件和别名数据库中查找。关键字 aliaslocal 可被放置在某一通道上，以使被重写到该通道的地址也可在别名文件和别名数据库中查找。查找所造之探查句的具体格式由 ALIAS_DOMAINS 选项控制。

子地址的处理

关键字：subaddressexact, subaddressrelaxed, subaddresswild

作为有关子地址的概念的背景资料，本地和 ims-ms 通道需特别解释地址 （邮箱部分）的本地部分中的 + 字符：在格式为 *name+subaddress@domain* 的地址中， MTA 将 + 字符后面的邮箱部分视为子地址。本地通道把子地址当作附加的修饰信息加以处理，并在不考虑子地址的情况下将其传递到帐户名； ims-ms 通道则将子地址解释为文件夹名，即需将其传递到的文件夹。

子地址还对下列各项有影响：按本地通道查找的别名 （即 UNIX 上的 L 通道） 、按标记有 aliaslocal 关键字之任何通道查找的别名，以及按目录通道查找的邮箱。对以此种方式匹配的子地址的具体处理，其方法是可以配置的：当对照一个条目比较子地址时， MTA 总是先检查包括全字匹配的子地址的整个邮箱；另外， MTA 是否在此后需进行其它或额外检查，这也是可以配置的。

关键字 subaddressexact 用于指示 MTA 在匹配条目期间不进行特殊的子地址处理；整个邮箱 （包括子地址）必须与一条目匹配，以使别名被视为与之匹配。系统将不进行额外的比较（特别是不进行通配符的比较或子地址已被移除项的比较）。关键字 subaddresswild 将指示 MTA 在寻找包括整个子地址在内的精确匹配项后， MTA 下一步应寻找格式为名称 +* 的条

目。关键字 subaddressrelaxed 用于指示 MTA 在寻找精确匹配以及与之匹配的格式为名+* 的项目后，MTA 应只对名称部分的匹配情况再次检查。使用关键字 subaddressrelaxed 时，具下列格式的别名条目可匹配于名称或名称 + 子地址，从而将原名转换为新名称，并将名称 + 子地址转换为新名称 + 子地址。关键字 subaddressrelaxed 为默认值。

```
name:   newname+*
```

因此，关键字 subaddresswild 或关键字 subaddressrelaxed 可在别名或目录通道被占用但用户想接收用任意子地址定址的邮件时使用。这些关键字免除了为一个地址上的每一单个子地址变体提供分开的条目之必要。

需注意的一点是，这些关键字只对本地通道 （即 UNIX 上的 L 通道）和目录通道，或任何有 aliaslocal 关键字标记的通道有意义。

标准的 Messaging Server 配置只转接到真正有 subaddressrelaxed 行为的 L 通道（当其它关键字没有明确使用时，此乃默认关键字）。

启用具体通道的重写规则检查

关键字：rules,norules

关键字 rules 用于指示 MTA 强制对该通道的重写规则进行检查。这是默认值。关键字 norules 用于指示 MTA 不检查该通道。这两个关键通常在调试时使用，很少在实际应用中使用。

移除源路由

关键字：dequeue_removeroute

关键字 dequeue_removeroute 可用来在邮件出队时从信封 To：地址中移除源路由。该关键字目前只能在 tcp-* 通道上执行。当把邮件传送到不能正确处理源路由的系统时，可用此关键字。

指定必须来自别名的地址

关键字：viaaliasoptional,viaaliasrequired

viaaliasrequired 可指定：与通道匹配的最终收件人地址必须由一别名生成。最终收件人地址是指进行别名扩展后 （如果相关的话）的匹配项。该地址不能作为收件人地址直接交与 MTA ； 也就是说，只将地址重写到通道是不够的。在重写至通道后，地址还需通过别名扩展，然后才能被视为真正与通道匹配。

例如，关键字 viaaliasrequired 可在一本地通道上使用，以防止被传送到任意帐户 （如 UNIX 系统上的任意本地 Berkeley 邮箱）。

默认关键字为 viaaliasoptional，这意味系统并不要求与通道匹配的最终收件人地址一定要从一别名而生。

配置邮件头处理功能

本节将就处理邮件头或报头以及信封信息的关键字加以说明。这一部分由下列分节组成：

- 重写嵌入邮件头
- 移除选定的邮件标题行
- 生成 / 移除 X-Envelope-to: 标题行
- 将日期转换为二或四位数
- 指定日期中的星期
- 自动分割长标题行
- 报头对齐和折行
- 指定报头最大长度
- 阅读权限检查
- 设置报头的默认语言

重写嵌入邮件头

关键字：`noinner`, `inner`

标题行的内容只在必要时才予以解释。然而，由于 MIME 邮件能在邮件中嵌入邮件（message/RFC822），故可含多套邮件头。MTA 通常只解释和重写邮件头的最外围的部分。也可通过选择指示 MTA 对邮件内的内部邮件头同样应用邮件头重写。

此项操作可通过使用 `noinner` 和 `inner` 两个关键字得以控制。关键字 `noinner` 可指示 MTA 不重写邮件内的标题行。这是默认值。关键字 `inner` 可指示 MTA 对邮件语法进行分析并重写邮件内的邮件头。这些关键字可应用于任何通道。

移除选定的邮件标题行

关键字：`headertrim`, `noheadertrim`, `headerread`, `noheaderread`, `innertrim` `noinnertrim`

MTA 可提供针对每一通道的工具，用以修剪或移除所选邮件的标题行。这项操作可通过通道关键字与相关的一个或两个报头选项文件之结合而实现。关键字 `headertrim` 可指示 MTA *在对原邮件头进行处理后*，先查找与通道相关的邮件头选项文件，然后对排列在该目的地通道中的邮件之报头进行相应的修剪。关键字 `noheadertrim` 可免除对邮件头的修剪。关键字 `noheadertrim` 是默认值设置。

关键字 `innertrim` 用于指示 MTA 同时在里面的邮件部分进行邮件头修剪，即嵌入的 MESSAGE/RFC822 部分。默认关键字 `noinnertrim` 可用于指示 MTA 不对里面的邮件部分进行邮件头修剪。

关键字 headerread 可指示 MTA *在对原邮件头进行处理前*，先查找与通道相关的邮件头选项文件，然后对排列在该源通道中的邮件之报头进行相应的修剪。请注意， headertrim 邮件头的修剪却是在邮件处理后应用的，而且是目的地通道，而非源通道。关键字 noheaderread 可免除入队邮件报头修剪。 noheaderread 是默认关键字。

与关键字 headeromit 和 headerbottom 不同的是，关键字 headertrim 和 headerread 可应用于任何通道。然而须注意的情况是，从邮件中去除重要的报头信息可能会使 MTA 出现不正常的操作。因此在选择需移除或限制的报头时，须务必谨慎为佳。之所以要提供这种工具，是因为被选取的标题行有时必须移除或通过其它方式加以限制。

注意 从邮件中去除报头信息可能会使 MTA 出现不正常的操作。因此在选择需移除或限制的报头时，须谨慎为佳。之所以要提供这 ie 关键字，是因为被选取的标题行有时必须移除或加以限制。在修剪或移除任何标题行之前，您必须理解标题行的用途，并考虑到移除后可能带来的影响。

关键字 headertrim 和 innertrim 的报头选项文件所具有的名称呈 *channel*_headers.opt 格式加上通道，即报头选项文件与之相关的通道名称。同样，关键字 headerread 所具有的名称呈 channel_read_headers.opt 格式。这些文件储存于 MTA 配置目录：*server_root*/msg-*instance*/imta/config/。

生成 / 移除 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 用于控制在排列于具体通道中的邮件副本上生成或抑制 X-Envelope-to 标题行。在标记有 single 关键字的通道上，关键字 x_env_to 可启用这些报头的生成，而 nox_env_to 则可从入队的邮件中移除此类报头。默认关键字是 nox_env_to。

关键字 x_env_to 还需要有 single 关键字与之一起使用才能起作用。

将日期转换为二或四位数

关键字：datefour, datetwo

原有的 RFC 822 规范要求邮件头中的日期字段应为两位数年份。后来出版的 RFC 1123 将日期格式改为四位数，然而，有些老邮件系统却无法接受四位数日期。更麻烦的是，较新的邮件系统又不能忍受两位数的日期。

备注 凡是不能处理这两种日期格式的系统，都属违反标准。

关键字 datefour 和 datetwo 可用来控制 MTA 在处理邮件头中的年份字段的方法。默认的关键字 datefour 可指示 MTA 将所有年份字段扩展为四位数。系统将在小于 50 的两位数日期值中添加 2000，而在大于 50 的值中添加 1900。

注意 关键字 datetwo 可指示 MTA 从四位数日期中删除前面的两位数。这是为需要使用两位数日期的不符合标准的邮件系统提供兼容性；但决不应用于任何其它目的。

指定日期中的星期

关键字：dayofweek, nodayofweek

RFC 822 规范允许在邮件头的日期字段中存在主要的星期格式。然而，有些系统则不能接受有关星期的信息。致使某些系统不愿将星期信息包括在内，即使在邮件头中包括这样的信息很有用处。

关键字 dayofweek 和 nodayofweek 可控制 MTA 处理星期信息的方式。默认关键字 dayofweek 可用来指示 MTA 保留任何星期信息，并在缺失的情况下将其添加到日期和时间报头中。

注意 关键字 nodayofweek 可指示 MTA 从日期和时间报头中移除任何主要的星期信息。这是为不能处理星期信息的不符合标准的邮件系统提供的一种兼容方式；但决不应用于任何其它目的。

自动分割长标题行

关键字：maxheaderaddrs, maxheaderchars

有些邮件传递程序，特别是有些 sendmail 系统，不能妥善地处理长标题行。其结果往往不仅是使报头损坏，而且会误使邮件遭到拒绝。虽然这种操作严重违反了标准，但却是一个较常见的问题。

MTA 提供的、针对具体通道的工具可将长标题行分割（拆开）成多个独立的标题行。关键字 maxheaderaddrs 用于控制一行上可以显示多少个地址。关键字 maxheaderchars 用于控制一行上可以显示多少个字符。这两个关键字都需要一个单一的整数参数，用以指定相关的限制。默认设置是：不限制标题行的长度，也不限制显示的地址数量。

报头对齐和折行

关键字：headerlabelalign, headerlinelength

关键字 headerlabelalign 用于控制在该通道上排列的邮件头的成行点；需使用一整数值的变量。对齐点乃是报头内容对齐的页边距。例如，取 10 为样本标题行的对齐点时，其格式为下列：

```
To:       joe@siroe.com
From:     mary@siroe.com
Subject:  Alignment test
```

默认 headerlabelalign 是 0，可使报头不对齐。关键字 headerlinelength 用于控制在该通道上排列的邮件标题行的长度。长度超过这一限制的行将按照 RFC 822 折行规则折行。

这些关键字只控制邮件队列中的邮件报头格式；报头的实际显示通常由用户代理程序控制。此外，当邮件在因特网上传输的时候，报头会定期被重新格式处理，所以这些关键字可能没有显著的效果，即使与不能重新格式处理邮件头的简单用户代理程序一起使用时，也是如此。

指定报头最大长度

关键字：maxprocchars

处理含许多地址的长标题行是一项非常耗用系统资源的操作。关键字 maxprocchars 可用来指定 MTA 能处理并重写的最大报头长度。报头长度超过此限的邮件仍可被接受和传递，但唯一不同的是长标题行将不会被以任何方式重写。此项操作需使用单一的整数参数。默认设置是处理任何长度的报头。

阅读权限检查

关键字：sensitivitynormal, sensitivitypersonal, sensitivityprivate sensitivitycompanyconfidential

阅读权限检查关键字可设定某通道可接受的邮件阅读权限的上限。默认关键字是 sensitivitycompanyconfidential ；即任何阅读权限的邮件都可通过。无 Sensitivity: 报头的邮件被视为正常邮件，即最低的阅读权限。邮件阅读权限高于由此关键字指定之限制者，将在其于通道入队之时予以拒收，并拌以下列出错讯息：

```
message too sensitive for one or more paths used
```

请注意， MTA 的这种阅读权限检查是根据每封邮件的情况，而不是在每个收件人级上进行的：即如果一个收件人的目的地通道没有通过阅读权限检查，则所有收件人的邮件都将被退回，而不是只退回与此阅读权限通道相关的收件人的邮件。

设置报头的默认语言

关键字：language

报头中的编码文字可以为某种特定语言。关键字 language 可指定所需的默认语言。

附件与 MIME 处理

本节将就附件和 MIME 处理所需使用的关键字加以说明。这一部分由下列分节组成：

- 忽略 Encoding: 标题行
- 自动重组邮件 / 部分邮件
- 大型邮件自动拆分
- 实施邮件行长度限制

忽略 Encoding: 标题行

关键字：ignoreencoding, interpretencoding

MTA 可用 Yes CHARSET-CONVERSION 将各种非标准的邮件格式转换为 MIME。特别是 RFC 1154 格式，因为这种格式使用了一种非标准的 Encoding: 标题行。然而，有些网关会在这种标题行上传送一些不正确的信息，其结果是有时最好忽略这种标题行。关键字 ignoreencoding 可用来指示 MTA 忽略任何 Encoding: 标题行。

备注	除非 MTA 启用了 CHARSET-CONVERSION，否则这种报头在任何情况下都予以忽略。关键字 interpretencoding 可用来指示 MTA 严加注意任何有 Encoding: 的标题行（如果是通过其它方式如此配置的话）；该关键字是默认设置。

自动重组邮件 / 部分邮件

关键字：defragment, nodefragment

MIME 标准规定了可将邮件分成几个小部分的邮件 / 部分内容类型。这一规定的用处在于：当邮件需在有大小限制的网络上传输时，或在不可靠的网络上传输时邮件分段可被“检查点”阻挡，从而使邮件在传输期间因网络故障而无法随后进行全面复制还原。这一标准规定了邮件每一部分中应包括的信息，以便邮件可在抵达目的地后自动重新组装。

通道关键字 defragment 和重组通道为在 MTA 中重新组装邮件提供了有效的手段。当某通道被标记为 defragment 时，通道中排列的任何部分邮件都将被转到重组通道队列。待所有“部分”抵达后，系统将重建邮件，然后发送出去。关键字 nodefragment 用于关闭此特殊处理功能。关键字 nodefragment 为默认值。

大型邮件自动拆分

关键字：maxblocks,maxlines

有些电子邮件系统或网络传输装置不能处理超过一定大小限制的邮件。MTA 提供的工具可用来在每一通道的基础上实行这种限制。超过设定限制的邮件将自动被拆分 （分段）为几个小邮件。用于这种拆分作业的内容类型是 message/partial，并添加有一独特的 ID 参数，以便同一邮件的各个部分可相互关联，并可由接收邮件程序自动重新组装。

关键字 maxblocks 和 maxlines 用于实施大小限制，一旦有超限的邮件，拆分功能便可自动启用。这两个关键字后面都需跟有单一的整数值。关键字 maxblocks 用于指定邮件中允许的最大信息块数量。 MTA 的一个信息快通常为 1024 字节；这一数量可用 MTA 选项文件中的 BLOCK_SIZE 选项进行变换。关键字 maxlines 用于指定邮件中允许的最多行数。需要时，这两个极限可同时实施。

从某种程度上讲，邮件的大小包括邮件头。因为邮件头不能被分成多个邮件，但邮件头本身却能超过指定的大小限制，故须使用一个非常复杂的机制来计算邮件头的大小。这一逻辑受控于 MTA 选项文件中的 MAX_HEADER_BLOCK_USE 和 MAX_HEADER_LINE_USE 选项。

MAX_HEADER_BLOCK_USE 用于指定 0 和 1 之间的一个实数。默认值是 0.5。系统只允许邮件头占用邮件可消耗的总信息块数量的一定数量（由关键字 maxblocks 指定）。如果邮件头较大， MTA 则取 MAX_HEADER_BLOCK_USE 和 maxblocks 的乘积作为邮件头的大小 （邮件头的大小取实际邮件头大小和 maxblocks 之间的较小者） * MAX_HEADER_BLOCK_USE。

例如，如果 maxblocks 是 10 且 MAX_HEADER_BLOCK_USE 是默认值 （即 0.5），则任何大于 5 个信息块的邮件头都将作为 5-block 报头处理，如果邮件的大小是 5 个信息块或更少，则不予以拆分。就邮件大小极限而言， 0 值会使报头有效地得以忽略。

该值为 1 时，系统则允许邮件头使用所有可用的量。每一拆分的部分至少要有一行，不论其是否超过极限。MAX_HEADER_LINE_USE 在与关键字 maxlines 一起使用时，其作业方法与此相同。

实施邮件行长度限制

关键字：linelength

SMTP 规范允许文本行数可含 1000 字节。然而，有些传输装置则可对行长度实施严格的限制。关键字 linelength 提供的机制可用来以通道为基础限制最大允许的邮件行长度。如果在特定通道入队的邮件，其长度超过了为该通道指定的极限，系统则自动对其进行编码处理。

MTA 中可用的各种编码功能总能将行长度降至少于 80 个字符。原邮件可在经过这种编码后得以还原，方法是：应用适当的解码过滤器。

备注	编码功能只能将行长度减至不多于 80 个字符。小于 80 的行长度值规范可能不会真正地生成符合所述限制的行长。

关键字 linelength 可使数据的编码作业为传输目的而进行 “软”折行。编码通常在接收端解码，以便恢复原来的 “长”行。有关 “硬”折行的说明，请见 “Record, text” CHARSET-CONVERSION。

邮件大小限制、用户定额和特权

本节说明设定邮件大小限制、用户定额和特权所需使用的关键字。这一部分由下列分节组成：

- 指定邮件的绝对大小极限
- 处理超定额用户的邮件传递

指定邮件的绝对大小极限

关键字：blocklimit, noblocklimit, linelimit, nolinelimit, sourceblocklimit

虽然拆分可自动将邮件分成小块，但在有些情况下，较为适宜的做法是拒收那些超过管理部门界定之极限的邮件 （例如，为了防止因蓄意的攻击而出现拒绝服务现象）。

关键字 blocklimit、linelimit 和 sourceblocklimit 用于实施绝对大小限制。这几个关键字后面都需跟有单一的整数值。

关键字 blocklimit 用于指定邮件中允许的最大信息块数量。对于信息块数量超过此限量的邮件，MTA 将拒绝把其排入通道的尝试。MTA 的一个信息快通常为 1024 字节；这一数量可用 MTA 选项文件中的 BLOCK_SIZE 选项进行变换。

关键字 sourceblocklimit 用于指定入站邮件中允许的最大信息块数量。对于信息块数量超过此限量的邮件，MTA 将拒绝把其提交到通道的尝试。换言之，blocklimit 适用于目的地通道； sourceblocklimit 适用于源通道。 MTA 的一个信息快通常为 1024 字节；这一数量可用 MTA 选项文件中的 BLOCK_SIZE 选项进行变换。

关键字 linelimit 用于指定邮件中允许的最多行数。对于行数超过此限量的邮件， MTA 将拒绝把其排入通道的尝试。必要时，关键字 blocklimit 和 linelimit 可同时施加。

MTA 选项 LINE_LIMIT 和 BLOCK_LIMIT 可在所有通道上实施类似的限制。这些极限的好处是它们可在所有通道上使用。因此， MTA 服务器可在获得邮件收件人信息之前，使邮件客户程序对此有所准备。对于某些通信协议而言，这种限制简化了邮件拒收过程。

通道关键字 nolinelimit 和 noblocklimit 都是默认值，这意味着除了通过 LINE_LIMIT 或 BLOCK_LIMIT MTA 选项施加的任何全局限制外，没有其它限制。

处理超定额用户的邮件传递

关键字：holdexquota, noexquota

关键字 noexquota 和 holdexquota 可用来控制如何处理传送给 Berkeley 邮箱用户（UNIX）的邮件，即用户传递到 uid 本地通道，但用户超过了他们的磁盘定额。

noexquota 可指示 MTA 将传送给超定额用户的邮件退回给邮件的发件人。 holdexquota 则指示 MTA 暂时保留传送给超定额用户的邮件；这类邮件将保留在 MTA 队列中，直至被传递或超时为止，然后通过邮件退回作业将其退回给发件人。

在 MTA 队列 中创建文件

本节描述您可用之控制磁盘资源的关键字，具体方法是在 MTA 队列中指定需创建的文件。这一部分由下列分节组成：

- 控制如何处理邮件上的多地址
- 在多个子目录上分布通道邮件队列

控制如何处理邮件上的多地址

关键字：`multiple`, `addrsperfile`, `single`, `single_sys`

MTA 允许每一入队的邮件显示多个目的地址。有些通道程序只能处理有一个收件人的邮件，或有有限数量收件人的邮件，或每个邮件副本只有一个目的地系统的邮件。例如，SMTP 通道主程序在特定的事务处理中只能与单一远程主机建立连接，至此只有定址到该主机的地址能够得到处理 （即尽管某单一通道通常可用于所有 SMTP 业务）。

另一个例子是，有些 SMTP 服务器可能会就其一次处理收件人的数量施加限量，同时又不能处理此类错误。

关键字 `multiple`、`addrsperfile`、`single` 和 `single_sys` 可用于控制如何处理多个地址。关键字 `single` 可指定为每个目的地址在通道上创建一个单独的邮件副本。关键字 `single_sys` 可为每个所用目标系统创建一个单一的邮件副本。默认关键字 `multiple` 可用来为整个通道创建邮件的单一副本。

备注 不论使用哪个关键字，系统都将为邮件入队的每个通道至少创建一个邮件副本。

关键字 `addrsperfile` 用于在限制收件人的最大数量，即与通道队列中单一邮件文件相关的收件人数量，这样便可限制一次作业处理的收件人数量。该关键字需要使用单一整数变量，用以指定邮件文件中允许的最大收件人地址数量；如果达到了这个数，MTA 将自动创建额外的邮件文件将其容纳在其中。（默认关键字 `multiple` 总体上相当有于不在邮件文件中施加收件人数量限制，但 SMTP 通道的默认设置为 99。）

在多个子目录上分布通道邮件队列

关键字：`subdirs`

其默认设置是：所有入队的邮件都作为文件储存在 `/imta/queue/`*channel-name* 目录中，其中 *channel-name* 为通道名。然而，对于需处理大量邮件的通道而言，如 TCP/IP 通道，因为总是累积有大量等待处理的邮件文件，所以若把这些邮件文件分布到几个子目录，文件系统的性能可能会有所改善。通道关键字 `subdirs` 提供了这一能力：其后应跟有一个整数，用以指定在其上分布该通道邮件的子目录的数量；例如：

```
tcp_local single_sys smtp subdirs 10
```

配置日志记录和调试

本节说明关键字 logging 和 debugging。

- 日志记录关键字
- 关键字 Debugging
- 设置循环检查

日志记录关键字

关键字： `logging`, `nologging`

MTA 提供的工具可记录入队和出队的每一封邮件的情况。关键字 `logging` 和 `nologging` 可针对每个通道控制邮件的日志记录。在默认状态下，初始配置将打开所有通道的日志记录功能。在通道定义中替换成 `nologging` 关键字可禁用某个特定通道的日志记录功能。

有关日志记录的详细说明，请见第 13 篇，“日志记录和日志分析”。

关键字 Debugging

关键字：`master_debug`, `slave_debug`, `nomaster_debug`, `noslave_debug`

一些通道程序包含有可选代码，以便产生附加的诊断输出来协助调试。有两个通道关键字可用来启用产生针对每一个通道的调试输出。这两个关键字是：在主程序中启用调试输出的 `master_debug` 和在从属程序中启用调试输出的 `slave_debug`。默认状态下，两类调试输出都被禁用，相应关键字为 `nomaster_debug` 和 `noslave_debug`。

启用后，调试输出将出现在与通道程序相关的日志文件中。日志文件的位置因程序而异。日志文件通常保存在日志目录中。主程序日志文件名的形式通常为 *x*`_master.log`，此处的 *x* 为通道名。从属程序日志文件名的形式通常为 *x*`_slave.log`。

在 UNIX 中，当 `master_debug` 和 `slave_debug` 启用用于 `1` 通道时，用户随后会在含 MTA 调试信息的当前目录中收到 `imta_sendmail.log-`*uniqueid* 文件（如果他们有写入该目录的权限的话；否则调试输出转到 stdout）。

设置循环检查

关键字：`loopcheck`, `noloopcheck`

关键字 `loopcheck` 可将字串放置在 SMTP EHLO 应答标志区，以便 MTA 检查其自身是否在与之通信。当设定了 `loopcheck` 时， SMTP 服务器将以 XLOOP 扩展文件出面。

当它与支持 XLOOP 的 SMTP 服务器通信时， MTA 的 SMTP 客户程序将用其 MTA 值比较显示的字串，并在客户程序与 SMTP 服务器实际通信之时立即退回邮件。

其它关键字

本节描述其它关键字的使用方法。这一部分由下列分节组成：

- 通道操作类型
- 管道通道
- 指定邮箱过滤器文件的位置

通道操作类型

关键字：submitsubmit

Messaging Server 支持 RFC 2476 的邮件提交协议。关键字 submit 可用于将一通道标记为仅用于提交的通道。这通常对 TCP/IP 通道最为有用，如一个运行在专用于提交邮件的特殊端口上 SMTP 服务器； RFC 2476 将端口 587 确定为用于此类邮件提交。

管道通道

关键字：user

关键字 user 用于在管道通道上指示在哪个海洋名下运行。

请注意，user 的参数或变量通常被强制使用小写，但如果是引用参数，则保留原来的大小写字样。

指定邮箱过滤器文件的位置

关键字：filter, nofilter, channelfilter, nochannelfilter, destinationfilter nodestinationfilter, sourcefilter, nosourcefilter, fileinto, nofileinto)

关键字 filter 可用来在本机和 ims-ms 通道上指定该通道的用户过滤器文件的位置。描述过滤器文件位置时，须用 URL 参数。nofilter 是默认设置，它意味着用户邮箱过滤器没有为该通道而启用。

关键字 sourcefilter 和 destinationfilter 可用来在一般的 MTA 通道上指定通道级过滤器，以分别应用于入站和出站邮件。这些关键字需使用 URL 参数描述通道过滤器文件的位置。 nosourcefilter 和 nodestinationfilter 是默认设置，它意味着没有为通道的任何后一个方向启用通道邮箱过滤器。

已废弃的关键字 channelfilter 和 nochannelfilter 分别与 destinationfilter 和 nodestinationfilter 同义。

目前只支持 ims-ms 通道的关键字 fileinto 用于指定施加了邮箱过滤器的 fileinto 算符后如何改变地址。对于 ims-ms 通道而言，通常的用法为：

```
fileinto $U+$S@$D
```

上述例子指定：文件夹名称应作为子地址插入到原地址，以此替换任何原有的子地址。

第 9 篇

使用预定义通道

在第一次安装 iPlanet Messaging Server 时，一些通道已经定义（参见表 9-1）。本章说明如何在 MTA 中使用预定义通道的定义。

如果尚未阅读第 6 篇，“关于 MTA 服务与配置”，请在阅读后再回到本章内容。有关在 `imta.cnf` 文件中配置重写规则方面的信息，请参阅第 7 篇，“配置重写规则”。

本章包括以下各节：

- 使用管道通道传递邮件到程序
- 配置本机 （/var/mail）通道
- 使用保存通道临时保存邮件
- 转换通道
- 字符集转换和邮件重格式化

表 9-1　预定义通道

通道	定义
`l`	**仅限 UNIX 使用。**用于做路由决定和用 UNIX 邮件工具发送邮件。
`ims-ms`	将邮件传递至本地存储库。
`native`	**仅限 UNIX 使用。**将邮件传递至 `/var/mail`。（请注意，Messaging Server 不支持对 `/var/mail` 的访问。用户必须使用 UNIX 工具访问 `/var/mail` 存储库中的邮件。）
`pipe`	用于通过站点提供的程序或脚本执行传递。管理员可通过 imsimta 程序界面控制管道通道执行的命令。有关详细信息，请参阅第 212 页“使用管道通道传递邮件到程序”。
`reprocess` `process`	这些通道用于延迟及离线邮件的处理。`reprocess` 作为源或目标通道通常是不可见的， `process` 则同其它 MTA 通道一样是可见的。
`defragment`	提供重新组装 MIME 拆分邮件的手段。
`conversion`	对 MTA 中流动的邮件实施正文部分到正文部分的转换。
`bitbucket`	用于需放弃的邮件。

表 9-1　预定义通道（接上页）

通道	定义
inactive/deleted	用于为已在目录中被标记为非活动 / 已删除状态的用户处理邮件。典型的处理是：退回邮件并向邮件的发送者返回定制的退信消息。
hold	用于为用户暂存邮件。例如，当用户从一个邮件服务器迁移到另一个时。
autoreply	用于处理自动回复和休假通知请求。
tcp_local tcp_intranet tcp_auth tcp_submit tcp_tas	在 TCP/IP 上实现 SMTP。多线程的 TCP SMTP 通道包括一个在 Dispatcher 控制下运行的多线程 SMTP 服务器。外发的 SMTP 邮件由通道程序 tcp_smtp_client 处理，并在需要时在 Job Controller 的控制下运行。 tcp_local 从远程 SMTP 主机接收入站邮件。根据您是否使用 smarhost/ 防火墙配置，可以直接将出站邮件发送到远程 SMTP 主机或发送到 smarthost/ 防火墙系统。 tcp_intranet 在 intranet 内部接收和发送邮件。 tcp_auth 用作 tcp_local 的切换通道，授权的用户为躲避 realy-blocking 限制可切换到 tcp_auth 通道。 tcp_submit 在保留的提交端口 587（参见 RFC 2476）接受通常由用户代理服务器提交的邮件。 tcp_tas 是提供 “一体化通信”服务的网站使用的特殊通道。

使用管道通道传递邮件到程序

用户可能希望将来件发往一个程序而不是他们的邮箱。例如，用户可能希望将来件发往邮件分类程序或发往类似于 Vacation Notice（休假通知）这样的自动回复代理程序。这种 pipe 通道使用针对每位用户的站点提供的程序来执行邮件传递。

为了便于程序传递，必须首先注册需要使用的程序，以便 pipe 通道调用。请用实用程序 imsimta program 进行程序注册。该实用程序对每一个注册的、可被 pipe 通道调用的命令赋予一个唯一的名字。然后最终用户就可以将该程序名作为其 mailprogramdeliveryinfo 的 LDAP 属性的值。

例如，要添加 UNIX 命令 myprocmail 作为能够被用户调用的程序，应该首先使用实用程序 imsimta program 来注册该命令，如下例所示。此例注册了一个名为 myprocmail 的程序；该程序以参数 -d *username* 执行程序 procmail 并作为用户而执行：

```
imsimta program -a -m myprocmail -p procmail -g "-d %s" -e user
```

请确保可执行程序位于 programs 目录 - *server-instance*/imta/programs - 并且执行许可设置为 “others”。

为了使用户能访问此程序，该用户的 LDAP 条目中必须包含下列属性和值：

```
maildeliveryoption:program
mailprogramdeliveryinfo: myprocmail
```

有关实用程序 `imsimta program` 的更多信息，请参阅 **iPlanet Messaging Server Reference Manual**。

备用传递程序必须符合以下退出码和命令行参数限制：

退出码限制。被 `pipe` 通道调用的传递程序必须返回含义确切的错误代码，以便通道得知是否将邮件出队、递交后续处理或退回邮件。

如果子进程以退出码 0 退出（`EX_OK`），即认为邮件已经成功传递并且从 MTA 队列中删除。如果以退出码 71、74、75 或 79（`EX_OSERR`、`EX_IOERR`、`EX_TEMPFAIL` 或 `EX_DB`）退出，即认为发生了临时错误并且邮件的传递被延迟。如果返回任何其他退出码，即认为邮件无法传递并将退回给发件人。这些退出码已在系统主文件 `sysexits.h` 中定义。

命令行参数。传递程序可以带有任意个固定参数以及可变参数，%s，代表用户执行之程序的用户名，或代表程序的用户名 + 域名（由邮局管理员 “inetmail” 执行）。例如，下列命令行使用程序 `procmail` 传递一封收件人的邮件：

```
/usr/lib/procmail -d %s
```

配置本机 （/var/mail）通道

您可通过一个选项文件控制本机通道的各种不同特性。此本机通道选项文件必须存储于 MTA 的配置目录并且命名为 `native_option`（例如，*server_root*`/msg-`*instance*`/imta/config/native_option`）。

选项文件包含若干行，每一行包含一个选项的设置信息。选项设置格式为：

```
option=value
```

此 *value* 根据选项的要求可以是一个字符串或是一个整数。

表 9-2　本地通道选项

选项	说明
`FORCE_CONTENT_LENGTH` （0 或 1，仅限 UNIX 使用）	如果 `FORCE_CONTENT_LENGTH`=1，则 MTA 添加一个 Content-length: 标题行至传递到本机通道的邮件，使得通道在 “From” 位于行首时不使用 “>From” 语法。这使本地 UNIX 邮件与 Sun 公司的新邮件工具兼容，但存在潜在的与其它 UNIX 邮件工具不兼容的问题。
`FORWARD_FORMAT` （字符串）	指定用户的 `.forward` 文件的位置。字符串 %u 的位置用每个用户 ID 取代。字符串 %h 的位置用每个用户的主目录替代。如果此选项未明确指定，则默认行为对应于： `FORWARD_FORMAT=%h/.forward`

表 9-2　本地通道选项 （接上页）

选项	说明
REPEAT_COUNT （整数） SLEEP_TIME （整数）	当 MTA 试图传递新邮件时，如果用户的邮件文件被阻塞，这些选项提供了控制本机通道程序尝试重试的次数和频率的方法。如果在指定的重试操作次数之后文件仍未打开，则邮件继续保留在本机队列中，在下一次本机通道运行时再将此邮件作为新邮件传递。 REPEAT_COUNT 选项用于控制在放弃之前通道程序尝试打开文件的次数。REPEAT_COUNT 的默认值为 30 （尝试 30 次）。 SLEEP_TIME 选项控制两次尝试之间间隔的秒数。 SLEEP_TIME 的默认值为 2 （两次重试之间间隔 2 秒）。
SHELL_TIMEOUT （整数）	控制通道在一 .forward 中等待一用户外壳命令的完成的时间长度，以秒为单位。在超时的情况下，邮件退回给原发送者并带有类似这样的出错信息 “Time-out waiting for *user*'s shell command *command* to complete”。默认值为 600 （10 分钟）。
SHELL_TMPDIR （特定目录）	控制在当传递到一个外壳命令时本地通道创建临时文件的位置。默认情况下，这样的临时文件创建在用户的主目录。使用此选项，管理员可选择将临时文件建立在其它 （单个）目录中。例如： SHELL_TMPDIR=/tmp

使用保存通道临时保存邮件

保存通道用来保存被临时停止接收新邮件之收件人的邮件。停止接收邮件可能是由于正在修改用户名或收件人邮箱正在从一邮件主机 （域）移向另一邮件主机。也可能还有其他原因导致用户临时被停止接收邮件，但这些最为常见。

通过将一个用户的 maildeliveryoption 值之一设置为 hold，邮件即可放置在保存通道中。 maildeliveryoption 的所有其他的值将被忽略 （maildeliveryoption 是一个多值属性），发往用户的邮件即路由到保存通道中。

与大多数通道不同的是，保存通道的主程序没有配置为自动运行。排入保存通道队列中的邮件将保持不动，直到管理员调用 hold_master 程序为止。

转换通道

此 conversion 通道可用于对流经 MTA 的指定邮件执行任意的正文部分到正文部分的处理。（注意：一个正文部分与一个邮件不同之处在于，一邮件可包含多个正文部分，例如，在一个附件中。 ）这种处理可由任意站点提供的程序或命令程序完成，而且可执行象这样的处理：将一种文本或图象格式转换为另一种文本或图象格式，病毒扫描，语言翻译等等。从流经 MTA 的邮件中选择各种类型的邮件进行转换，并且可以为每一种类型的邮件正文指定一组特定的进程或程序。

使用本章说明的先决条件是要理解通道的概念（请参见第 85 页“通道”）。有关使用 conversion 通道进行病毒扫描的补充信息，请查阅在 iPlanet Messaging Server Documentation 站点底部的 **iPlanet Messaging Server Technical Notes**。

转换通道的执行过程包括 A）选择需处理的邮件流量； B）确定如何处理不同的邮件。这些步骤将在后面做更详细的讨论。

备注 MTA 配置文件（imta.cnf）可自动建立默认的转换通道。这个通道可直接使用，无需任何修改。

MIME 概要

转换通道广泛使用 MIME （多用途 Internet 邮件扩充协议）标题行。用户需对邮件结构和 MIME 标题段有一定的了解。有关 MIME 的完整信息，请查阅 RFC 1806、 2045 到 2049 以及 2183。为方便起见，这里给出关于 MIME 的简短概述。

邮件结构

一个简单的邮件由一个标题和一段正文组成。标题位于邮件的顶端包含一些如日期，主题，发件人和收件人等控制信息。在标题下第一个空行的后面是正文。 MIME 规定了一种构造更复杂邮件的方法，这个方法使邮件可包含多个正文部分，甚至一个正文部分可以嵌套在另一个正文部分中。象这样的邮件称之为“multi-part”邮件，并且，如前面提到的，转换通道执行正文部分到正文部分的处理。

MIME 标题

MIME 规范为各种正文部分定义了一套标题行。它们包含了 MIME-Version、 Content-type、 Content-Transfer-Encoding、 Content-ID 和 Content-disposition。 Content-type 和 Content-disposition 是转换通道最常用的邮件头。含有若干 MIME 标题行的例子如下所示：

```
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"
```

Content-type （内容类型）标题

MIME Content-Type 标题描述了正文部分的内容。 Content-Type 标题格式 （加实例）如下所示：

Content-type: *type/subtype; parameter1=value; parameter2=value...*

type（类型）描述了正文部分内容的类型。类型的例子有 Text、 Multipart、 Message、 Application、 Image、 Audio 和 Video。

subtype（子类型）更进一步描述内容的类型。每一种 Content-type 都有它自己的子类型设置。例如：text/plain、application/octet-stream 和 image/jpeg。MIME 邮件的内容子类型由 IANA （因特网编号授权委员会）指定和开列。列表副本请见：http://www.isi.edu/in-notes/iana/assignments/media-types/media-types

parameter（参数）是针对每个特定的 Content-type/subtype 对的。例如，charset 和 name 参数如下所示：

```
Content-type: text/plain; charset=us-ascii
Content-type: application/msword; name=temp.doc
```

这里的 charset 参数用于指定文本邮件的字符集。如果数据要写入某个文件，这里的 name 参数给出一个建议的文件名。

备注 Content-Type 值， subtypes 和参数名都是不区分大小写的。

Content-disposition（内容配置）标题

MIME Content-disposition 标题为正文部分提供信息表示的方法。这些显示信息常被加到附件中，用以指定附件正文部分是否要显示 （inline），或是当作要复制文件的文件名显示 （attachment）。 Content-disposition 标题格式如下：

Content-disposition: *disposition_type; parameter1=value;parameter2=value...*

disposition_type 通常是 inline （显示正文部分）或 attachment （以要保存的文件形式显示）。 Attachment 通常有参数文件名和一个值，用以为保存的文件指定一个建议的名字。

关于 Content-disposition 标题的详细信息，请查阅 RFC 2183。

选定转换处理流量

与其它 MTA 通道不同，转换通道不是象通常那样在一个地址或 MTA 重写规则中指定。取而代之的是，邮件是用 CONVERSIONS 映射表 （由 imta_tailor 文件中的参数 IMTA_MAPPING_FILE 指定）而被发送到转换通道的。表条目格式如下：

IN-CHAN=*source-channel*;OUT-CHAN=*destination-channel*;CONVERT *Yes/No*

MTA 处理每个邮件时要探查 CONVERSIONS 映射表（如果映射表已给出）。如果 *source-channel*（源通道）是邮件进入的通道并且 *destination-channel*（目标通道）是外发邮件的通道，则在 CONVERT 后执行（Yes 意味着 MTA 将邮件从其 *destination-channel* 转移到转换通道；如果没找到匹配项，邮件将入队到常规的目标通道）。

备注 形如 user@conversion.*localhostname* 或 user@conversion 的地址将经由转换通道路由，而不管 CONVERSIONS 的映射表是何种状态。

下面的例子将所有的非内部邮件 （起源于或去往 Internet 的邮件）路由到转换通道。

```
CONVERSIONS

   IN-CHAN=tcp_local;OUT-CHAN=*;CONVERT    Yes
   IN-CHAN=*;OUT-CHAN=tcp_local;CONVERT      Yes
```

第一行指定来自 tcp_local 通道的邮件将被处理。第二指定去往 tcp_local 通道的邮件也将被处理。tcp_local 通道处理所有去往或来自于 Internet 的邮件。由于默认的是不通过转换通道，因而任何其它邮件都将不通过转换通道。

注意这是最基本的表，对于一个要使用更多定制配制的站点来说可能是不够的，例如，使用多重出站到 Internet 的 tcp_* 通道，或使用多重入站自 Internet 的 tcp_* 通道。

控制转换处理

当一个邮件发送到转换通道时，系统将按正文部分到正文部分的方式对其进行处理。处理由 MTA conversions 文件控制，该文件是由在 imta_tailor 文件中的 IMTA_CONVERSION_FILE 选项指定的 （默认值为：*server_root*/msg-*instance*/imta/conversions）。该 conversions 文件包含一些条目，用来控制要处理什么类型的正文部分以及如何进行处理。

每一个条目包含一行或多行，每行包含一个或多个 name=*value* 参数子句。这些参数子句中的 value 符合 MIME 约定。除最后一行外，每行必须以分号 （;）结尾。该文件中的物理行被限制在 252 个字符以内。可用反斜线（\）续行符号将一个逻辑行分为多个物理行。条目要么由一个以非分号结尾的行终止，要么由一个或多个空白行终止，也可以两种情况同时出现。

下面是一个简单的 conversion 文件条目的例子：

范例 9-1 conversion 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。即指定了要转换部分的类型。每一部分的标题被读取并抽取其中的 Content-Type: 和其它的标题信息。在 conversion 中的条目然后从第一条到最后一条被顺序扫描；任何给出的 in-* 参数，以及 OUT-CHAN 参数，如果给出，均予以检查。如果所有这些参数与正被处理的正文部分的相应信息相匹配，则执行 command= 或 delete= 子句所指定的转换，并且设置 out-* 参数。

如果没有匹配项，该部分就与下一个 conversions 文件条目进行匹配。一旦正文部分全部被扫描和处理（假设有一个合格的匹配），则将邮件向前发送到下一个通道。如果没有匹配项，则无处理，邮件被发送到下一个通道。

out-chan=ims-ms 指定只有发往 ims-ms 通道的邮件部分将被转换。in-type=application 和 in-subtype=wordperfect5.1 指定 MIME Content-type 邮件的标题部分必须是 application/wordperfect5.1。

通过额外的 in-* 参数可进一步限定邮件部分。（参阅表 9-5。）上面的条目将引发针对一邮件部分的转换，该邮件具有下列 MIME 标题行：

```
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"
```

在范例 9-1 中的三个 conversion 文件限定参数的后面，有另两个参数，out-type=application 和 out-subtype=msword，指定用置换的 MIME 标题行附加于“已处理”的正文部分。 out-type=application 和 out-subtype=msword 指定：外发邮件的 MIME Content-type/subtype 是 application/msword。

注意，既然 in-type 和 out-type 两参数是相同的， out-type=application 则不是非有不可，因为转换通道对外发正文部分默认采用原始 MIME 标签。通过额外的输出参数还可以为外发正文部分指定额外的 MIME 标签。

out-mode=block （范例 9-1）可指定站点提供的程序将返回的文件的类型。换句话说，它指定文件如何存储及转换通道，并如何在返回的文件中回读。例如，一个 html 文件存为文本模式，而一个 .exe 程序文件或 zip 文件则存为块 / 二进制文件模式。模式是一种描述方法，它表明被读取文件所具有的特定存储格式。

范例 9-1 中的最后参数：

```
command="/usr/bin/convert -in=wordp -out=msword 'INPUT_FILE'
'OUTPUT_FILE'"
```

指定对正文部分要采取的操作。参数 command= 指定一个将针对正文部分执行的程序。/usr/bin/convert 是假设的命令名； -in=wordp 和 -out=msword 是假设的用来指定输出文本和输入文本格式的命令行参数； INPUT_FILE 和 OUTPUT_FILE 是转换通道环境参数（参阅第 219 页“使用转换通道环境变量”）用来指定一个包含原始正文部分的文件和一个程序将变换后的正文部分存储于其中的文件。

与执行一个针对正文部分的命令不同，邮件部分可通过用 DELETE=1 取代 command 参数而简单地加以删除。

转换通道信息流

信息的流动如下所示：包含正文部分的邮件进入转换通道。转换通道分析邮件，并逐个处理各个部分。转换通道限定正文部分，换句话说，转换通道通过将 MIME 标题行与*限定参数*进行比较，确定正文部分是否应加以处理。如果正文部分符合要求，则开始进行转换处理。如果 MIME 或正文部分信息须传递给转换脚本，则如*信息传递参数*所指定的那样被存储在一个环境变量 （表 9-3）中。

此时，由*操作参数*指定的一个针对正文部分的操作被执行。典型的操作是正文部分被删除或被传递给一个包装在脚本中的程序。脚本处理正文部分随后将它发送回转换通道以便重新装配而成为处理后邮件。脚本也能使用转换通道的 *output options* 发送信息到转换通道。这样的信息可能是：添加到输出正文部分的新 MIME 标题行，返回给邮件发送者的出错信息文本，指示 MTA 起动一些如退回、删除、保存邮件之类操作的专用指令等。

最后，转换通道为*输出参数*所指定的正文部分替换标题行。

使用转换通道环境变量

当对正文部分进行操作时，将 MIME 标题行信息，或全部正文部分，传递到或取自站点提供的程序，通常是有用的。例如，一个程序可能需要 `Content-type` 和 `Content-disposition` 标题行信息以及一邮件的正文部分。通常一个站点提供的程序的主输入是从一个文件读出的一邮件的正文部分。在正文部分处理之后，此程序需要将正文部分写到一个以后能被转换通道读取的文件中。这样的信息传递是通过使用转换通道的环境变量实现的。

建立环境变量可以在 `conversions` 文件中使用 `parameter-symbol-*` 参数创建，也可以使用一组预定义的转换通道环境变量 （请参阅第 222 页表 9-4）。

下列 `conversions` 文件条目和进入的标题显示如何使用环境变量将 MIME 信息传递到站点提供的应用程序。

`conversions` 文件条目：

```
in-channel=*; in-type=application; in-subtype=*;
  parameter-symbol-0=APPARENT_NAME; parameter-copy-0=*;
  dparameter-symbol-0=APPARENT_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'"
```

入站邮件报头：

```
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：一个来自类型为 application 的任意输入通道的邮件正文部分将被处理。

parameter-symbol-0=APPARENT_NAME 指定：第一个 Content-type 参数值 （如此例中的 Draft1.doc）被存储在一个称为 APPARENT_NAME 的环境变量中。

parameter-copy-0=* 指定：输入正文部分的所有 Content-type 参数被复制到输出正文部分。

dparameter-symbol-0=APPARENT_FILENAME 指定：第一个 Content-disposition 参数值 （如此例中的 Draft1.doc）被存储在一个称为 APPARENT_FILENAME 的环境变量中。

dparameter-copy-0=* 指定：输入正文部分的所有 Content-disposition 参数被复制到输出正文部分。

message-header-file=2 指定：原始邮件的标题作为一个整体（最外层的标题）写入环境变量 MESSAGE_HEADERS 所指定的文件中。

original-header-file=1 指定：包括在 MESSAGE/RFC822 部分的原始标题写入环境变量 INPUT_HEADERS 所指定的文件中。

override-header-file=1 指定：MIME 标题从环境变量 OUTPUT_HEADERS 所指定的文件中读出，优先于包括在 MIME 部分中的原始标题。$OUTPUT_HEADERS 是一个在转换运行时建立的随时会消失的临时文件。一个站点提供的程序将使用这个文件存储在转换过程中改变了的标题。转换通道在重新装配正文部分时会从这个文件读取标题行。

override-option-file=1 指定：转换通道从环境变量 OUTPUT_OPTIONS 所指定的文件读取*转换通道选项*。请参阅第 221 页 “使用转换通道输出选项”。

command="SERVER_ROOT/msg-INSTANCE/bin/viro-scan500.sh" 指定针对邮件正文部分执行的命令。

表 9-3 转换通道环境变量

环境变量	说明
INPUT_ENCODING	正文部分原有的编码。
INPUT_FILE	包含原始正文部分的文件的名称。站点提供的程序将读取这个文件。
INPUT_HEADERS	包含正文部分的原始标题行的文件的名称。站点提供的程序将读取这个文件。
INPUT_TYPE	输入邮件部分的 MIME Content-type。
INPUT_SUBTYPE	输入邮件部分的 MIME 内容子类型。
INPUT_DESCRIPTION	输入邮件部分的 MIME content-description。
INPUT_DISPOSITION	输入邮件部分的 MIME content-disposition。
MESSAGE_HEADERS	包含一附加邮件 （不仅仅是正文部分）的原始最外层标题或部分中直接附加 MESSAGE/RFC822 部分的标题的文件的名称。站点提供的程序将读取这个文件。

表 9-3　转换通道环境变量（接上页）

环境变量	说明
OUTPUT_FILE	文件名称，即站点提供的程序应将其输出存储于其中的文件。站点提供的程序应建立并且写入这个文件。
OUTPUT_HEADERS	文件名称，即站点提供的程序应将附加部分的 MIME 标题行存储于其中的文件。站点提供的程序应建立并且写入这个文件。注意：文件将包含实际的标题行 （不是 option=value 行），后随一空行作为其最后一行。
OUTPUT_OPTIONS	文件名称，站点提供的程序将从中读取转换通道选项。请参阅第 221 页“使用转换通道输出选项”。

使用转换通道输出选项

转换通道输出选项（表 9-4）是将信息和专用指令从转换脚本传递到转换通道的动态变量。例如，在正文部分处理过程中，脚本可能要发送一个专用指令让转换通道退回邮件并把一些错误出错信息文本添加到退回邮件中以声明邮件包含病毒。

输出选项的初始化是通过在所需的转换条目中设置 OVERRIDE-OPTION-FILE=1 实现的。此后，输出选项在需要时由脚本设置并存储到环境变量文件 OUTPUT_OPTIONS 中。当脚本完成了对正文部分的处理，转换通道从 OUTPUT_OPTIONS 文件读取选项。

这里的 OUTPUT_OPTION 变量是一个文件名，转换通道即从该文件读取选项。通常它被当作一个随时会消失的临时文件用于传递信息。下面的例子显示脚本使用输出选项给发送病毒的发件人返回的出错讯息。

```
/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
```

在这个例子中，系统诊信息和状态码将被添加到 $OUTPUT_OPTIONS 所定义的文件中。如果读这个 $OUTPUT_OPTIONS 临时文件，将看到类似这样的内容：

```
OUTPUT_DIAGNOSTIC="Virus found and deleted."
STATUS=178029946
```

文本行 OUTPUT_DIAGNOSTIC='Virus found and deleted' 可指示转换通道将文本 Virus found and deleted 添加到邮件中。

178029946 是每个从 server-root/bin/msg/imtasdk/include/pmdf_err.h 找到的 pmdf_err.h 文件的 PMDF__FORCERETURN 状态。这个状态码指示转换通道将邮件退回给发送者。（有关使用专用指令的详细说明，请参阅第 224 页“用转换通道输出退回、删除或保存邮件”。）

完整的输出选项列表如下所示。

表 9-4　　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	在一邮件被转换通道强制退回时，作为发送给发送者邮件一部分的而包含的文本。
OUTPUT_DISPOSITION	输出邮件部分的 MIME content-disposition。
OUTPUT_ENCODING	需在输出邮件部分使用的 MIME 内容传输编码。
OUTPUT_MODE	转换通道用于写输出邮件部分的 MIME 模式，这同时也是收件人读取输出邮件部分所用的模式。
STATUS	转换器的退出状态。这通常是转换通道起动某个操作的专用指令。完整的指令列表位于 server-root/bin/msg/imtasdk/include/pmdf_err.h。

附加在 MESSAGE/RFC822 部分中的报头

在对邮件部分执行转换操作时，转换通道可使用附加的 MESSAGE/RFC822 部分中的标题，如果没有附加 MESSAGE/RFC822 部分，则使用邮件头。标题中的信息对站点提供的程序是有用的。

如果选中的条目有 ORIGINAL-HEADER-FILE=1，则附加的 MESSAGE/RFC822 部分的所有标题行被写入环境变量 OUTPUT_HEADERS 所描述的文件。如果是 OVERRIDE-HEADER-FILE=1，则转换通道将把环境变量 OUTPUT_HEADERS 所描述文件的内容作为该附加部分上的标题而读取和使用。

从转换条目调用映射表

out-parameter-* 值可以在任意命名的映射表中存储和检索。如果客户机对所发送的全部附件使用一个如 att.dat 这样的总名称，而不管它们是否是 postscript、msword、text 或其他任何格式，则上述特性对更改客户机传送来的附件的名称很有用。这是一个重新标注“部分”的基本方法，可使其它客户程序（如 Outlook）能够通过读取扩展名而打开“部分”。

从映射表检索参数值的语法如下：

'mapping-table-name:mapping-input[*$Y,$N*]'

$Y 返回一个参数值。如果没有匹配的值或返回 $N，则忽略转换文件条目中的那个参数，或作为空串处理。缺少匹配值或 $N 并不会导致转换条目自身中止。

考虑下面的映射表：

```
X-ATT-NAMES

   postscript        temp.PS$Y
   wordperfect5.1    temp.WPC$Y
   msword            temp.DOC$Y
```

根据上述映射表转换下列条目可将附件中的指定文件名替换为一般文件名：

```
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'"
```

在上面的例子中，out-chan=tcp_local; in-type=application; in-subtype=* 指定：要处理的邮件必须来自 tcp_local 通道并带有 application/*（* 表示任何子类型都可以）的 content-type 标题。

in-parameter-name-0=name; in-parameter-value-0=* 进一步指定：邮件必须以 name=*（同样，此处的 * 表示任何参数值均可）为其第一参数类型。

out-type=application; 指定：处理后邮件的 MIME Content-type 参数是 application

out-subtype='INPUT-SUBTYPE'; 指定：处理后正文部分的 MIME subtype 参数是环境变量 INPUT-SUBTYPE，此环境变量是输入 subtype 的原值。因此，如果想将

Content-type: application/xxxx; name=foo.doc

改变为

Content-type: application/msword; name=foo.doc

则应使用

out-type=application; out-subtype=msword

out-parameter-name-0=name；指定：输出正文部分的第一 MIME Content-type 参数具有 name= 类型。

out-parameter-value-0='X-ATT-NAMES:\\'INPUT_SUBTYPE\\'';用于指示要提取的第一个 MIME subtype 参数值并搜索映射表 X-ATT-NAMES 以寻找一个 subtype 匹配。如果找到匹配项，name 参数就会接收到一个在 X-ATT-NAMES 映射表中指定的新值。因此，如果参数类型是 msword， name 参数将是 temp.DOC

用转换通道输出退回、删除或保存邮件

本节记述如何使用转换通道选项退回，删除或保存邮件。基本过程如下：

1. 在适当的转换文件条目中设置 OVERRIDE-OPTION-FILE=1。此设置将指示转换通道从 OUTPUT_OPTIONS 文件读取输出选项。
2. 然后用转换脚本确定特定邮件正文部分需要进行何种操作。
3. 在脚本中，通过在 OUTPUT_OPTIONS 文件中写入 STATUS=*directive_code* 选项来指定专用指令。

完整的专用指令列表位于 server_root/bin/msg/imtasdk/include/pmdf_err.h。转换通道经常使用的有：

名字	十六进制值	十进制值
PMDF__FORCEHOLD	0x0A9C86AA	178030250
PMDF__FORCERETURN	0x0A9C857A	178029946
PMDF__FORCEDELETE	0x0A9C8662	178030178

我们将用例子解释这些指令的功能。

退回邮件

要用转换通道退回邮件，在适当的 conversions 文件条目设置 OVERRIDE-OPTION-FILE=1 并在转换脚本中添加下面这一行：

```
echo "STATUS=178029946" >> $OUTPUT_OPTIONS
```

如果希望添加一短文本串到退回邮件中，在转换脚本中添加下面这一行：

```
echo OUTPUT_DIAGNOSTIC= 文本串 >> $OUTPUT_OPTIONS
```

这里的“文本串”类似于："The message sent from your machine contained a virus which has been removed. Be careful about executing email attachments."

有条件地删除邮件部分

依据所包含的内容有条件地删除部分可能是有用的。使用输出选项设置即可做到这一点。相比之下， DELETE=1 转换参数子句则是无条件地删除邮件部分。

若需通过输出选项删除邮件部分，请在适当的转换文件条目中设置 OVERRIDE-OPTION-FILE=1 并在转换脚本中添加下面这一行：

```
echo "STATUS=178030178" >> $OUTPUT_OPTIONS
```

保存邮件

依据所包含的内容有条件地保存部分可能是有用的。要使用输出选项删除一邮件部分，在适当的转换文件条目中设置 OVERRIDE-OPTION-FILE=1 并在转换脚本中添加下面这一行：

```
echo "STATUS=178030250" >> $OUTPUT_OPTIONS
```

这就要求转换通道以转换通道队列中的一个 .HELD 文件的形式保存邮件。

转换通道范例

下面例子中的 CONVERSIONS 映射和转换规则集可使 GIF、 JPEG 和 BITMAP 文件发送到假想通道 tcp_docuprint，然后自动转换为 PostScript。这些转换中有几个使用假想的 /usr/bin/ps-converter.sh 实现转换。其中还包含一附加规则，用于将 WordPerfect 5.1 文件转换为 Microsoft Word 文件。

```
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'"
```

表 9-5　转换参数

参数	说明
限定参数（指定这样的参数：在转换之前必须与邮件匹配。）	
OUT-CHAN, OUT-CHANNEL	输出通道，以匹配转换（允许使用通配符）。此条目指定的转换只有在邮件是发往此指定通道的情况下才执行。
IN-CHAN, IN-CHANNEL	输入通道，以匹配转换（允许使用通配符）。此条目指定的转换只有在邮件是来自此指定通道的情况下才执行。
IN-TYPE	输入 MIME 类型，以匹配转换（允许使用通配符）。指定的转换只有在此字段与正文部分的 MIME 类型相匹配的情况下才执行。
IN-SUBTYPE	输入 MIME 子类型，以匹配转换（允许使用通配符）。此条目指定的转换只有在此字段与正文部分的 MIME 子类型相匹配的情况下才执行。
IN-PARAMETER-NAME-*n*	输入必须与转换相匹配的 MIME Content-Type 参数名；*n* = 0, 1, 2.... 这个参数可与 IN-PARAMETER-VALUE-*n* 一起使用以便通过其名称和所具有的值明确识别一个参数。
IN-PARAMETER-VALUE-*n*	输入必须与转换相匹配的对应于 IN-PARAMETER-NAME 的 MIME Content-Type 参数值。此条目指定的转换只有在此字段与正文部分的 Content-Type 参数列表中的对应参数相匹配的情况下才被执行。允许使用通配符。
IN-PARAMETER-DEFAULT-*n*	在没有提供参数情况下输入 MIME Content-Type 默认参数值。当正文部分没有指定这样的参数时，这个值被当作默认值用于 IN-PARAMETER-VALUE-*n* 测试。

表 9-5　转换参数 （接上页）

参数	说明
IN-DISPOSITION	输入 MIME Content-Disposition 以匹配转换。
IN-DPARAMETER-NAME-*n*	输入必须与转换相匹配的 MIME Content-Disposition 参数名； *n* = 0, 1, 2.... 这个参数可与 IN-DPARAMETER-VALUE-*n* 一起使用，以便通过其名称和所具有的值明确识别一个参数。
IN-DPARAMETER-VALUE-*n*	输入必须与转换相匹配的对应于 IN-PARAMETER-NAME 的 MIME Content-Disposition 参数值。通过此条目指定的转换只有在此字段与正文部分的 Content-Disposition: 参数列表中的对应参数相匹配的情况下才被执行。允许使用通配符。
IN-DPARAMETER-DEFAULT-*n*	在没有提供参数情况下输入 MIME Content-Disposition 默认参数值。当正文部分没有指定这样的参数时，这个值被当作默认值用于 IN-DPARAMETER-VALUE-*n* 测试。
IN-DESCRIPTION	输入 MIME Content-Description 以匹配转换。
IN-SUBJECT	输入来自 MESSAGE/RFC822 部分的主题。
输出参数 （用于指定正文部分转换后的输出设置。）	
OUT-TYPE	如果与输入类型不同则输出 MIME 类型。
OUT-SUBTYPE	如果与输入类型不同则输出 MIME 子类型。
OUT-PARAMETER-NAME-*n*	输出 MIME Content-Type 参数名； *n* = 0, 1, 2...
OUT-PARAMETER-VALUE-*n*	输出对应于 OUT-PARAMETER-NAME-*n* 的 MIME Content-Type 参数值。
PARAMETER-COPY-*n*	一个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 参数的列表； *n*=0, 1, 2... 使用与 MIME 参数相同的名字去复制，如 IN-PARAMETER-NAME-*n* 子句所匹配的那样。
OUT-DISPOSITION	如果与输入 MIME Content-Disposition 不同，就输出 MIME Content-Disposition。
OUT-DPARAMETER-NAME-*n*	输出 MIME Content-Disposition 参数名； *n*=0, 1, 2...
OUT-DPARAMETER-VALUE-*n*	输出对应于 OUT-DPARAMETER-NAME-*n* 的 MIME Content-Disposition 参数值。
DPARAMETER-COPY-*n*	一个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: 参数的列表。 *n* = 0, 1, 2,... 取要复制的 MIME 参数的名称作为参数，如 IN-PARAMETER-NAME-*n* 子句所匹配的那样。在参数中可以使用通配符。特别是，参数 * 意味着复制全部原始 Content-Disposition: 参数。
OUT-DESCRIPTION	如果与输入 MIME Content-Description 不同，就输出 MIME Content-Description。
OUT-MODE	读取和存储已转换文件的模式。这应是 BLOCK （二进制文件和可执行文件）或 TEXT。

表 9-5　转换参数 （接上页）

参数	说明
OUT-ENCODING	在邮件重新装配时应用于转换文件的编码。
操作参数 （指定一个针对邮件部分的操作。）	
COMMAND	实施转换而执行的命令。实施转换而执行的命令。这个参数是必须的；如果没有指定命令，此条目被忽略。
DELETE	0 或 1。如果设置了这个标志，则删除邮件部分。（如果这是邮件中唯一的部分，则被一个空的文本部分取代。）
RELABEL	RELABEL=1 将按输出参数的指定重新标注 MIME 标签。Relabel=0 则什么都不做。通常对错误标注的部分进行重新标注 （例如：从 Content-type:application/octet-stream 到 Content-type:application/msword）于是用户可以通过 “双击”打开一个部分，而不必将此部分保存到一个文件并用一个程序打开它。
SERVICE-COMMAND	SERVICE-COMMAND=command 将执行一个站点提供的作用于整个 MIME 邮件（MIME 标题和内容正文部分）的程序。同样，与其他 CHARSET-CONVERSION 操作或转换通道操作不同的是，服务命令需由自己完成 MIME 分解、解码、重编码和重新组装。请注意，这个标志在转换通道处理时导致一个条目被忽略，而 SERVICE-COMMAND 条目却在字符集转换处理时被执行。
TAG	输入标记，由邮件列表 CONVERSION_TAG 参数设置。
信息传递参数 （用于与站点提供的程序之间传递信息。）	
DPARAMETER-SYMBOL-*n*	用于存储 Content-disposition 参数值（如果已提供）的环境变量； *n* = 0, 1, 2,... 每个 DPARAMETER-SYMBOL-*n* 顺序取自 Content-Disposition: 参数列表 （n=0 是第一个参数， n=2 是第二个参数，等等。）并在执行站点提供的程序之前放置在指定的环境变量中。
PARAMETER-SYMBOL-*n*	用于存储 Content- Type 参数值 （如果已提供）的环境变量； *n* = 0, 1, 2... 每个 PARAMETER-SYMBOL-*n* 顺序取自 Content-Type: 参数列表 （n=0 是第一个参数， n=2 是第二个参数，等等。）并在执行站点提供的程序之前放置在同名的环境变量中。取存放 MIME 参数转换结果的变量名作为参数，如 IN-PARAMETER-NAME-*n* 子句所匹配的那样。
MESSAGE-HEADER-FILE	将一邮件的所有部分，或除原始标题意外的部分，写入到环境变量 MESSAGE_HEADERS 所指定的文件中。如果设置为 1，直接附加正文部分的原始标题被写入到环境变量 MESSAGE_HEADERS 所指定的文件中。如果设置为 2，作为邮件的原始标题作为整体 （最外层的邮件标题）被写入到文件。
ORIGINAL-HEADER-FILE	0 或 1。如果设置为 1，附加 MESSAGE/RFC822 部分 （不仅是正文部分）的原始标题被写入到环境变量 OUTPUT_HEADERS 描述的文件中。
OVERRIDE-HEADER-FILE	0 或 1。如果设置为 1，则 MIME 标题行通过转换通道从环境变量 OUTPUT_HEADERS 中读取，优先于在附加 MIME 部分中的原始标题行。
OVERRIDE-OPTION-FILE	如果 OVERRIDE-OPTION-FILE=1，转换通道从环境变量 OUTPUT_OPTIONS 中读取选项。
PART-NUMBER	用点分隔的整数：*a. b. c*...MIME 正文部分的部分号。

字符集转换和邮件重格式化

字符集转换表是 Messaging Server 中最为基础的映射表。该表的名为 CHARSET-CONVERSION。它用于指定可以做哪种类型的通道对通道的字符集转换和邮件重格式化。

在许多系统中没有必要进行字符集转换或邮件重格式化，因此也不需要此表。但，某些情况下必须进行字符集转换。

CHARSET-CONVERSION 映射表也能够用于改变邮件的格式。系统提供了将很多非 MIME 格式转换为 MIME 格式的功能。也可以修改 MIME 的编码和结构。当邮件被传递到只支持 MIME 或 MIME 的某个子集的系统时，须使用这些选项。最后，只提供了少数几种从 MIME 到非 MIME 格式的转换。

MTA 用两种不同的方式查找 CHARSET-CONVERSION 映射表。第一种方式的查找用来确定 MTA 是否应该重格式化邮件，若是，应使用什么样的格式化选项。（如果没有指定重格式化，MTA 就无需检查指定的字符集转化了。）第一种查找方式下输入字符串的一般形式为：

IN-CHAN=*in-channel*;OUT-CHAN=*out-channel*;CONVERT

这里的 *in-channel* 为源通道（邮件即来源于该处）的名字，*out-channel* 为目标通道（邮件即去往该处）的名字。如果发现相匹配的项，结果字符串为用逗号分开的关键字列表。表 9-6 列出了这些关键字。

表 9-6　CHARSET-CONVERSION 映射表关键字

关键字	说明
Always	强制转换，即使邮件在去往 *out-channel* 之前要通过转换通道。
Appledouble	将其他 MacMIME 格式转换为 Appledouble 格式。
Applesingle	将其他 MacMIME 格式转换为 Applesingle 格式。
BASE64	将 MIME 编码切换为 BASE64。
Binhex	将其他 MacMIME 格式或包含 Macintosh 类型和 Mac 创建者信息的部分转换为 Binhex 格式。
Block	从 MacMIME 格式部分只抽取数据分支。
Bottom	将任意的 message/rfc822 正文部分 （已转发邮件）转换为邮件的内容部分和标题部分。
Delete	将任意的 message/rfc822 正文部分 （已转发邮件）转换为一个邮件的内容部分，并删除已转发的标题。
Level	删除邮件的多部分级别。
Macbinary	将其他 MacMIME 格式或包含 Macintosh 类型和 Macintosh 创建者信息的部分转换为 Macbinary 格式。
No	禁用转换。
QUOTED-PRINTABLE	将 MIME 编码切换为 QUOTED-PRINTABLE。

表 9-6　CHARSET-CONVERSION 映射表关键字（接上页）

关键字	说明
`Record,Text`	文本 / 无格式部分在 80 个字符处换行。
`Record,Text= n`	文本 / 无格式部分在 n 个字符处换行。
`RFC1154`	将邮件转换为 RFC 1154 格式
`Top`	将任意的 message/rfc822 正文部分 （已转发邮件）转换为标题部分和邮件内容部分。
`UUENCODE`	将 MIME 编码切换为 X-UUENCODE。
`Yes`	启用转换。

字符集转换

如果 MTA 查找并发现到邮件要被重格式化，它将进一步检查邮件的每一部分。要查找所有文本部分，它们的字符集参数要用于第二步查找。只有当 MTA 已经核实并发现需要做转换时才执行第二步查找。第二步查找的输入字符串的形式如下所示：

`IN-CHAN=`*in-channel*`;OUT-CHAN=`*out-channel* ； `IN-CHARSET=`*in-char-set*

这里的 *in-channel* 和 *out-channel* 和以前的含义一样， *in-char-set* 为与问题中特定部分相关联的字符集的名字。如果第二次查找没有发现匹配项，不执行任何字符集转换 （尽管有可能根据第一次查找中匹配的关键字对邮件进行重格式化，例如修改 MIME 结构）。如果有匹配项，将产生如下形式的字符串：

`OUT-CHARSET=`*out-char-set*

这里的 *out-char-set* 指定 `in-char-set` 要被转换成的哪个字符集的名字。注意，这两个字符集都必须在字符集定义表 `charsets.txt` 中定义，该表位于 MTA 表目录中。如果没有在此文件中正确定义字符集，则不进行任何转换。这通常不会成为问题，因为此文件定义了几百个字符集，大多数今天常用的字符集在此文件中都已定义。要得到 `charsets.txt` 文件更进一步的信息，请参阅有关实用程序 `imsimta chbuild`（UNIX 和 NT）的说明。

如果符合所有的条件，MTA 将着手构建字符集映射表并进行转换。被转换的邮件部分将使用转换后的字符集名字重新标注。

邮件重格式化

如前所述， `CHARSET-CONVERSION` 映射表也用于影响附件在 MIME 和几个专有邮件格式之间的转换。

下面给出一些其他种类的邮件重格式化例子， `CHARSET-CONVERSION` 映射表能够影响这些重格式化。

Non-MIME Binary 附件转换

某种非标准（non-MIME）格式邮件，例如某种专有格式的邮件或来自 Microsoft Mail（MSMAIL）SMTP 网关的邮件，当处理这些邮件所涉及到的任何通道都启用 CHARSET-CONVERSION 时，将自动转换为 MIME 格式。如果有一个 tcp_local 通道，则它通常是来自 Microsoft Mail SMTP 网关的邮件的接收通道，以下设置将对传递给本地用户的邮件启用转换功能：

```
CHARSET-CONVERSION

   IN-CHAN=tcp_local;OUT-CHAN=ims-ms;CONVERT          Yes
```

也可换一种方法，即简单地指定 OUT-CHAN=* 来代替 OUT-CHAN=ims-ms 以覆盖每一个通道。但这样做可能为导致邮件处理的额外开销，因为这样做须详细检查所有进入 tcp_local 通道的邮件，而不仅仅局限于那些绑定到特定通道的邮件。

更为重要的是，如此不加区分的转换可能将系统置于难以驾御邮件转换的地步。因为邮件不一定都是自己站点的，有些邮件只是简单地通过系统而已，此时系统仅需起着传输工具的作用就可以了，除了邮件信封和相关传输信息之外没有必要对邮件做任何改变。

要将 MIME 转换为 Microsoft Mail SMTP 网关识别的格式，应在 MTA 配置中为 Microsoft Mail SMTP 网关使用单独的通道，例如 tcp_msmail，并且将以下内容放到映射表文件中：

```
CHARSET-CONVERSION

   IN-CHAN=*;OUT-CHAN=tcp_msmail;CONVERT         RFC1154
```

重标注 MIME 标题

某些用户代理或网关可能发出带有 MIME 标题的邮件，这种标题所包含信息不像它应该包含的那样多，但也足够用来构建更为精细的 MIME 标题。尽管最好的解决方法是对这些用户代理或网关进行正确地配置，但如果不能控制这些用户代理和网关，也可转而请求 MTA 尝试重新构建更为有用的 MIME 标题。

如果第一次查找 CHARSET-CONVERSION 映射表时产生的关键字为 Yes 或 Always，那么 MTA 将核实是否有一个 conversions 文件存在。如果有 conversions 文件，MTA 即在文件中查找 RELABEL=1 的条目，若找到此条目， MTA 将执行条目中指定的任何 MIME 重标注。

例如，如下所示的 CHARSET-CONVERSION 表和 MTA conversions 文件条目的组合将导致一些邮件被重标注：那些到达 tcp_local 通道并且路由到 ims-ms 通道的邮件将重标注为 application/postscript；那些到达时原先的 MIME 标注为 application/octet-stream，但具有扩展名 ps 或 msw 的文件名参数的邮件将重标注为 application/msword。（注意，更为精确的标注应由最初用户代理或网关自己执行。）

字符集转换表

```
CHARSET-CONVERSION

   IN-CHAN=tcp_local;OUT-CHAN=mr_local;CONVERT            Yes
```

MTA 转换文件条目

```
out-chan=ims-ms; in-type=application; in-subtype=octet-stream;
  in-parameter-name-0=name; in-parameter-value-0=*.ps;
  out-type=application; out-subtype=postscript;
     parameter-copy-0=*; relabel=1

out-chan=ims-ms; in-type=application; in-subtype=octet-stream;
  in-parameter-name-0=name; in-parameter-value-0=*.msw;
  out-type=application; out-subtype=msword;
     parameter-copy-0=* relabel=1
```

MacMIME 格式转换

Macintosh 文件有两部分，资源分支包含 Macintosh 的特定信息，数据分支包含可在其他平台上使用的数据。这为传输 Macintosh 文件带来额外的复杂性，因为传输 Macintosh 文件各个部分时通常要使用 4 种不同的格式。这些格式种的三种，Applesingle、Binhex 和 Macbinary 将 Macintosh 资源分支和 Macintosh 数据分支合并编码在一起。第四种格式，Appledouble，是一种多部分格式，资源分支和数据分支位于相互独立的部分中。因此 Appledouble 成为非 Macintosh 平台上最为有用的格式，这种格式能够忽略资源分支，而数据分支则则为非 Macintosh 应用程序所利用。当在特地向 Macintoshes 发送时其他格式可能很有用。

MTA 能够在这些不同 Macintosh 格式间进行转换。`CHARSET-CONVERSION` 的关键字 `Appledouble`、`Applesingle`、`Binhex` 或 `Macbinary` 通知 MTA 分别将其他 MacMIME 结构部分转换为 multipart/appledouble、application/applefile、application/mac-binhex40 或 application/macbinary 的 MIME 结构。更进一步，关键字 `Binhex` 或 `Macbinary` 也请求转换为非 MacMIME 格式部分的指定格式，虽然 `X-MAC-TYPE` 和 `X-MAC-CREATOR` 参数包含于 MIME Content-type: 标题中。`CHARSET-CONVERSION` 的关键字 `Block` 通知 MTA 从 MacMIME 格式部分只提取数据分支，放弃资源分支；（这样做丢失信息，使用 `Appledouble` 进行替代通常更为合适）。

例如，以下 CHARSET-CONVERSION 表将通知 MTA 在向 ims-ms 通道传递时转换成 Appledouble 格式。

```
CHARSET-CONVERSION

  IN-CHAN=*;OUT-CHAN=l;CONVERT            Appledouble
```

向 Appledouble 格式的转换只应用于已经是一种 MacMIME 格式的部分。

当向 Appledouble 或 Block 格式转换时，MAC-TO-MIME-CONTENT-TYPES 映射表用于表明在 Appledouble 部分或 Block 部分数据分支上的标注什么指定的 MIME 标签取决于原始 Macintosh 文件中 Macintosh 创建者和 Macintosh 类型信息。查找此表采用的形式为 format|type|creator|filename，这里的 format 是 SINGLE、BINHEX 或 MACBINARY 中的一种，type 和 creator 分别为十六位进制的 Macintosh 类型和 Macintosh 创建者信息，filename 为文件名。

例如，要在向 ims-ms 通道发送邮件时转换为 Appledouble，且进行转换时对从 MACBINARY 或 BINHEX 部分转换来的任意的 MS Word 或 PostScript 文档使用指定的 MIME 标签，则适当的表应为：

```
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
```

注意，映射表条目模板（右侧）必须设有 $Y 标志，以便指定要执行的标注。在 MTA 表目录的 mac_mappings.sample 文件中可以找到更多附件类型的样例条目。

如果希望将非 MacMIME 格式部分转换为 Binhex 或 Macbinary 格式，这些部分需要为 X-MAC-TYPE 和 X-MAC-CREATOR MIME Content-type:parameter 提供值。注意，MIME 的重标注能够用来在这些部件上强制生成别的方式不会有的参数。

服务转换

MTA 转换服务功能可用于用站点提供的过程来处理邮件以产生一新形式的邮件。既不同于上面讨论的 CHARSET-CONVERSION 操作种类，也不同于对单个 MIME 邮件部分的内容进行操作的 conversion 通道，转换服务对整个 MIME 邮件部分 （MIME 标题和内容）以及整个 MIME 邮件进行操作。同样，与其他 CHARSET-CONVERSION 操作或转换通道操作不同，转换服务由自己完成 MIME 分解、解码、重编码和重新组装。

类似于其他 CHARSET-CONVERSION 操作，转换服务通过 CHARSET-CONVERSION 映射表被启用。如果第一次查找 CHARSET-CONVESION 映射表产生一 Yes 或 Always 关键字，那么 MTA 将核实 MTA conversions 文件的存在。如果 conversions 文件存在， MTA 将在文件中查找指定 SERVICE-COMMAND 的条目，发现该条目，则执行该条目。 conversions 文件条目应有如下形式：

```
in-chan=channel-pattern;
  in-type=type-pattern; in-subtype=subtype-pattern;
  service-command=command
```

请注意 command 字符串。它是一个应被执行以实施服务转换（例如，调用文档转换器）的命令。该命令必须处理一输入文件，其中包含需要得到服务的邮件文本，并作为输出生成一个包含新邮件文本的文件。在 UNIX 系统中，如果命令成功，退出时必须返回 0，否则返回非 0 值。

环境变量用于传递输入和输出文件的名字，同样也可用来传递包含邮件信封收件人地址列表的文件的名字。这些环境变量的名字是：

- INPUT_FILE - 要处理的输入文件的名称
- OUTPUT_FILE - 要处理的输出文件的名称
- INFO_FILE - 包含信封收件人地址的文件的名称

这三个环境变量的值可能使用标准命令行代入法代入到命令行中：也就是说，在 UNIX 变量名字之前加上美元符号。

第 10 篇

邮件过滤与访问控制

本章介绍邮件服务的访问控制方法以及通过映射表和服务器端规则（SSR）过滤邮件的方法。

有时您可能需要在系统级上拒收发自（或发至）某些用户的邮件，或在某些用户之间设定较复杂的信量限制条件，或准许用户为其各自的来件设置过滤器（包括根据邮件头内容拒收邮件）。

如果需要在信封级上进行控制，则可用映射表过滤邮件。如果需要使用基于邮件头的控制，或如果用户希望实现他们各自的个人化控制，则可采用较一般的邮件过滤方法，服务器端规则在此种情况下较为适切。

本章共分两个部分：

第一部分：映射表

第二部分：邮箱过滤器

第一部分：映射表

第一部分包括下列章节：

- 用映射表控制访问
- 实施访问控制的时机
- 测试访问控制映射
- 添加 SMTP 转发
- 配置 SMTP 转发阻塞
- 处理大量访问条目
- 访问控制映射表标志

用映射表控制访问

您可通过配置映射表对用户访问邮件服务实行控制。您可用映射表控制哪些用户能或不能发送邮件、接收邮件或收发兼而有之 （表 10-1） 。有关映射文件格式和使用的一般信息，请参见 **iPlanet Messaging Server Reference Manual**。

表 10-1 列示了本节描述的映射表。

表 10-1　访问控制映射表

映射表	说明
SEND_ACCESS （参见 236。）	用于以信封 From 地址，信封 To 地址，源通道和目标通道为根据，阻塞入站连接。在完成了重写、别名扩展等操作后，系统将对 To 地址加以核实。
ORIG_SEND_ACCESS （见 236。）	用于以信封 From 地址，信封 To 地址，源通道和目标通道为根据，阻塞入站连接。在完成了重写后但在别名扩展操作前，系统将对 To 地址加以核实。
MAIL_ACCESS （见 238。）	用于阻塞入站连接，所用根据是在 SEND_ACCESS 和 PORT_ACCESS 表中找到的综合信息：即 SEND_ACCESS 表中找到的通道和地址信息与 PORT_ACCESS 表中找到的 IP 地址和端口号信息的结合体。
ORIG_MAIL_ACCESS （见 238。）	用于阻塞进入的连接，所用根据是在 ORIG_SEND_ACCESS 和 PORT_ACCESS 表中找到的综合信息：即 ORIG_SEND_ACCESS 表中找到的通道和地址信息与 PORT_ACCESS 表中找到的 IP 地址和端口号信息的结合体。
FROM_ACCESS （见 239。）	用于根据信封 From 地址过滤邮件。如果 To 地址不相关，可使用此表。
PORT_ACCESS （见 241。）	可根据 IP 号阻塞外来的连接。

MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射是最通用者，不仅能提供可用于 SEND_ACCESS 和 ORIG_SEND_ACCESS 的地址和通道信息，而且还能提供任何可通过 PORT_ACCESS 映射表而使用的信息，其中包括 IP 地址和端口号信息。

SEND_ACCESS 和 ORIG_SEND_ACCESS 表

您可用 SEND_ACCESS 和 ORIG_SEND_ACCESS 映射表控制谁能或不能发送邮件、接收邮件或收发兼而有之。访问检查可确认邮件的信封 From 地址和信封 To 地址是可用的，并知晓邮件从何通道进入以及准备从何通道的发出。

如果 SEND_ACCESS 或 ORIG_SEND_ACCESS 映射表存在，MTA 则对通过 MTA 的每封邮件的每一收件人用下列格式的字符串在表中扫描 （请注意使用的竖杠字符 |）：

src-channel|*from-address*|*dst-channel*|*to-address*

src-channel 是排列该邮件的通道； *from-address* 是发件人的地址； *dst-channel* 是邮件将被列于其中队列的通道； *to-address* 是邮件的收件人地址。如果在这四个字段中的任何一个字段中输入一个星号，则可使该字段与任何适当的通道或地址相匹配。

这里的地址指信封地址；也就是信封 From 地址和信封 To 地址。对于 SEND_ACCESS，信封 To 地址是在重写、别名扩展等操作完成后才予以检查；而对于 ORIG_SEND_ACCESS，原先指定的信封 To 地址是在重写后，但在别名扩展前予以检查。

如果搜索字符串与某一模式相匹配（即表中项目左侧者），系统则对随后生成的映射输出进行检查。如果输出包括 $Y 或 $y 标志，那么针对该特定的收件人地址的入队是允许的。如果输出含任何 $N、$n、$F 或 $f 标志，则拒绝该特定地址入队。在出现被拒绝的情况时，系统可在映射输出中提供一则任选讯息，以说明被拒原因。该字符串将包括在 MTA 发出的拒收错误讯息之中。如果输出中没有字符串 （$N、 $n、 $F 或 $f 标志以外的），系统将使用默认的拒收讯息。有关其它标志的说明，请见第 254 页 “访问控制映射表标志”。

在下面的范例中，从 mail、Pine 等 UNIX 用户代理程序发送的邮件来自本地通道 `l`，通往互联网的邮件须经由某种 TCP/IP 通道送出。假定您不准许本地用户 （postmaster 除外）向互联网发送邮件，但可以从互联网接收邮件。那么可以实行这一限制规定的方法是通过如图 10-1 中所示的 SEND_ACCESS 映射表。在映射表中，本地主机名被假定为 `sesta.com`。在通道名 “`tcp_*`” 中则使用通配符，以便与任何可能的 TCP/IP 通道名匹配（例如，`tcp_local`）。

在拒收讯息中，系统使用了美元符号摘引该则讯息中的空格。没有这些美元符号，拒收将会过早停止并且只显示 “Internet” 而不是 “Internet postings are not permitted” 。注意，本例忽略其他可能的 “本地” 邮件传送源，比如来自基于 PC 的邮件系统，或者来自 POP 或 IMAP 客户机。

图 10-1 SEND_ACCESS 映射表

```
SEND_ACCESS

  *|postmaster@sesta.com|*|*     $Y
  *|*|*|postmaster@sesta.com     $Y
  l|*@sesta.com|tcp_*|*          $NInternet$ postings$ are$ not$ \
    permitted
```

备注 试图发送邮件的客户机可决定是否向企图发送该邮件的用户显示 MTA 拒收错误讯息。如果 SEND_ACCESS 被用来拒收来自 SMTP 的邮件， MTA 则只发出一组 SMTP 拒收代码，其中包括可选用的拒收讯息；此后便由负责发送邮件的 SMTP 客户机用该信息组成一则退回讯息并将其回送给原发件人。

MAIL_ACCESS 和 ORIG_MAIL_ACCESS 映射表

MAIL_ACCESS 映射表是 SEND_ACCESS 和 PORT_ACCESS 两个映射表的超集。它综合了 SEND_ACCESS 的通道和地址信息以及 PORT_ACCESS 的 IP 地址和端口号信息。与之相类似的是，ORIG_MAIL_ACCESS 映射表是 ORIG_SEND_ACCESS 和 PORT_ACCESS 两个映射表的超集。MAIL_ACCESS 的探查字符串格式为：

port-access-probe-info|*app-info*|*submit-type*|*send_access-probe-info*

ORIG_MAIL_ACCESS 的探查字符串格式与之类似，即：

port-access-probe-info|*app-info*|*submit-type*|*orig_send_access-probe-info*

此处的 *port-access-probe-info* 中，包含有在 SMTP 来电情况下通常于 PORT_ACCESS 映射表探查项中包括的所有信息，否则是空的。在通过 SMTP 提交邮件的情况下，*app-info* 通常为 SMTP，否则是空的。*submit-type* 可为 MAIL、SEND、SAML 或 SOML 中的任何一项，与邮件被提交到 Messaging Server 的方法相一致。该值通常为 MAIL，表示是以邮件形式提交的；在有向 SMTP 服务器提交广播请求（或综合广播 / 邮件请求）的情况下，则会出现 SEND、SAML 或 SOML。至于 MAIL_ACCESS 映射，*send-access-probe-info* 中包含有 SEND_ACCESS 映射表探查项中通常包括的所有信息。ORIG_MAIL_ACCESS 映射与之类似，*orig-send-access-probe-info* 中包含有 ORIG_SEND_ACCESS 映射表探查项中通常包括的所有信息。

使进入的 TCP/IP 连接信息在与通道和地址信息相同的映射表中可用，这会方便实施某些类型的控制，比如强制允许信封发件人地址出现在来自特定 IP 地址在邮件中。这可以限制伪造电子邮件，或者鼓励用户适当的配置他们的 POP 和 IMAP 客户机的发件人地址。例如，一个站点希望只允许信封发件人地址 vip@siroe.com 出现在来自于 IP 地址 1.2.3.1 和 1.2.3.2 的邮件中，并保证来自 1.2.0.0 子网络的任何系统的邮件中的信封发件人地址都来自于 siroe.com，该站点可能使用 MAIL_ACCESS 映射表，如图 10-2 所示。

图 10-2 MAIL_ACCESS 映射表

```
MAIL_ACCESS

  ! Entries for vip's two systems
  !
  TCP|*|25|1.2.3.1|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|*  $Y
  TCP|*|25|1.2.3.2|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|*  $Y
  !
  ! Disallow attempts to use vip's From: address from other
  ! systems
  !
  TCP|*|25|*|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|*  \
      $N500$ Not$ authorized$ to$ use$ this$ From:$ address
  !
  ! Allow sending from within our subnet with siroe.com From:
  ! addresses
  !
  TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*|*@siroe.com|*|*  $Y
  !
  ! Allow notifications through
  !
  TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*||*|*  $Y
  !
  ! Block sending from within our subnet with non-siroe.com
  ! addresses
  !
  TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*|*|*|*  \
      $NOnly$ siroe.com$ From:$ addresses$ authorized
```

FROM_ACCESS 映射表

FROM_ACCESS 映射表可能用于控制哪些人可以发送邮件，或者用已认证的地址覆盖虚设的发件人地址，或者同时实现这两种功能。

用于 FROM_ACCESS 映射表的输入探查字符串与 MAIL_ACCESS 映射表类似，但没有目标通道和地址，增加的部分有经验证的发件人信息（如果有的话）。因此，如果 FROM_ACCESS 映射表存在， Messaging Server 则用下列格式的字符串对每一邮件提交企图在表中进行搜索（请注意使用的竖杠字符 |）：

port-access-probe-info|*app-info*|*submit-type*|*src-channel*|*from-address*|*auth-from*

此处的 *port-access-probe-info* 中，包含有在 SMTP 来电情况下通常于 PORT_ACCESS 映射表探查项中包括的所有信息，否则是空的。在通过 SMTP 提交邮件的情况下， *app-info* 通常为 SMTP，否则是空的。*submit-type* 可为 MAIL、SEND、SAML 或 SOML 中的任何一项，与邮件被提交到 MTA 的方法相一致。该值通常为 MAIL，表示是以邮件形式提交的；在有向 SMTP 服务器提交广播请求 （或综合广播 / 邮件请求）的情况下，则会出现 SEND、SAML 或 SOML。 *src-channel* 是原发邮件使用的通道 （即排列邮件的通道）； *from-address* 是邮件所指的发件人地址； *auth-from* 是经验证的发件人地址 （如果可获得该信息的话），如果没有经认证的信息则为空白。

如果搜索字符串与某一模式相匹配（即表中项目左侧者），系统则对随后生成的映射输出进行检查。如果输出包括 $Y 或 $y 标志，那么针对该特定的收件人地址的入队是允许的。如果输出含任何 $N、$n、$F 或 $f 标志，则拒绝该特定地址入队。在出现被拒绝的情况时，系统可在映射输出中提供一则任选讯息，以说明被拒原因。该字符串将包括在 Messaging Server 发出的拒收错误讯息之中。如果输出中没有字符串 （$N、$n、$F 或 $f 标志以外的），系统将使用默认的拒收讯息。有关其它标志的说明，请见第 254 页 “访问控制映射表标志”。

除了可以根据发件方决定是否允许提交邮件以外，FROM_ACCESS 还可以通过 $J 标志来改变信封发件人地址，或者通过 $K 标志修改 authrewrite 通道关键字的效果（在接受的邮件中添加发件人标题地址）。例如，这个映射表可用来使已认证的地址代替原信封发件人地址：

```
FROM_ACCESS

  *|SMTP|*|tcp_local|*|        $Y
  *|SMTP|*|tcp_local|*|*       $Y$J$3
```

在使用 FROM_ACCESS 映射表修改使用效果，以使 authrewrite 在某些源通道上设置为非零值时，如果经认证的地址将逐字引用，则无需使用 FROM_ACCESS。

例如，当在 tcp_local 通道上设置了 authrewrite 2 后，便无需使用下列 FROM_ACCESS 映射表，因为 authrewrite 本身就足以取得这一效果 （逐字添加经认证的地址）：

```
FROM_ACCESS

  *|SMTP|*|tcp_local|*|      $Y
  *|SMTP|*|tcp_local|*|*     $Y$K$3
```

然而，正如图 10-3 所示， FROM_ACCESS 的真正目的是允许您进行更复杂、更细微的改动。如果要将 From 标题行（显示 SMTP AUTH 已认证的提交人地址）添加到进入的邮件，只需 authrewrite 关键字就可以了。然而，假设只有在 SMTP AUTH 已认证提交人的地址与信封发件人地址不一致时，才要强制添加一个发件人标题行到进入的邮件中 （也即，如果地址一致就不必费心添加发送人标题行了），进一步假设希望 SMTP AUTH 和信封发件人地址不会仅仅因为信封发件人包含了可选的子地址信息就被认为不一致。

图 10-3 FROM_ACCESS 映射表

```
FROM_ACCESS

  ! If no authenticated address is available, do nothing
  *|SMTP|*|tcp_local|*|              $Y
  ! If authenticated address matches envelope From:, do nothing
  *|SMTP|*|tcp_local|*|$2*           $Y
  ! If authenticated address matches envelope From: sans
  ! subaddress, do nothing
  *|SMTP|*|tcp_local|*+*@*|$2*@$4*    $Y
  ! Fall though to...
  ! ...authenticated address present, but didn't match, so force
  ! Sender: header
  *|SMTP|*|tcp_local|*|*              $Y$K$3
```

PORT_ACCESS 映射表

Dispatcher 能够根据 IP 地址和端口号，有选择地接受或拒绝外来连接。当 Dispatcher 启动时，Dispatcher 将寻找一个名为 PORT_ACCESS 的映射表。如果该表存在，Dispatcher 将按下列格式对连接信息进行格式化处理：

TCP | *server-address* | *server-port* | *client-address* | *client-port*

Dispatcher 将针对所有 PORT_ACCESS 映射表项进行匹配。如果映射结果中包含 $N 或 $F，该连接就此被关闭。若有任何其它映射结果，则表明该连接将被接受。 $N 或 $F 后面可随附一则拒收讯息（选项）。如果有的话，该邮件将在关闭前顺连接被送回。请注意，在顺连接被送回前，字符串上将附加一个 CRLF 终止符。

如果映射探查项相匹配，则后面附有可选字符串的 $< 标志将指示 Messaging Server 把该字符串发至系统日志（UNIX）或事件日志（NT）。如果访问被拒，后面附有可选字符串的 $> 标志亦将指示 Messaging Server 把该字符串发至系统日志（UNIX）或事件日志（NT）。如果 LOG_CONNECTION MTA 选项的位 1 已设置，而且 $N 标志亦经设置以拒绝连接，则再指定 $T 标志将致使 “T” 项被写入连接日志。如果 LOG_CONNECTION MTA 选项的位 4 已设置，由网站提供的文字部分则可能已在 PORT_ACCESS 表项中提供，以将其包括在 “C” 项连接日志表项之中。若需指定此类文字，可在该表项右侧输入两个竖杠字符，表 10-2 然后即可在后面输入所需的文字。

表 10-2　PORT_ACCESS 映射标志

标志	说明
$Y	允许访问。
带参数的标志，以参数读取顺序 +	
$< *字符串*	如果探查项相匹配，则将字符串发送至系统日志 （UNIX）或事件日志 （NT）。
$> *字符串*	如果访问被拒，则将字符串发送至系统日志 （UNIX）或事件日志 （NT）。
$N *字符串*	以供选用的错误文字字符串拒绝访问
$F *字符串*	$N 字符串的同义词；即以供选用的错误文字字符串拒绝访问
$T *文本*	如果 LOG_CONNECTION MTA 选项的位 1 已设置，而且 $N 标志亦经设置以拒绝连接， $T 将致使 “T” 项被写入连接日志；供选用的文字 （须在两条竖杠字符后显示）可能已包括在连接日志表项之中。
+ 使用带参数的多重标志时，请用竖杠字符	将参数隔开，并按照表中所列顺序放置参数。

例如，下列映射将只接受来自单一网络的 SMTP 连接（至端口 25 者，正常 SMTP 端口），被选出予以拒绝连接且不提供解释文字的特定主机除外：

```
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，在对 PORT_ACCESS 映射表做了任何更改后，您都须重新启动 Dispatcher，以使 Dispatcher 看到所做变更。（如果使用的是经过编译的 MTA 配置，则须先重新编译您的配置，以将变更情况纳入编译配置。）

PORT_ACCESS 是专门用于执行基于 IP 拒收任务的映射表。对于在电子邮件地址级上进行的较通用的控制，最好使用 SEND_ACCESS 或 MAIL_ACCESS 映射表。

限制指定的 IP 地址到 MTA 的连接

使用端口访问映射表中的共享库 conn_throttle.so 可以限制特定的 IP 地址与 MTA 连接的频度。对特定 IP 地址的连接限制对于防止在拒绝服务攻击中的过渡连接是十分有用的。

conn_throttle.so 是一个在 PORT_ACCESS 映射表中用来限制特定 IP 地址与 MTA 过多连接的的共享库。所有配置选项均被指定为连接节流共享库的参数，如下所示：

$[*server_root*/lib/conn_throttle.so， throttle,IP-address,max-rate]

IP-address 是远程系统的点分隔十进制地址。max-rate 是 IP 地址作为强制最高频率的每分钟连接数。

对于例程的惩罚版本，例程名 throttle_p 可以用来代替 throttle。throttle_p 将会拒绝连接，如果过去已进行过太多的连接。如果最高频率为 100 次，而在过去的一分钟内有 250 次连接尝试，那么不仅在过去的一分钟内的前 100 次连接后远程站点会被阻塞，而且这种阻塞会持续到第 2 分钟。或者说，每分钟后，最高频率从连接尝试的总数中扣除，只要连接尝试的总次数大于最高频率就会阻塞远程系统。

如果指定的 IP 地址没有超过每分钟连接的最高频率，共享库调用将失败。

如果超过最高频率，调用将成功但不会有任何内容返回。这是在 $C/$E 结合体中实现的，如例子中那样：

```
PORT_ACCESS

  TCP|*|25|*|* \
$C$[server_root/lib/conn_throttle.so， throttle,$1,10]\
$N421$ Connection$ not$ accepted$ at$ this$ time$E
```

其中，

$C 继续从下一个表条目开始的映射处理；将该条目的输出字符串作为映射处理的新的输入字符串使用。

$[*server_root*/lib/conn_throttle.so，throttle,$1,10] 作为将 throttle 作为库例程调用的库， $1 为服务器 IP 地址， 10 为每分钟节流的连接极限。

$N421$ Connection$ not$ accepted$ at$ this$ time 拒绝访问并且返回 421 SMTP 代码 （transient negative completion）并伴随着 “连接此时未被接受”的讯息。

$E 马上停止映射处理。将此条目的输出字符串用作映射处理的最终结果。

实施访问控制的时机

Messaging Server 应尽量早地对访问控制映射进行检查。这种现象发生的确切时间依赖于使用中的电子邮件协议 - 当必须检查的信息可用时。

对于 SMTP 协议，FROM_ACCESS 拒收情况的发生是对 MAIL FROM: 命令所作出的响应，即在发送端发送收件人信息或邮件数据之前。SEND_ACCESS 或 MAIL_ACCESS 拒收情况的发生是对 RCPT TO: 命令所作出的响应，即在发送端开始发送邮件数据之前。如果 SMTP 邮件被拒收， Messaging Server 则根本不接受或看不到该邮件数据，因此可最大限度地减少因执行此类拒收任务而增加的系统开销。

如果有多个访问控制映射表， Messaging Server 将对其一一进行检查。也就是说，FROM_ACCESS、 SEND_ACCESS、 ORIG_SEND_ACCESS、 MAIL_ACCESS 和 ORIG_MAIL_ACCESS 五个映射表可能全部有效。

测试访问控制映射

imsimta test -rewrite 实用程序 - 尤其是带有 --from、 - source_channel 和 -destination_channel 等选项时 - 可用于测试访问控制映射。例如，图 10-4 所示为 SEND_ACCESS 映射表和探查结果的一个样本。

图 10-4 样本 SEND_ACCESS 映射表和探查项

映射表

```
SEND_ACCESS

  tcp_local|friendly@siroe.com|l|User@sesta.com     $Y
  tcp_local|unwelcome@varrius.com|l|User@sesta.com  $NGo$ away!
```

探查项

```
$ TEST/REWRITE/FROM="friendly@siroe.com" -
_$  /SOURCE=tcp_local/DESTINATION=l User@sesta.com
...
Submitted address list:
  l
    User (SESTA.COM) *NOTIFY FAILURES* *NOTIFY DELAYS* Submitted
notifications list:


$ TEST/REWRITE/FROM="unwelcome@varrius.com" -
_$  /SOURCE=tcp_local/DESTINATION=l User@sesta.com
...
Submitted address list:
Address list error -- 5.7.1 Go away! User@sesta.com

Submitted notifications list:
```

添加 SMTP 转发

按照默认设置， iPlanet Messaging Server 被配置为阻塞 SMTP 转发的尝试；也即，拒绝将邮件提交至来自未认证外部源 （外部系统指除服务器所驻留的主机之外的任何其他系统）的外部地址。这样的默认配置在阻塞 SMTP 转发中十分苛刻，因为它将所有其它系统都作为外部系统。

尝试通过 iPlanet Messaging Server 系统的 SMTP 服务器，以外部地址或不使用 SMTP AUTH (SASL) 认证之处为目标提交邮件的 IMAP 和 POP 客户程序，将会发现提交尝试被拒绝。因此，可能希望修改配置，从而可以识别自己内部的系统和子网络，使得从这些地方转发邮件总被接受。

至于哪些系统和子网络被识别为内部的，这通常由 INTERNAL_IP 映射表控制，该表可以在文件 < *InstanceRoot*>/imta/config/mappings 中找到。

例如，其 IP 地址为 123.45.67.789 的 iPlanet Messaging Server 系统中，默认 INTERNAL_IP 映射表应如下所示：

```
INTERNAL_IP

   $(123.45.67.89/32)   $Y
   127.0.0.1   $Y
   *   $N
```

在这里，使用语法 $(IP- 模式 / 有效前缀二进制位) 的初始条目指定：任何与 123.45.67.89 的所有 32 位相匹配的 IP 地址都应该是匹配成功的，并被认作内部。第 2 个条目将循环返回 IP 地址 127.0.0.1 认作内部。最后条目指定：所有其它 IP 地址均不认作内部。注意：所有条目前至少要有一个空格。

可以通过在最后 $N 条目前指定另外的 IP 地址或子网络来添加更多的条目。这些条目必须在左侧指定一个 IP 地址或子网络（使用 $(.../...) 语法指定子网络），在右侧指定 $Y。或者修改现存的 $(.../...) 条目以接受一个更一般化的子网络。

例如，如果同样的样本站点有一个 class-C 网络，也即，它拥有所有的 123.45.67.0 子网络，那么该站点可能需要修改初始条目以改变用于匹配地址的位数。在下面的映射表中，将 32 位改为 24 位。这样就允许 class-C 网络上的所有客户程序都可通过 SMTP 转发服务器转发邮件。

```
INTERNAL_IP

   $(123.45.67.89/24)   $Y
   127.0.0.1   $Y
   *   $N
```

或者，如果该站点只有 123.45.67.80 到 123.45.67.99 范围内的那些 IP 地址，则该站点可能需要使用：

```
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
```

注意：<*InstanceRoot*>/imsimta test -match 实用程序可以用于检查 IP 地址是否与特定的 $(.../...) 测试条件匹配。<*InstanceRoot*>/imsimta test -mapping 实用程序在检查 INTERNAL_IP 映射表对各种 IP 地址输入的返回结果是否是预期结果方面，既有更广泛的用途。

在修改 INTERNAL_IP 映射表之后，一定要执行 <*InstanceRoot*>/imsimta restart 命令（如果运行使用的配置是已编译的），或者 <*InstanceRoot*>/imsimta refresh 命令（如果运行使用的配置是未编译的），以使修改生效。

有关映射文件和一般映射表格式的信息，以及有关 imsimta 命令行实用程序的信息，可以在 **iPlanet Messaging Server Reference Manual** 中找到。

允许对外部站点进行 SMTP 转发

所有内部 IP 地址都应当如前面讨论的那样添加到 INTERNAL_IP 映射表。如果希望允许从友好或同伴系统 / 站点进行 SMTP 转发，最简单的方法就是将它们与你的真实内部 IP 地址一起包含在 INTERNAL_IP 映射表中。

如果不希望将这些系统 / 站点作为真实的内部系统 / 站点，（例如，如果为了日志记录或者其他控制目的，希望区分*真实内部系统*和*拥有分程转发特权的友好非内部系统*），可以用其他方法配置系统。

一种方法就是建立一个特殊通道来接受来自友好系统的邮件。具体做法是：创建一个 *tcp_friendly* 通道，类似于现存的带有正式主机名 *tcp_friendly-daemon* 的 *tcp_internal* 通道，并创建一个 FRIENDLY_IP 映射表，类似于列出友好系统 IP 地址的 INTERNAL_IP 映射表。然后在当前重写规则的后面：

```
! Do mapping lookup for internal IP addresses
[]    $E$R${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
```

添加一条新的重写规则：

```
! Do mapping lookup for "friendly", non-internal IP addresses []
$E$R${FRIENDLY_IP,$L}$U%[$L]@tcp_friendly-daemon
```

另一种选择是将新条目添加到 ORIG_SEND_ACCESS 映射表中最后 $N 条目的上面，新条目的格式为：

```
  tcp_local|*@siroe.com|tcp_local|*     $Y
```

其中 siroe.com 是一个友好域的名称，并以如下格式添加一个 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
```

表，其中 $(...) 这样的 IP 地址语法和前一节描述的语法相同。只要地址正确，ORIG_SEND_ACCESS 检查就能成功，因此可以继续进行 ORIG_MAIL_ACCESS 检查，这一检查更加严格：只有 IP 地址也对应于一个 siroe.com IP 地址时才成功。

配置 SMTP 转发阻塞

您可用访问控制映射功能防止别人通过您的 Messaging Server 系统转发 SMTP 邮件。例如，您可通过该功能防止别人使用您的邮件系统向百计或以千计的互联网邮箱转发垃圾邮件。

Messaging Server 的默认配置是预防所有的 SMTP 转发活动，其中包括本地 POP 和 IMAP 用户的转发活动。

若需在阻塞未授权的转发活动的同时又允许合法的本地用户使用转发功能，则需对 Messaging Server 进行配置，以使其知道如何区分这两类用户。例如，使用 POP 或 IMAP 的本地用户所依靠的是用 Messaging Server 进行 SMTP 转发。

若需预防 SMTP 转发，您必须能：

- 区分内部邮件和外部邮件
- 区分已认证用户邮件
- 防止邮件分程转发

要启用内部主机和客户程序的 SMTP 转发，必须将 “内部” IP 地址或者子网络添加到 INTERNAL_IP 映射表中。

MTA 如何区分内部邮件和外部邮件

为了阻塞邮件转发活动，您首先必须能够区分您所在网站来的内部邮件和从互联网来的并通过您的系统回到互联网上的外部邮件。在这两类邮件中，前者是您需要准许通行的邮件；后者是您需要阻塞的邮件。区分是通过将 switchchannel 关键字用于入站 SMTP 通道上而实现的，该通道通常就是 tcp_local 通道，并且是默认的。

switchchannel 关键字可使 SMTP 服务器对与外来 SMTP 连接相关的实际 IP 地址进行检查。Messaging Server 可通过该 IP 地址，加上您制定的重写规则，二者可结合起来对域内来的 SMTP 连接和域外来的连接进行区分。这一信息随后便可用来隔离内部和外部邮件信量。

以下说明的 MTA 配置是默认设置的，在这样的配置下服务器可以区分内部和外部邮件传送。

- 配置文件中，在本地通道之前是带有关键字 noswitchchannel 的 defaults 通道：

```
! final rewrite rules
defaults noswitchchannel
! Local store
ims-ms ...
```

- 入站 TCP/IP 通道指定了 switchchannel 和 remotehost 这两个关键字；例如：

```
tcp_local smtp single_sys mx switchchannel remotehost
TCP-DAEMON
```

- 在入站 TCP/IP 通道定义之后是一个名字不同的类是通道；例如：

```
tcp_intranet smtp single_sys mx allowswitchchannel routelocal
tcp_intranet-daemon
```

  routelocal 通道关键字在重写地址到通道时促使 MTA 尝试使任何通过该通道的地址中的显式接路由 “短路”，从而对通过内部 SMTP 主机借助于显式源路由地址进行循环转发的尝试加以阻塞。

在做了上述配置变更后，您所在域中生成的 SMTP 邮件都将通过 tcp_intranet 通道入站。所有其它 SMTP 邮件都将通过 tcp_local 通道入站。根据邮件入站的通道区分内部和外部邮件。

这是如何实现的？关键在于 switchchannel 这个关键字。该关键字被用于 tcp_local 通道。当一封来件送达到 SMTP 服务器时，该关键字可使服务器查找与外来连接相关的源 IP 地址。服务器此时将尝试对外来连接的实际 IP 地址以反指向进行信封重写，以期查找相关的通道。如果源 IP 地址与 INTERNAL_IP 映射表中的 IP 地址或子网络匹配，应用于该映射表的重写规则将使地址重写到 tcp_intranet 通道。

因为 tcp_intranet 通道标有 allowswitchchannel 关键字，所以该邮件将被转换到 tcp_internal 通道，并从该通道入站。如果邮件来自于其 IP 地址不在 INTERNAL_IP 映射表中的某个系统，反向信封重写可能重写到 tcp_local 或其他通道。但绝不会在 tcp_intranet 通道里重写；同时，由于所有其它通道都在第 1 步中被标志为 noswitchchannel，所以邮件只能保留在 tcp_local 通道而不会转换到另一通道。

备注 注意，任何使用 “tcp_local” 字符串的映射表或转换文件条目可能需要根据其用途被改变为 “tcp_*” 或者 “tcp_intranet”。

区分已认证用户邮件

您所在站点可能有一些并非属于实际网络一部分的 “本地” 客户机用户。当这些用户提交邮件时，其邮件将通过某一外部 IP 地址提交，如：任意 Internet 服务供应商。如果用户使用的邮件客户程序能执行 SASL 认证，他们的认证连接则可与任意的其它外部连接区分开来。至此，您便可在拒收未经认证的转发邮件的提交企图之同时，允许认证的邮件通过。您可通过 saslswitchchannel 关键字在入站 SMTP 通道上区分认证的和未经认证的连接，该通道通常为 tcp_local 通道。

saslswitchchannel 关键字将取用一个参数 （或变元），用以指定待转入之通道；如果 SMTP 发件人认证成功，则可考虑允许他们提交的邮件入站并将其置入指定的交换通道。

若需添加认证提交之邮件的区分功能，请按下列步骤操作：

1. 在配置文件中，以一独特的名称添加一个新的 TCP/IP 通道定义；例如：

   ```
   tcp_auth smtp single_sys mx mustsaslserver noswitchchannel
   TCP-INTERNAL
   ```

   该通道不应允许正常的通道交换（也就是说，该通道上应该有 noswitchchannel 之定义，不论是直接添加的还是以前默认行所隐含的）。该通道上应该有 mustsaslserver。

2. 如下面的范例所示，修改 tcp_local 通道时，请在其中添加 maysaslserver 和 saslswitchchannel tcp_auth：

   ```
   tcp_local smtp mx single_sys maysaslserver saslswitchchannel
   tcp_auth \
   switchchannel
   |TCP-DAEMON
   ```

有了这一配置后，那些能用本地口令通过认证的用户，他们发送的 SMTP 邮件便可通过 tcp_auth 通道入站。从内部主机发送的未经认证的 SMTP 邮件仍将通过 tcp_internal 入站。所有其它 SMTP 邮件都将通过 tcp_local 入站。

防止邮件分程转发

下面介绍本范例的另一个题目：怎样防止未经认证的人通过您管理的系统转发 SMTP 邮件。首先应记住的一点是：要允许本地用户转发 SMTP 邮件。例如， POP 和 IMAP 用户是依靠 Messaging Server 发送邮件的。需注意的一点是：本地用户既可以是身在本地的用户 （在这种情况下，其邮件通过一内部 IP 地址入站），也可以是身在远端的用户，但能够以本地用户身份通过认证者。

您想防止互联网上的闲散之人把您管理的服务器当作转发站使用。通过下节说明的配置步骤，您不仅能够区分这类用户，而且能阻塞您想阻塞的类别。具体而言，您需要的是阻塞邮件从 tcp_local 通道入站，并从同一通道出站。您可通过 ORIG_SEND_ACCESS 映射表达到此目的。

ORIG_SEND_ACCESS 映射表可根据来源和目的地通道阻塞通信流。在本例中，被阻塞的是源于和发往 tcp_local 通道的通信流。这乃是通过下面的 ORIG_SEND_ACCESS 映射表实现的：

```
ORIG_SEND_ACCESS

   tcp_local|*|tcp_local|*        $NRelaying$ not$ permitted
```

此例中的条目规定：邮件不得通过 tcp_local 通道入站和出站。也就是说，该条目不允许外部邮件进入您的 SMTP 服务器，然后再转发回到互联网。

使用 ORIG_SEND_ACCESS 映射表而不使用 SEND_ACCESS 映射表的原因在于，阻塞将不会因此而套用到原来与 ims-ms 通道匹配的地址上（但却可通过别名或邮件发送列表定义经扩展而回到外部地址）。若使用 SEND_ACCESS 映射表，则需费很大的周折才能允许外来的人向邮件发送列表发送邮件，因为邮件发送列表可向外扩展至外部用户，并可将邮件发送给那些能向外部地址转发邮件的用户。

使用 DNS 查找，其中包括针对 SMTP 转发阻塞的 RBL 检查

在 iPlanet Messaging Server 中存在着多种不同的方法可确保所有传递或转发自一个具有有效 DNS 名的地址的邮件都被接受。最简单的方法就是将 mailfromdnsverify 通道关键字放置于 tcp_local 通道上。

iPlanet Messaging Server 还提供了 dns_verify 程序，该程序可确保所有传递或转发自一个具有有效 DNS 名的地址的邮件都被接受，这需要使用 ORIG_MAIL_ACCESS 中的以下规则：

```
ORIG_MAIL_ACCESS

  TCP|*|*|*|*|SMTP|MAIL|*|*@*|*|*\
$[<server_root>/bin/msg/imta/lib/dns_verify.so,\
dns_verify,$6|$$y|$$NInvalid$ host:$ $$6$ -$ %e]
```

上面例子中的断行对于这样的映射表条目具有语法意义。反斜杠字符是续行的一种合法方法。

dns_verify 映像还可用通过参照 RBL （实时黑洞列表）、 MAPS （防止滥发邮件系统）、 DUL （拨号上网用户列表）以及 ORBS （开放转发行为修正系统）等列表检查进入的连接，从而成为保护系统免受 UBE（垃圾邮件）影响的另一种尝试。利用新的 mailfromdnsverify 关键字，针对上述检查可以采用另外的 “更易于配置” 的方法，而不必进行 dns_verify 调用。这种更简单的方法就是使用 dispatcher.cnf 文件中的 DNS_VERIFY_DOMAIN 选项。例如，在 [SERVICE=SMTP] 节，将选项的实例设置为检查时需要参照的各种列表。

```
[SERVICE=SMTP]
PORT=25
! ...rest of normal options...
DNS_VERIFY_DOMAIN=rbl.maps.vix.com
DNS_VERIFY_DOMAIN=dul.maps.vix.com
!...etc...
```

这种简单方法的缺点是它检查所有正常进入的 SMTP 邮件，包括内部用户发送的邮件。这可能使网络的连通性下降，导致效率降低或其他潜在问题。另一种选择就是从 PORT_ACCESS 映射表或 ORIG_MAIL_ACCESS 映射表调用 dns_verify。在 PORT_ACCESS 映射表中，可以使初始条目或其他条目不对本地内部的 IP 地址或邮件提交人进行检查，而使其后的条目对其他情况进行所需要的检查。或者，在一个 ORIG_MAIL_ACCESS 映射表中，如果只检查通过 tcp_local 通道进入的邮件，就可以避开对来自内部系统 / 客户机的邮件的检查。使用指向 dns_verify 的条目的例子如下。

```
PORT_ACCESS

! Allow internal connections in unconditionally
  *|*|*|*|*  $C$|INTERNAL_IP;$3|$Y$E
! Check other connections against RBL list
  TCP|*|25|*|*\
$C$[server_root>/bin/msg/imta/lib/dns_verify.so,\
dns_verify_domain_port,$1,rbl.maps.vix.com.]EXTERNAL$E


ORIG_MAIL_ACCESS

  TCP|*|25|*|*|SMTP|*|tcp_local|*@*|*|*\
$C$[<server_root>/bin/msg/imta/lib/dns_verify.so,\
dns_verify_domain,$1,rbl.maps.vix.com.]$E
```

支持基于 DNS 的数据库

从 iPlanet Messaging Server 5.2 开始，dns_verify 程序支持基于 DNS 的数据库，用以确定可能发送垃圾邮件的 SMTP 连接。某些向公共提供的 DNS 数据库不包含通常用于此目的 TXT 记录。取而代之的是，它们只包含 A 记录。

在一个典型的安装中，为一特定的 IP 地址而在 DNS 中找到的 TXT 记录包含一个出错消息，用于在拒收邮件时返回到 SMTP 客户机。但是，如果没有找到 TXT 记录，而是找到一个 A 记录，那么在 iPlanet Messaging Server 5.2 之前的 dns_verify 的版本返回的消息是 *“无可用的出错消息”*

dns_verify 现在支持一选项用于指定在没有可用的 TXT 记录的情况下使用的默认文本。例如，如下的 PORT_ACCESS 映射表展示如何启动这一选项：

```
PORT_ACCESS

    *|*|*|*|* $C$|INTERNAL_IP;$3|$Y$E
    TCP|*|25|*|*
$C$[/export/home/iplanet/server51/msg/bin/imta/lib/dns_verify.so
,dns_verify_domain_port,$1,dnsblock.siroe.com,Your$ host$ ($1)$
found$ on$ dnsblock$ list]$E
    * $YEXTERNAL
```

在这个例子中，如果在 dnsblock.siroe.com 域的查询中找到远程系统，但是没有可用 TXT 记录，那么将会返回如下信息，*“Your host a.b.c.d found on dnsblock list.”*

处理大量访问条目

那些在映射表中使用大量条目的网站应该考虑在其映射表中设立几个带同配符的通用条目。这些通用条目可调用通用数据库查找具体项目。与直接在映射表中使用大量条目之作法相比，在映射表中设置几个可调用通用数据库查找具体项目的条目之作法效率更高。

对那些想控制每一个用户以限制哪些用户能从互联网上收发电子邮件的站点而言，后一种作法尤其可取。这种控制可轻而易举地用 ORIG_SEND_ACCESS 一类的访问映射表实现。对于此类用途而言，将大批量的具体信息（如具体地址）储存在通用数据库并可用映射表条目随时调用通用数据库之作法可大幅度地提高操作效率和系统性能。

例如，您可考虑使用图 10-5 所示的映射表结构。

图 10-5 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...
```

这种映射表需在表中逐个输入每一名用户，如果您认为这种方式工作量过大，则可使用图 10-6 所示的一种更有效的设置方法（如果有成千上万的用户条目，此种方法效率最高）。该图表所示为一通用数据库条目样本和 ORIG_SEND_ACCESS 映射表样本。

图 10-6 数据库条目和映射表样本

数据库条目

```
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
```

映射表

```
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
```

此例中，通用数据库左侧使用的任意字符串 SEND| 和 RECV|（及由此而在通用数据库中由映射表生成的探查）提供了一种可区分所生成的两类探查项的方法。如上表所示，用 $C 和 $E 标志包裹通用数据库探察项之作法是典型的映射表向通用数据库请求的调出项。

上例所示为一简单的映射表探察项对应通用数据库条目进行检查的情况。如果映射表带有更复杂的探察项，亦可通过通用数据库获得许多使用上的便利。

访问控制映射表标志

表 10-3 显示与 SEND_ACCESS、ORIG_SEND_ACCESS、MAIL_ACCESS、ORIG_MAIL_ACCESS 和 FROM_ACCESS 等映射表相关的访问映射标志。请注意，PORT_ACCESS 映射表所支持的标志组有所不同 （参见表 10-2）。

表 10-3　访问映射标志

标志	说明
$B	将邮件重定向到位存储桶 （bitbucket）。
$H	将邮件保存为 .HELD 文件。
$Y	允许访问。
带参数的标志，以参数读取顺序 +	
$J *地址*	将原信封 From 地址替换为指定的*地址*。 *
$K *地址*	用指定 的*地址*取代原 “From” 地址。 * ++
$I *用户* | *标识符*	检查指定用户的用户组 ID。
$< *字符串*	将*字符串*发送至 syslog （UNIX， user.notice 实用程序和 severity）或者若探查匹配成功则发送至 event log （NT）。 +++
$> *字符串*	将*字符串*发送至 syslog （UNIX， user.notice 实用程序和 severity）或者若访问被拒绝则发送至 event log （NT）。 +++
$D *延迟*	延迟应答为百分之一秒的*延迟*间隔；正值将致使延迟时间施加于事务处理中的每一个命令；负值将致使延迟时间只施加于地址移交 （SMTP MAIL FROM: 用于 FROM_ACCESS 表的命令；SMTP RCPT TO: 用于其它表的命令）。
$T *标志*	前缀之以*标志*。
$A *标题*	将标题行*标题*添加到邮件中。
$X *错误代码*	如果拒收邮件，则发出指定的*错误代码*扩展的 SMTP 错误代码。
$N *字符串*	拒绝访问并给出可选的出错信息文本*字符串*。
$F *字符串*	*$N 字符串*的同义语；也即，拒绝访问并给出可选的出错信息文本*字符串*。

* 仅用于 FROM_ACCESS 表。

\+ 使用带参数的多重标志时，请用竖杠字符 | 将参数隔开，并按照表中所列顺序放置参数。

++ 为了让 $K 标志在 FROM_ACCESS 映射表中生效，源通道必须包括 authrewrite 关键字。

+++ 在对付不守规矩的发件人时，最好使用 $D 标志，以防他们的攻击瘫痪整个服务。尤其是，最好将 $D 用于任何 $> 条目中，否则 $< 条目拒绝访问。

第二部分：邮箱过滤器

第二部分包括下列章节：

- 绪论
- 针对每个用户创建过滤器
- 创建通道级过滤器
- 创建 MTA 级过滤器
- 调试用户过滤器

绪论

过滤器由可作用于电子邮件的一项或多项制约性操作组成。Messaging Server 的过滤器通常储存在服务器上，并由服务器进行估算。因此，过滤器有时被称为服务器端规则 （SSR）。Messaging Server 的过滤器基于 SIEVE 过滤语言 （Draft 9 of the SIEVE Internet Draft）。

作为管理员，您可创建通道级过滤器和 MTA 级过滤器，以防范无用邮件的传递。可以通过 iPlanet Delegated Administrator for Messaging 界面创建过滤器模板并让所有最终用户使用。最终用户可用这些模板为其个人邮箱设立过滤器，以防无用邮件传递到他们的邮箱。

服务器以下列优先级施用过滤器：

1. 用户级过滤器 （Per-user filter）

   如果某个人邮箱过滤器可直接接收或拒收邮件，则该邮件的过滤处理到此结束。但是如果收件用户没用邮箱过滤器，或者用户的邮箱过滤器未能直接应用于有问题的邮件，则 Messaging Server 下一步就应用通道级过滤器。

2. 通道级过滤器 （channel-level filter）。

   如果通道级过滤器可直接接收或拒收邮件，则该邮件的过滤处理到此结束。否则 Messaging Server 将随即施用 MTA 级过滤器 （如果有的话）。

3. MTA 级过滤器 （MTA-wide filter）

根据默认设置，用户都没有邮箱过滤器。当用户通过 Delegated Administrator 界面创建了一个或多个过滤器时，这些过滤器将储存在目录中，并在目录同步处理期间由 MTA 进行检索。

针对每个用户创建过滤器

用户级过滤器适用于目的地为特定用户邮箱的邮件。作为管理员，可以通过 iPlanet Delegated Administrator for Messaging 界面创建过滤器模板并让所有最终用户使用。最终用户可用这些模板建立个人服务器过滤器以控制向其邮箱传递的邮件；也就是说，最终用户可拒收无用的邮件，重定向邮件，将邮件筛选到邮箱的文件夹等。

过滤器模板可归纳 Sieve 脚本，其方法是用提示符和输入字段替代 Sieve 脚本的“硬代码”元素。然后用 Java servlet 分析筛选模板并在浏览器中生成 UI 页面。当最终用户在输入字段中键入值时， servlet 将取这些值并将其储存到用户目录配置文件条目的某个筛选脚本中。提示和输入字段通过 Delegated Administrator 界面向最终用户显示。

提供了一套样本模板并随 Delegated Administrator 一起安装。模板文件位于下列目录：

```
nda-path/nda/nda/default/lang/templates/enduser/ssr/*.txt
```

您可用 Sieve 语言修改过滤器模板或创建新的过滤器模板。如果创建了新的过滤器模板，必须将其保存在上述 `ssr` 目录的文本文件中。必须保证该文件的字可读，并为过滤器模板添加一个 LDAP 条目，如下面的例子所示：

```
dn: cn=Subject Discard,cn=ssrconf,cn=en,
              cn=domainConfiguration,ou=config,o=isp
objectclass: top
objectclass: nsValueItem
cn: Subject Discard
nsvaluetype: nsValueCIS
nsvaluecis: ../templates/enduser/ssr/subject-discard.txt
```

图 10-7 显示样本模板。

图 10-7 样本 Sieve 模板

```
#RULE: $Template="File To Folder"
require "fileinto";
if header :contains # Q1
     # Q2
{
     fileinto # Q3
    ;
}

#PRE: "This rule files messages into a folder."
#PRE: "Choose the header line to search on"
#PRE: "And specify the phrase you wish to search for"
#Q1: header "If the header line"
#Q2: value "Contains the phrase"
#Q3: folder "Then file into the folder"
```

上例中， Q1、Q2 和 Q3 用作输入值的占位符，以便 UI 能够找到替换值的位置。每一标志都将映射到某个问题和输入值的某一数据类型。

每一标志的注释行中都对数据类型和相关问题有所定义。定义形式为 *token*:*data-type-variable*，后面有一加引号的字符串，包含实际的问题。上例中的 `header value` 以及 `folder` 均是数据类型，它们都可显示一个下拉列表、编辑框，或其它工具。UI 可通过这些数据类型变量得知需从用户处获取的信息种类。

对模板进行语法分析后，将为用户生成并显示一个对话，如图 10-8 所示。此例中的括号表示下拉列表。

图 10-8 模板输出样本

```
+-----------------------------------------------------------------+
| Template: File To Folder Name: ___________________              |
+-----------------------------------------------------------------+
|           This rule files messages to a folder                  |
|           Choose the header line to search on                   |
|       And specify the phrase you wish to search for             |
|                                                                 |
|   If the header line: [From       ]                             |
|   Contains the phrase: ____________________________             |
|   Then file into the folder: ___________________                |
+-----------------------------------------------------------------+
```

用户输入数据后，该项规则将储存在用户的 `mailSieveRuleSource` 属性中。

模板语法有下列限制条件：

- `#RULE` 行需在任何其它行之前显示，并需指定 `$Template`。
- 任何开头为 `#PRE` 的注释行都将在 GUI 页面中先于输入字段予以显示。

  `#PRE` 语句需用双引号字符串括起来。
- 任何开头为 `#POST` 的注释行都将在 GUI 页面结尾显示。

  `#POST` 语句需用双引号字符串括起来。
- 其它注释行不在 GUI 页面显示。
- 标志应为 ASCII 字符串，无需区分大小写；标志中不能含任何空白区域（白空间）。
- 数据类型变量应跟在注释行标志字符串的后面；这些变量也无需区分大小写。
- 实际问题应在注释行中定义，直接放在数据类型变量之后，并以双引号括之。

Sieve 模板支持下列数据类型变量：

- `header` - 在 GUI 中显示时，系统将使用一个列表框，可用值包括下列：`Subject`，`To`，`From`。

  当筛选规则被保存到用户条目时，`Subject` 值将被扩展为 Subject、Comments、Keywords；`From` 值将被扩展为 From、Sender、Resent-from、Resent-sender、Return-path；`To` 值将被扩展为 To、Cc、Bcc、Resent-to、Resent-cc、Reset-bcc。
- `value` - 将用一文字字段显示。
- `address` - 将用一文字字段显示。地址的语法将按照 RFC 822 邮件地址格式进行检查。

- `folder` - 将用一文字字段显示。
- `size` - 用户可以从 Kilobyte， Megabyte 中选择，或者指定任何数字。
- `message` - 将用一文字区域显示。

创建通道级过滤器

通道级过滤器可施用于某通道中排列的每一封邮件。此类过滤器的典型用途是在特定通道中阻塞穿行的邮件。

创建通道级过滤器：

1. 使用 SIEVE 编写过滤器。
2. 然后将过滤器储存到下列目录的一个文件中：

   `msg-`*instance*`/imta/config/`*file*`.filter`

   该文件须为文字可读文件并为 MTA 的 uid 所有。
3. 请在通道配置中包括下列：

   `destinationfilter file:IMTA_TABLE:`*file*`.filter`
4. 重新编译配置文件，然后重新启动 Dispatcher。

   请注意：过滤器文件更改后，无需重新编译或重新启动 Dispatcher。

`destinationfilter` 通道关键字此时启用邮件过滤功能，筛选*发至*过滤通道中排列的邮件。 `sourcefilter` 通道关键字此时启用邮件过滤功能，筛选*来自*过滤通道中排列的邮件。按要求，这些关键字都有一个参数。该参数用于指定通往相关通道过滤器文件的路径（即与该通道相关过滤器文件）。

`destinationfilter` 通道关键字的语法为：

`destinationfilter` *URL-pattern*

`sourcefilter` 通道关键字的语法为：

源 `sourcefilter` *URL-pattern*

其中， *URL-pattern* 是一个 URL，用于指定相关通道过滤器文件的路径。在下面的例子中，*channel-name* 为通道名称。

目标过滤器文件 `:///usr/tmp/filters/`*channel-name*`.filter`

`filter` 通道关键字此时启用该过滤器所施加的通道上的邮件过滤功能。按要求，该关键字有一个参数，用于指定与每一信封收件人（通过该通道接收邮件者）相关的过滤器文件的路径。

`filter` 通道关键字的语法为：

`filter` *URL-pattern*

URL-pattern 是一个 URL，在对特殊的替换顺序进行处理之后可针对给定的收件人地址将路径让给过滤器文件。*URL-pattern* 可含特殊的替换顺序，而且在遇到此种情况时，可用从相关的收件人地址 （即 `local-part@host.domain`）导出的字符串予以取代。有关替换顺序，请见第 259 页表 10-4。

`fileinto` 关键字用于指定施加了邮箱过滤器的 `fileinto` 算符后如何改变地址。下列例子指定：文件夹名称应作为子地址插入到原地址，以此替换原有的子地址：

```
fileinto $U+$S@$D
```

表 10-4　置换标志 （不区别大小写）

标志	含义
*	执行用户组扩展。请参阅第 430 页 “处理组条目”。
**	扩展 `mailForwardingAddress` 属性。此属性可以是导致几个传递地址产生的多值属性。
$$	在 $ 字符中替换
$\	强制将随后的文本改为小写字母
$^	强制将随后的文本改为大写字母
$_	对随后的文本中不进行大小写转换
$~	在与地址本地部分相关的主目录的文件路径中替换
$1S	同 `$S`，但若无可用子地址则不进行任何插入操作。
$2S	`$S`，但若无可用子地址则不进行任何插入操作，同时删除前导字符。
$3S	同 `$S`，但若无可用子地址则不进行任何插入操作，同时忽视后随字符。
$A	在地址 local-part@ host.domain 中替换
$D	在 host.domain 中替换
$E	插入第二备用属性的值， `LDAP_SPARE_1`
$F	插入传递文件名 （`mailDeliveryFileURL` 属性）
$G	插入第二备用属性的值， `LDAP_SPARE_2`
$H	在主机中替换
$I	插入托管域 （UID 在 `domainUidSeparator` 指定的分隔符的右侧部分）。如果没有可用的托管域，操作失败。
$1I	同 `$I`，但若无可用的托管域则不进行任何插入操作。
$2I	同 `$I`，但若无可用的托管域则不要进行任何插入操作，同时删除前导字符。
$3I	同 `$I`，但若无可用子地址则不进行任何插入操作，同时忽视后随字符。
$L	在本地部分中替换

表 10-4　置换标志 （不区别大小写）（接上页）

标志	含义
$M	插入 UID，删除了任何托管域
$P	插入程序名 （mailProgramDeliveryInfo 属性）
$S	插入与当前地址相关的子地址。子地址通常为子地址分隔符 （通常就是 +）后原始地址的用户部分，但是可以用 MTA 选项 SUBADDRESS_CHAR 指定。如果不给出子地址，操作失败。
$U	插入当前地址的邮箱部分。可能是符号 @ 左侧部分整体，或者是子地址分隔符 + 前的地址的左侧部分。

创建 MTA 级过滤器

MTA 级过滤器适用于归队于 MTA 的所有邮件。这种过滤器的一个典型用途就是阻塞垃圾邮件或其他无用邮件，无论邮件的目标地是什么。若需创建 MTA 级过滤器，请按下列步骤操作：

1. 使用 SIEVE 编写过滤器
2. 将过滤器储存在下列文件：

   msg-*instance*/imta/config/imta.filter

   该过滤器文件必须为世界可读。如果存在，则可自动使用。
3. 重新编译配置文件，然后重新启动 Dispatcher。

使用编译的配置时， MTA 级过滤器文件已结合到编译的配置之中。

以路由选择将放弃的邮件排除到 FILTER_DISCARD 通道

根据系统默认设置，被邮箱过滤器放弃的邮件将立即从系统中删除。然而，当用户首次设置邮箱过滤器时（及弄错时）或调试时，最好先不要使用删除作业，以推迟一段时间再用为上策。

若需把邮箱过滤器放弃的邮件临时保留在系统上以待以后删除，可先在 MTA 配置文件中添加一条 filter_discard 通道，添加时需用 notices 通道关键字指定删除前保留邮件的时间长度 （通常为天数）。具体作法，请见下面例子：

```
filter_discard notices 7
FILTER-DISCARD
```

然后便可设置 MTA 选项文件中的 FILTER_DISCARD=2 选项。filter_discard 队列区域中的邮件应考虑放在用户个人废纸篓文件夹的扩展部分内。在此情况下，需注意的一点是：对于 filter_discard 队列区域内的邮件，系统从不发送警告讯息，而且也不将此类邮件退回给发件人，即使有退回请求也不例外。对于此类邮件的处理方法如下：当最终通知值过期时或有人以 imsimta return 之类的实用程序请求以手动方式退回时，系统所能采取的唯一行动是最终将这些邮件默默地删除。

调试用户过滤器

如果系统上的用户过滤器出现问题，下列信息可帮助您解决问题。

目录同步（dirsync）进程将利用与用户过滤器有关的信息更新 MTA 的 SSR 数据库。短过滤器储存在该数据库中。对长过滤器而言，数据库将储存一个 LDAP dn。请注意，在 dirsync 进程没有更新数据库之前， MTA 看不到用户过滤器的变更情况。

为了便于排除过滤器的问题，请按下列步骤操作：

- 在 `imta.cnf` 文件中，检查 `ims-ms` 通道是否被标志为下列：

  ```
  filter ssrd:$a fileinto $u+$s@$d
  ```

- 确信 `dirsync` 进程能够通过 `configutil` 命令按下列对过滤器信息进行同步处理：

  `configutil -l -o service.imta.ssrenabled -v true`

  ```
  OK SET
  ```

  `configutil | fgrep ssr`

  service.imta.ssrenabled = true

- 测试过滤器时，请按下列方式使用 `imsimta test` 命令：

  `imsimta test -rewrite -debug -filter user@domain`

  请在输出中查找下列：

  ```
  mmc_open_url called to open ssrd:user@ims-ms
     URL with quotes stripped: ssrd:user@ims-ms
  Determined to be an SSRD URL.
     Identifier: user@ims-ms-daemon
  Filter successfully obtained.
  ```

- 如果过滤器有语法问题，请查找下列：

  ```
  Error parsing filter expression:...
  ```

  此错误可能明确表示出过滤器出了问题。

- 如果过滤器没有问题， `test` 命令将在输出结尾处显示过滤器。

- 如果过滤器有问题 `test` 命令将在输出结尾处显示下列：

  ```
  Address list error -- 4.7.1 Filter syntax error: user@siroe.com
  ```

  另外， `SMTP RCPT TO` 命令还将返回一临时的错误应答码，如：

  ```
  RCPT TO:<user@siroe.com>
  452 4.7.1 Filter syntax error
  ```

- 如果知道用户地址的最终重写形式，则可用 `imsimta test -url` 命令查看一下 MTA 是用什么作为该用户的过滤器的：

  `imsimta test -url ssrd:user@ims-ms-daemon`

  您可通过 `imsimta test -rewrite` 命令查找用户地址的最终重写形式。

第 11 篇

邮件存储库的管理

本章说明邮件存储库和邮件存储库管理界面。本章包括以下各节：

- 概要
- 邮件存储库目录布局
- 存储库如何清除邮件
- 指定管理员的存储库访问权限
- 关于邮件存储库空间配额
- 配置邮件存储库空间配额
- 指定时限策略
- 配置邮件存储库分区
- 维护和恢复作业
- 备份与恢复邮件存储库
- 对邮件存储库进行故障诊断

概要

邮件存储库中包含有特定 Messaging Server 实例的用户信箱。邮件存储库的大小随着邮箱、文件夹、日志文件等的数量的增加而增长。您可通过下列方法控制存储库的大小：指定邮箱的容量限度（磁盘空间配额），指定邮件总数的最大允许限度和设置存储库中邮件的时限策略。

随着系统中用户数量的不断增加，对磁盘存储空间的需求也随之增加。邮件存储库需配备的物理磁盘数量（一个或多个）取决于服务器所支持的用户数量。将另外的磁盘空间整合到系统上的方法有两种。最简单的方法是添加另外的分区。还可以选择性地添加另外的 Messaging Server 实例，分别对特定的邮件存储库负责。但是，此方法更为复杂。

另外，如果要支持多个托管域，则应为单独的大型网域配置专用的服务器实例。您可通过此种配置为特定的域指定存储库管理员。还可以通过添加更多分区扩展邮件存储库。

为了便于邮件存储库的管理， iPlanet Messaging Server 不仅提供了 iPlanet Console 界面，而且还提供了一套命令行实用程序。有关这些命令行实用程序的说明，请见表 11-1。有关使用这些实用程序的信息，请参见第 278 页“维护和恢复作业”和 **iPlanet Messaging Server Reference Manual**。

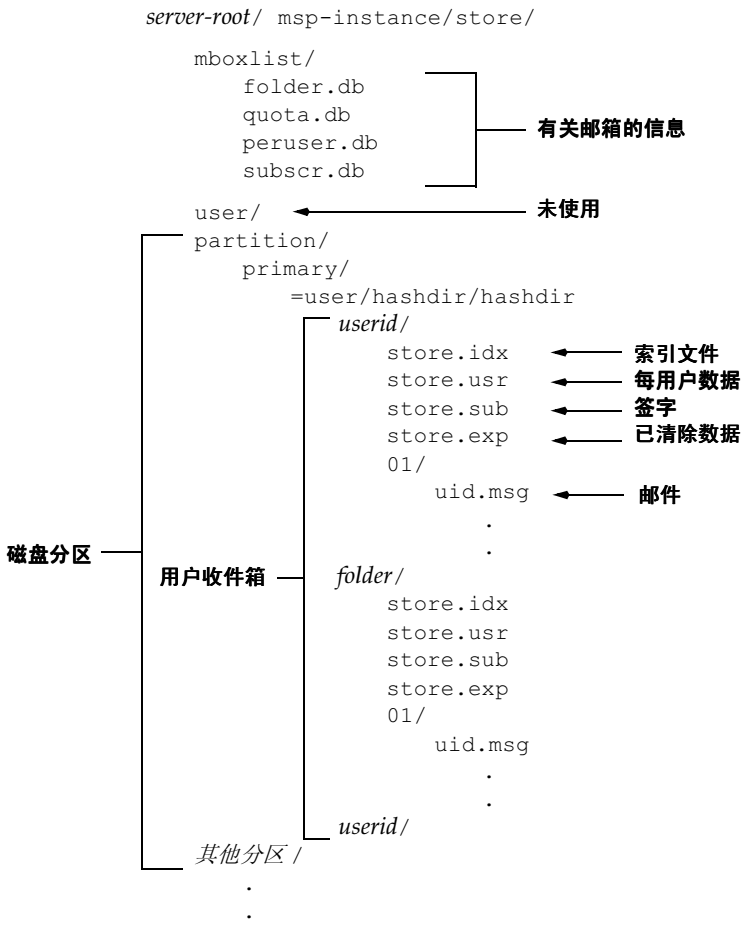
表 11-1　邮件存储库命令行实用程序

实用程序	说明
`configutil`	用于设置和修改存储库的配置参数。
`deliver`	直接将邮件传递到可由 IMAP 或 POP 邮件客户程序访问的邮件存储库。
`hashdir`	用于确定保含特定用户邮件存储库的目录。
`iminitquota`	从 LDAP 目录中重新初始化配额限制并重新计算使用的磁盘空间。
`imsasm`	处理用户邮箱的保存和恢复。
`imsbackup`	备份储存的邮件。
`imsexport`	将 Certificate Management System 邮箱导出到 UNIX `/var/mail` 格式文件夹。
`imsrestore`	用于恢复备份的邮件。
`imscripter`	IMAP 服务器协议脚本工具。执行命令或序列命令。
`mboxutil`	用于列示、创建、删除、重命名、移动邮箱，并报告空间配额使用情况。
`mkbackupdir`	创建和保持备份目录与在邮件存储库中信息的同步。
`MoveUser`	用于将用户帐户从一个邮件服务器移动到另一个邮件服务器。
`quotacheck`	计算在邮件存储库中每个用户的总邮箱大小，并将其与指定的配额进行比较。
`readership`	用于在共享 IMAP 文件夹中收集 readership 信息。
`reconstruct`	用于重建损坏的邮箱。
`stored`	用于执行各项后台任务和日常任务，清除和删除储存在磁盘中的邮件。

邮件存储库目录布局

图 11-1 所示为某服务器实例的邮件存储库目录布局。邮件存储库在设计上可为邮箱内容的存取提供快速访问能力。有关存储库目录的说明，请见表 11-2。

图 11-1 邮件存储库目录布局



例如，示例性的目录路经可以是：

server_root/msg-*instance*/store/partition/primary/=user/53/53/=mack1

表 11-2　邮件存储库目录说明

位置	内容 / 说明
server_root/msg-*instance*/store/	邮件存储库的顶层目录。包含 mboxlist、 user 和 partition 三个子目录。
.../store/mboxlist/	包含一个数据库 （Berkley DB），存储有与服务器中的邮箱有关的信息以及存储空间配额方面的信息。 文件 folder.db 中包含与邮箱有关的信息，其中包括存储邮箱的分区的名字、 ACL 以及 store.idx 中某些信息的副本。在 folder.db 中，每个邮箱都有一个条目。 文件 quota.db 中包含有关空间配额及其用量方面的信息。在 quota.db2 中，每个用户都有一个条目。 文件 peruser.db 中包含有关每个用户标志的信息。这些标志表明某用户是否看过或删除了某个邮件。 文件 subscr.db 中包含有关用户订阅方面的信息。
.../store/user/	未使用
.../store/partition/	包含默认的 primary 分区。还可在此分区中放置任何您自定义的子分区。
/*partition*/=user/	包含分区子目录中的所有用户邮箱。邮箱存储散列结构以利便于快速搜索。需要寻找含有特定用户邮箱的目录时，须使用 hashdir 实用程序。
/=user/*hashdir*/*hashdir*/*userid*/	ID 为 *userid* 之用户的顶层邮件夹。对默认域而言， *userid* 为 *uid*。对于托管域而言， *userid* 为 *uid@domain*。邮件即被传递到这个邮件夹中。
/*userid*/*folder*	用户定义的文件夹。
/*userid*/store.idx	一个索引，它提供了下列与存储在目录 /*userid*/ 中的邮件有关的信息：邮件数量、邮箱使用的空间配额、上一次向邮箱添加邮件的时间、邮件标志、每封邮件的可变长度信息，其中包括报头和 MIME 结构，以及每封邮件的大小等信息。对于每个用户而言，该索引还包含 mboxlist 信息的备份副本和每个用户的空间配额信息的备份副本。
/*userid*/store.usr	包含一个用户列表，即访问过该文件夹的用户。对于列出的每个用户，包含用户上一次访问该文件夹的时间、用户已查看邮件的列表和用户已删除邮件的列表。
/*userid*/store.exp	包含一个邮件文件列表，即已清除、但尚未从磁盘中去除的邮件文件。该文件只在有被清除邮件的情况下才会出现。

表 11-2　邮件存储库目录说明

位置	内容 / 说明
/*userid*/store.sub	包含与用户订用情况有关的信息。
/*userid*/*nn*/	这是一个散列目录，其中含有 *msgid*.msg 格式的邮件，这里的 *nn* 可以是从 00 到 99 的任一数字。 例如，邮件 1 至 99 存储于 00 目录中，邮件 100 至 199 存储于 01 目录中，邮件 9990 至 9999 存储于 99 目录中，邮件 10000 至 10099 存储于 00 目录中，依此类推。

存储库如何清除邮件

存储库中邮件的清除分三步进行：

1. **删除（Delete）**。客户标记要删除的邮件。此时，客户程序可以通过移除“删除”记号，恢复此邮件。
2. **清除（Expunge）**。客户或指定的时限策略从邮箱中清除已有删除标记的邮件。邮件一旦被清除，客户就再也不能将之恢复，但这些邮件仍然存储在磁盘中。（已连接到同一邮箱的第二个客户仍然能够取出这些被清除邮件。）
3. **清理（Cleanup）**。用 stored 实用程序从磁盘中抹掉任何已清除至少一个小时的邮件。

还可以通过设置 **expire**（失效）选项清除邮件。服务器根据 configutil 定义的时限策略删除邮件。时间耗尽，邮件即被清除，但在清理之前它们并没有从物理上移除。（参阅第 274 页“指定时限策略”。）

指定管理员的存储库访问权限

邮件存储库管理员可以查看和监控用户邮箱并为邮件存储库指定访问控制。存储库管理员具有代理认证权限，可以访问任何服务（POP、IMAP、HTTP 或 SMTP），这意味着他们可用任何用户的权限，经认证访问任何服务。存储库管理员可通过这些权限运行某些实用程序来管理存储库。例如，存储库管理员可用 MoveUser 将用户的帐户和邮箱从一个系统移到另一个系统。

本节讨论如何为安装的 Messaging Server 系统赋予邮件存储库的存取权限。

备注　其他用户也可能拥有访问存储库所需的管理员权限。例如，若你处站点使用 Delegated Administration（DA）产品，顶层 DA 管理员在默认状态下具有对邮件系统中所有 Messaging Server 的存储权。而 DA 域管理员在默认状态下只具有其管辖域的存储权限。有关 DA 管理员的更多信息，参见 **iPlanet Messaging Server Provisioning Guide** 和 DA 文档。

可以执行如下段落所描述的任务：

- 添加管理员
- 修改管理员条目
- 删除管理员条目

可以用 `configutil` 命令或 Console 来指定管理员访问存储库的权限。

如果用 Console，请按下列步骤操作：

1. 从 Console 中打开需配置的 Messaging Server。
2. 单击 “配置”选项卡并选择左面板中的 “邮件存储库”。
3. 单击右面板中的 “管理员”选项卡。

添加管理员

Console 若需通过 Console 添加一个管理员条目，请按下列步骤操作：

1. 单击 “管理员”选项卡。

   选项卡中包含现有管理员 ID 的列表。
2. 单击 “管理员 UID”窗口旁边的 “添加”按钮。
3. 在 “管理员 UID”字段中键入要添加的管理员的用户 ID。

   您键入的用户 ID 必须是 iPlanet Directory Server 知道的用户标识。
4. 单击 “确定”将管理员 ID 添加到 “管理员”选项卡中显示的那个列表中。
5. 单击 “管理员”选项卡中的 “保存”按钮以保存新修改过的管理员列表。

命令行 若需通过命令行添加管理员条目，请输入下列命令行：

```
configutil -o store.admins -v "adminlist"
```

其中 *adminlist* 是一个以空格分隔的管理员 ID 列表。如果需指定多个管理员，必须用引号将列表括起来。

修改管理员条目

Console 若需通过 Console 修改邮件存储库 “管理员 UID”列表中现有的条目，请按下列步骤操作：

1. 单击 “管理员”选项卡。
2. 单击 “管理员 UID”窗口旁边的 “编辑”按钮。
3. 在 “管理员 UID”字段中输入改动。

4. 单击“确定”提交所做的改动并关闭“编辑管理员”窗口。
5. 单击“管理员”选项卡中的“保存”按钮以提交和保存修改的管理员列表。

命令行 若需通过命令行修改邮件存储库“管理员 UID”列表中现有的条目，请输入下列命令行：

```
configutil -o store.admins -v "adminlist"
```

删除管理员条目

Console 若需通过 Console 删除邮件存储库“管理员 UID”列表中的一个条目，请按下列步骤操作：

1. 单击“管理员”选项卡。
2. 选择“管理员 UID”列表中的一个条目。
3. 单击“删除”后即可删除该条目。
4. 单击“保存”按钮以提交和保存对管理员列表所做的改动。

命令行 若需通过命令行删除存储库管理员，可按如下方式编辑管理员列表：

```
configutil -o store.admins -v "adminlist"
```

关于邮件存储库空间配额

本节包含下列信息：

- 用户空间配额
- 域空间配额和家庭群组空间配额
- Telephony Application Server 的例外情况

用户空间配额

您可通过指定用户邮箱大小的限度来限制邮件存储库的大小。可指定的空间配额类型有下列：

- 磁盘空间配额可用于限制分配给每个用户的磁盘空间量。磁盘空间配额是针对所有用户邮件的总容量，而不管用户有多少邮件夹，也不管用户邮件的总数是多少。如果磁盘空间有限，则需设置用户磁盘空间配额。
- 邮件空间配额用于限制存储于用户邮箱中的邮件数量。

空间配额信息以 LDAP 属性和配置变量的形式存储。如果启用了空间配额管制功能，Messaging Server 则检查空间配额高速缓存和配置文件，以确保在将邮件插入到邮件存储库之前空间配额未超限。如果启用了空间配额通知功能，系统将在磁盘空间配额超限时向用户发送出错讯息。还可通过设置使服务器在用户接近配额限度时发送警告讯息。

既可为所有用户设置默认的空间配额，也可为单个用户单独设置空间配额。确定一用户是否超出空间配额时， Messaging Server 首先检查是否为该用户单独设置了空间配额。如果没有设置， Messaging Server 接着查看为所有用户设置的默认空间配额。

如果一个用户的邮件超过了配额，则来件保留在 MTA 队列中，直到以下情况之一出现：

（1）所有用户的邮件总量或总数不再超限，此时服务器将邮件传递给用户。（2）未传递的邮件保留在 MTA 队列中的时间长于指定的宽限期。请参阅第 273 页 “设置宽限期”。

当用户删除并擦去邮件，或当服务器根据已建立的时限策略删除邮件后，磁盘空间变为可用。

域空间配额和家庭群组空间配额

您还可为某一特定的域或某个域中的家庭群组设置空间配额。这两种空间配额是非强制性的，但可用于报告目的。

Telephony Application Server 的例外情况

为了支持统一的邮件传输要求， Messaging Server 提供为邮件存储库所利用的重设配额限制的能力。这可保证已被某些代理，即电话应用服务器 （TAS）接受了的邮件的传递。 TAS 所接收的邮件是通过特殊的 MTA 通道路由传输的，这就保证了无论是否超出空间配额限度邮件都能传递到存储库。有关配置 TAS 通道的详细情况，请参阅第 8 篇，“配置通道定义”。

配置邮件存储库空间配额

您可通过 iPlanet Console 或用 `configutil` 命令为所有用户设置默认的空间配额。也可为单个用户、家庭群组以及托管域设置空间配额。

本文说明如何设置默认空间配额。有关为单个用户、家庭群组以及域设置空间配额的详细信息，请参阅 **Delegated Administrator 用户指南**。

本节说明下列任务：

- 指定默认用户配额
- 启用空间配额管制和空间配额通知功能
- 设置宽限期

如果用 iPlanet Console，请按下列步骤操作：

1. 从 iPlanet Console 中打开需配置的 Messaging Server。
2. 单击 “配置”选项卡并选择左面板中的 “邮件存储库”。
3. 单击右面板中的 “空间配额”选项卡。

指定默认用户配额

默认空间配额适用于那些尚未为之单独设置空间配额的用户。为单独用户设置的空间配额将取代默认空间配额。

Console 通过 Console 指定默认空间配额：

1. 单击“空间配额”选项卡。
2. 若要为“默认用户磁盘配额”字段指定默认用户磁盘配额，请选择下列选项之一：

   无限（Unlimited）。如果不需要设置默认的空间配额，请选择此项。

   指定大小（Size specification）。如果需要将磁盘空间配额限定为指定的大小，请选择此项。在按钮旁的字段中键入一个数字，并从下拉列表中选择 MB（Mbytes，兆字节）或 KB（Kbytes，千字节）。
3. 若要在“默认用户邮件配额”复选框中指定邮件的配额数，请键入一个数字。
4. 单击“保存”。

命令行 若需为邮件总量指定一个默认的用户磁盘空间配额，请按下列步骤操作：

```
configutil -o store.defaultmailboxquota -v [ -1 | number ]
```

其中 `-1` 表示没有配额； *number* 表示字节数。

若需为总邮件数指定一个默认的用户空间配额，请按下列步骤操作：

```
configutil -o store.defaultmessagequota -v [ -1 | number ]
```

其中 `-1` 表示没有配额； *number* 表示邮件数。

启用空间配额管制和空间配额通知功能

您可通过设置启用或关闭空间配额管制和空间配额通知功能。服务器的操作取决于这两个配置变量是如何设置的，如表 11-3 所示。

表 11-3　空间配额管制和空间配额通知

	启用管制	关闭管制
启用通知	邮件将在指定的宽容限期内延缓传递，期满则拒收。邮件不能添加到邮箱中。	邮件被传递到存储库。邮件能够添加到邮箱中。
	IMAP SELECT、IMAP APPEND、SMTP 发送邮件机制和 deliver 命令将显示出错讯息。	IMAP SELECT、IMAP APPEND、SMTP 发送邮件机制和 deliver 命令不显示出错讯息。
关闭通知功能	邮件将在指定的宽容限期内延缓传递，期满则拒收。邮件不能添加到邮箱中。	邮件被传递到存储库。邮件能够添加到邮箱中。
	IMAP SELECT 命令、 deliver 命令以及 SMTP 发送邮件机制不显示出错讯息。 IMAP APPEND 命令将显示出错讯息。	IMAP SELECT、IMAP APPEND、SMTP 发送邮件机制和 deliver 命令不显示出错讯息。

启用空间配额管制功能

Console 通过 Console 启用空间配额管制功能：

1. 单击“空间配额”选项卡。
2. 选中“启用空间配额强制”复选框。

   此复选框为切换开关。需关闭空间配额通知功能时，取消此复选框的选中状态即可。
3. 单击“保存”。

命令行 通过命令行启用空间配额管制功能：

```
configutil -o store.quotaenforcement -v [ yes | no]
```

如果指定 no，空间配额不会强制实施。

启用空间配额通知功能

Console 通过 Console 启用空间配额通知功能：

1. 单击“空间配额”选项卡。
2. 选中“启用空间配额通知”复选框。

   此复选框为切换开关。需关闭空间配额通知功能时，取消此复选框的选中状态即可。
3. 定义配额警告讯息

   请参阅第 272 页“定义空间配额警告讯息”。
4. 单击“保存”。

命令行 通过命令行启用空间配额通知功能：

```
configutil -o store.quotanotification -v [ yes | no ]
configutil -o store.quotaexceededmsg -v message
```

如果没有设置邮件，则将没有配额警告讯息发送到用户。

定义空间配额警告讯息

可以像下面这样定义警告讯息，以便在用户超出其磁盘空间配额时发送给用户。警告讯息将发送到用户的邮箱。

Console 通过 Console 定义空间配额警告讯息：

1. 单击“空间配额”选项卡。
2. 从下拉列表中选择要使用的语言。
3. 在下拉表列下方的邮件文本字段中键入想要发送的邮件。
4. 单击“保存”。

命令行 通过命令行定义空间配额警告讯息：

```
configutil -o store.quotaexceededmsg -v message
```

其中的邮件必须是 RFC 822 格式。

定义警告讯息发送的频度：

```
configutil -o store.quotaexceedmsginterval -v number
```

其中 *number* 表示天数。例如， 3 的意思是每 3 天发送一次邮件。

指定空间配额阈值

通过指定一个空间配额阈值，可以在 IMAP 用户超过其磁盘空间配额之前向他们发送警告讯息。当某用户的磁盘用量超出指定的阈值时，服务器就向该用户发送一则警告讯息。

对于其客户机支持 IMAP ALERT 机制的 IMAP 用户，每当用户选择一个邮箱时，警告讯息就会显示在用户的屏幕上 （该邮件同时写入 IMAP 日志）。

Console 通过 Console 指定空间配额阈值：

1. 单击 “空间配额”选项卡。
2. 在 “空间配额警告阈值”字段，输入一警告阈数值。

   这个数字表示允许空间配额的百分比。例如，若指定 90%，该用户则在允许磁盘空间配额的 90% 被后得到警告。默认值为 90%。若需关闭此功能，输入 100%。
3. 单击 “保存”。

命令行 通过命令行指定空间配额阈值：

```
configutil -o store.quotawarn -v number
```

其中 *number* 表示允许配额的百分比。

设置宽限期

宽限期指定在邮件被退回到发件人之前，邮件可以超过配额 （磁盘空间或邮件数）的时间。邮件被 MTA 接受，但保留在 MTA 队列中，直到以下情况之一出现才会传递到邮件存储库：

- 在邮箱不再超过配额时，邮件即被传递到邮箱。
- 用户超配额地保留了比指定的宽限期更长的时间，此时服务器将退回包括在队列中的所有邮件。
- 邮件滞留在队列中的时间超过邮件最大排队时间。

例如，如果宽限期设置为两天，而超过配额的时间为一天，新邮件将继续被接收并滞留在队列中，并且传递尝试将继续。第二天后，邮件被退回。

备注	宽限期不是邮件将在队列中滞留的时间，而是在包括在队列中的那些邮件在内的所有来件被退回之前，邮箱超过配额的时间。

Console 通过 Console 设置邮件滞留于队列中的宽容限期：

1. 单击“空间配额”选项卡。
2. 在“超过空间配额宽限期”字段中，输入一个数字。
3. 从下拉列表中指定 `Day(s)` 或 `Hour(s)`。
4. 单击“保存”。

命令行 通过命令行指定空间配额宽容期限：

```
configutil -o store.quotagraceperiod -v number
```

其中 *number* 表示小时数。

指定时限策略

时限策略是另一种控制服务器磁盘用量的手段。可以控制邮件在一个或多个邮箱中的存储时间。如果磁盘空间很有限，则可能需要设置时限策略，以便从存储库中删除邮件。如果设置了时限策略，则应教育用户了解这些策略，因为服务器在将邮件从存储库中删除之前不会发送警告讯息。

可基于下列标准创建时限规则：

- 邮箱中的邮件数
- 邮箱总大小
- 邮件滞留于邮箱的天数
- 超出指定大小的邮件滞留于邮箱的天数

如果为一邮箱指定了多个规则，所有指定的期满删除规则都将适用，但最严格的规则先行。例如，假定将两条规则应用于一个邮箱。第一条规则允许 1000 封邮件；第二条规则允许 500 封邮件。当出现过期现象时，服务器将删除邮箱中的邮件，直到剩下 500 封为止。再举一个例子。若第一条规则允许邮件的大小为 100,000 字节并滞留 3 天，第二条规则允许邮件的大小为 1000 字节并滞留 12 天，则作为结果的规则是将这两条规则合并，允许邮件的大小为 100,000 字节，滞留 3 天。服务器将删除超过 100,000 字节且在邮箱中滞留了 3 天的所有邮件。对于特定的邮箱或邮箱组，如果想确保一个特定的规则是其唯一的规则，则须使用 Exclusive 参数。

Console 通过 Console 创建新规则：

1. 从 iPlanet Console 中打开需配置的 Messaging Server。
2. 单击“配置”选项卡并选择左面板中的“邮件存储库”。
3. 单击右面板中的“时限”选项卡。
4. 单击“添加”转到“添加规则”窗口。
5. 输入新规则的名称。

6. 指定此规则适用的目标文件夹。

   可以输入路径名、文件名或部分字串。可以按如下说明使用 IMAP 统配符：

   * - 匹配任何字符序列。
   % - 匹配任何除斜杠外的任何字符序列。

   新规则只适用于匹配所指定之模式的文件夹。

7. 如果此规则是适用目标文件夹的唯一规则，则单击 “专用”复选框。

8. 如果要创建基于文件夹大小的规则，请遵照下面的步骤：

   - 在“邮件计数”字段中，指定在最老的邮件被移除前在文件夹中滞留邮件的最大数量。
   - 在 “文件夹大小”字段中指定表示文件夹大小的数字；从相关连的下拉列表中选择 MB 或 KB。

   当超出指定的文件夹大小时，服务器将删除最老的邮件，直到该大小不再超出为止。

9. 如果要创建一个基于时限的规则，须在 “天数”字段指定一个数字，用以表示邮件滞留于文件夹的天数。

10. 如果要创建基于邮件大小的规则，请按下列步骤操作：

    - 在 “邮件大小限制”字段中输入一个数字，用以表示文件夹中允许的最大邮件大小；从相关连的下拉列表中选择 MB 或 KB。
    - 在 “宽限期”字段中，输入一个表示超过指定大小的邮件应该滞留在文件夹中时间的数字。

    过了宽容限期，服务器将删除那些超大邮件。

11. 单击 “确定”将新规则添加到 “时限规则”列表并关闭 “添加”窗口。

12. 单击 “保存”按钮以提交并保存现行的 “时限规则”列表。

命令行 通过命令行创建新规则须使用下面的命令，其中 *name* 是为规则取的名字：请注意，这里描述的仅仅是最经常使用的 `store.expire*` 选项。有关完整的列表，请参见 **iPlanet Messaging Server Reference Manual**。

指定此规则适用的目标文件夹时，请按下列操作：

```
configutil -o store.expirerule.name.folderpattern -v pattern
```

例如，模式 `user/*` 匹配任何文件夹；模式 `user/%@siroe.com/*` 匹配在 `siroe.com` 域中所有用户的全部文件夹；而模式 `user/%/Trash` 则匹配所有用户的 Trash 文件夹。

若需将此规则指定为适用于目标文件夹的唯一规则，请按下列操作：

```
configutil -o store.expirerule.name.exclusive -v [ yes | no ]
```

若需指定在最老的邮件被删除之前可滞留于文件夹中的邮件的最大数量，请按下列操作：

```
configutil -o store.expirerule.name.messagecount -v number
```

指定文件夹大小时，请按下列操作：

```
configutil -o store.expirerule.name.foldersizebytes -v number
```

其中 *number* 是字节的大小。

指定邮件时限时，请按下列操作：

```
configutil -o store.expirerule.name.messagedays -v number
```

其中 *number* 表示天数。

指定邮件大小时，请按下列操作：

```
configutil -o store.expirerule.name.messagesize -v number
```

其中 *number* 是字节的大小。

若需指定超大邮件可在文件夹中滞留的时间，请按下列操作：

```
configutil -o store.expirerule.name.messagesizedays -v number
```

其中 *number* 表示天数。

指定失效时间和天

指定失效时间和天：

```
configutil -o store.expirestart -v time （示例：23 是 11:00PM）
configutil -o local.store.expire.workday -v day （0-6， 0 是星期日）
```

将 `local.store.expire.workday` 设置为 -1 或大于 6 的值将禁用失效 / 清理。 `stored` 将每天在 `store.expirestart` 指定的时间检查此配置变量。如果没有设置 `local.store.expire.workday`，则默认为每天运行。在更改此变量后，不需要重新启动 `stored`。

配置邮件存储库分区

在默认状态下，所有用户邮箱储存在目录 `msg-`*instance*`/store/partition/` 中。目录 `partition` 是一逻辑目录，其中可包含一个或多个子分区。子分区可映射单个物理磁盘，也可映射多个物理磁盘。在启动时，目录 `partition` 中只包含一个子分区，称做 `primary` 分区。

必要时可将分区添加到 `partition` 目录中。例如，有可能需要按如下方式划分一个单独的磁盘来组织用户：

```
msg-instance/store/partition/mkting/
msg-instance/store/partition/eng/
msg-instance/store/partition/sales/
```

随着磁盘存储量的加，可能需要将这些分区映射到不同的磁盘驱动器。

应该限制任何一个磁盘中邮箱的数量。在多个磁盘上合理地分布邮箱可提高邮件传递时间（但并不改变 SMTP 的接收速率）。为每个磁盘分配多少邮箱数量取决于磁盘容量和分配给每个用户的磁盘空间大小。例如，为每个用户分配的磁盘空间越少，为每个磁盘分配的邮箱就可越多。

如果邮件存储库需要多个磁盘，可使用 RAID（冗余廉价磁盘阵列）技术以简化多磁盘管理。RAID 技术可将数据分布在一系列磁盘中，但这些磁盘以一个逻辑磁盘卷出现，因此简化了磁盘的管理。还可为冗余目的使用 RAID 技术，即为了故障恢复目的而对存储的数据进行备份。

备注 为改进磁盘存取速度，邮件存储库和邮件队列应驻留在不同的磁盘中。

添加分区

添加分区时，您须指定磁盘存储分区的绝对物理路径和称为分区别名的逻辑名。

您可通过分区别名将用户映射到一个逻辑分区名，而不管其具体的物理路径为何。在为用户设立帐户和指定邮件存储库时，可以使用这个分区别名。输入的别名必须是由字母数字组成的名字，而且必须是小写。

在创建和管理分区时，用于运行服务器的用户 ID 必须具有针对相应物理路径所指定位置的写入许可。

备注 添加一个分区后，必须停止并重新启动服务器，以刷新配置信息。

Console 通过 Console 添加存储库的分区：

1. 从 iPlanet Console 中打开需配置的 Messaging Server。
2. 单击“配置”选项卡并选择左面板中的“邮件存储库”。
3. 单击右面板中的“分区”选项卡。
4. 单击“添加”按钮。
5. 输入分区别名。

   这是指定分区的逻辑名。
6. 输入分区路径。

   这是指定分区的绝对路径名。
7. 若需将此分区指定为默认分区，单击标有“使之成为默认分区”的复选框。
8. 单击“确定”以提交此分区的配置条目并关闭窗口。
9. 单击“保存”以提交并保存当前分区列表。

命令行 通过命令行添加存储库的分区：

```
configutil -o store.partition.nickname.path -v path
```

这里的 *nickname* 是分区的逻辑名， *path* 是存储分区的绝对路径名。

指定默认主分区的路径时，请输入：

```
configutil -o store.partition.primary.path -v path
```

将邮箱移动到其他的磁盘分区

默认情况下，邮箱是在 primary 分区内创建的。如果分区已满，额外的邮件将不能被储存。有几种解决这一问题的方法：

- 减少用户邮箱的大小
- 如果正在使用容量管理软件，可添加其他的磁盘
- 创建其他分区 （第 277 页 “添加分区”）并将邮箱移动到新的分区

如果可能的话，我们推荐使用容量管理软件在系统上添加其他的磁盘，因为此过程对用户来说最为透明。不过，也可以使用下列方法将邮箱移动到其他的分区：

1. 请确认在迁移过程中，用户与其邮箱是断开的。为此，可以通过通知用户在邮箱迁移过程中注销并保持注销状态，或通过设置 mailAllowedServiceAccess 属性，使 POP，IMAP 和 HTTP 服务在其注销后不再允许访问。（参见 **iPlanet Messaging Server Provisioning Guide** 的 “Provisioning Users”一章）。

备注	将 mailAllowedServiceAccess 设置为不允许 POP， IMAP， HTTP 访问并不断开任何到邮箱的打开连接。必须确保移动邮箱前关闭所有连接。

2. 使用以下命令移动用户的邮箱：

   ```
   mboxutil -r user/<userid>/INBOX user/<userid>/INBOX <partition_name>
   ```

   示例：

   ```
   mboxutil -r user/ofanning/INBOX user/ofanning/INBOX secondary
   ```

3. 将被移动用户的 LDAP 条目中的 mailMessageStore 属性设置为新分区的名称。

   示例：

   ```
   mailMessageStore: secondary
   ```

4. 通知用户现在允许连接邮件存储库了。如果适用，更改 mailAllowedServiceAccess 的属性以允许 POP， IMAP 和 HTTP 服务。

维护和恢复作业

本节提供之信息与邮件存储库的维护和恢复任务所用的实用程序有关。应经常阅读 Postmaster 邮件以获知服务器可能发送的警告或报警信息。还应监视日志文件以了解服务器的运行状况。有关日志文件的详细信息，请参阅第 13 篇，“日志记录和日志分析”。

本节包含以下内容：

- 管理邮箱
- 监视配额限制
- 监控磁盘空间

- 使用 stored 实用程序
- 修复邮箱和邮箱数据库

管理邮箱

本节说明下列管理和监控邮箱的实用程序：`mboxutil`、 `hashdir`、 `readership`。

mboxutil 实用程序

`mboxutil` 命令用于执行各种典型的邮箱维护任务。这些任务包括：

- 列示邮箱
- 创建邮箱
- 删除邮箱
- 重命名邮箱
- 将邮箱从一个分区移到另一个分区

也可用 `mboxutil` 命令查看有关空间配额方面的信息。有关详细信息，请参阅第 281 页 “监视配额限制”。

表 11-4 中列示了 mboxutil 命令的选项。有关详细的语法和使用要求，请参见 **iPlanet Messaging Server Reference Manual**。

表 11-4 `mboxutil` 选项

选项	说明
`-a`	列示所有用户空间配额信息。
`-c` *mailbox*	创建指定的邮箱。
`-d` *mailbox*	删除指定的邮箱
`-f` *file*	创建，删除或锁定指定数据文件中所列出的一个或多个邮箱。
`-g` *group*	列示指定组的空间配额信息。
`-k` *mailbox cmd*	在文件夹级锁定指定的邮箱，然后执行指定的命令，命令完成后解除锁定。
`-l`	列出服务器中的所有邮箱。
`-p` *pattern*	当与 `-l` 选项结合使用时，只列示其名字与 *pattern* 相匹配的那些邮箱。可使用 IMAP 通配符。
`-q` *domain*	列示指定域的空间配额信息。

表 11-4　mboxutil 选项（接上页）

选项	说明
-r *oldname newname* [*partition*]	邮箱名从 *oldname* 更改为 *newname*。若需将一个文件夹从一个分区移到另一个分区，请用 *partition* 选项。 此选项可用于重命名一个用户。例如， `mboxutil -r user/user1/INBOX user/user2/INBOX` 将 user1 的所有邮件和邮箱移动到 user2，新的邮件将在新的收件箱中出现。（如果 user2 已经存在，此操作将失败）。
-u *user*	列示诸如邮件存储库当前大小、空间配额 （如果设置了的话）、当前使用的空间配额百分比等用户信息。
-x	与 -l 选项结合使用时，显示邮箱的路径和访问控制。

邮箱命名约定

必须按下面的格式指定邮箱名：user/*userid*/*mailbox*，这里的 *userid* 标识拥有邮箱的用户，*mailbox* 即邮箱的名字。对于托管域， *userid* 为 *uid@domain*。

例如，下面的命令可用于创建名为 INBOX 的邮箱，其用户 ID 是 crowe。对于传递到用户 crowe。的邮件， INBOX 是默认邮箱。

```
mboxutil -c user/crowe/INBOX
```

重要提示：这个 INBOX 名字是保留名，作为每个用户的默认邮箱名。 INBOX 是唯一无需区分大小写的文件夹名。其他文件夹名都须区分大小写。

范例

列示所有用户的所有邮箱：

```
mboxutil -l
```

列示所有邮箱并包含路径和 ACL 信息：

```
mboxutil -l -x
```

为用户 daphne 创建名为 INBOX 的默认邮箱：

```
mboxutil -c user/daphne/INBOX
```

删除用户 delilah 的名为 projx 的邮件夹：

```
mboxutil -d user/delilah/projx
```

删除用户 druscilla 的名为 INBOX 的默认邮箱以及*所有邮件夹*：

```
mboxutil -d user/druscilla/INBOX
```

将用户 desdemona 的邮件夹 memos 更名为 memos-april：

```
mboxutil -r user/desdemona/memos user/desdemona/memos-april
```

锁定用户 dulcinea 的名为 legal 的邮件夹：

```
mboxutil -k user/dulcinea/legal cmd
```

这里的 *cmd* 是希望在文件夹被锁定过程中执行的命令。

将用户 dimitria 的邮件帐户移到一个新分区：

```
mboxutil -r user/dimitria/INBOX user/dimitria/INBOX partition
```

其中 *partition* 指定新分区的名称。

将用户 dimitria 的名为 personal 的邮件夹移到一个新分区：

```
mboxutil -r user/dimitria/personal user/dimitria/personal partition
```

hashdir 实用程序

邮件存储库中的邮箱存储为散列结构以利于快速搜索。因此，寻找包含特定用户的邮箱时，须使用 hashdir 实用程序。

用此实用程序可确定包含特定帐户的邮件存储库的目录。此实用程序报告通往邮件存储库的相对路径，诸如 d1/a7/。路径是相对于基于用户 ID 上一层的目录的。实用程序将路径信息发送到标准输出。

例如，要寻找到用户 crowe 邮箱的相对路径，可输入：

```
hashdir crowe
```

Readership 实用程序

Readership 实用程序可用来报告除邮箱所有者外还有多少用户阅读了共享 IMAP 文件夹中的邮件。

IMAP 文件夹的所有者可准许其他用户阅读该文件夹中的邮件。一个允许其他用户访问的文件夹称为*共享文件夹*。管理员可用 readership 实用程序了解除文件夹所有者外其他用户访问共享文件夹的情况，如访问人数。

此实用程序可用来扫描所有邮箱并为每个共享文件夹产生一行输出，报告读者数，后跟一个空格，然后是邮箱名。

在已过去的指定天数内选择了共享文件夹的每个用户具有独自的认证身份。阅读其个人邮箱的用户并不计算在内。除非除文件夹所有者外至少还有另外一个读者，否则报告中不包括个人邮箱查阅方面的信息。

例如，下面的命令把任何具有在最近的 15 天内选择了共享 IMAP 文件夹的用户统计为读者：

```
readership -d 15
```

监视配额限制

您可通过 mboxutil 实用程序监控空间配额的使用和限制情况。 mboxutil 实用程序可生成一份报告，列示任何已定义的空间配额和限制情况，并提供空间配额使用量方面的信息。报告中的空间配额及其使用量以千字节为单位。

例如，下面的命令列示所有用户的空间配额信息：

```
mboxutil -a
```

接下来的例子列示用户 crowe 的空间配额信息：

```
mboxutil -u crowe
```

接下来的例子列示 siroe.com 域的空间配额信息：

```
mboxutil -q siroe.com
```

监控磁盘空间

您可指定系统监控磁盘空间的频次，以及何种情况下系统发送警告信息。配置磁盘空间监控和通知功能时，请用 configutil 命令设置报警属性，方法见表 11-5 中的描述。

表 11-5　磁盘空间报警属性

磁盘空间属性	默认值
alarm.diskavail.msgalarmstatinterval	3600 秒
alarm.diskavail.msgalarmthreshold	10%
alarm.diskavail.msgalarmwarninginterval	24 小时

例如，若要系统每 600 秒监控一次磁盘空间，则指定用下面的命令：

```
configutil -o alarm.diskavail.msgalarmstatinterval -v 600
```

如果每当可用磁盘空间低于 20% 时都希望收到警告信息，则指定使用下面的命令：

```
configutil -o alarm.diskavail.msgalarmthreshold -v 20
```

有关设置警告属性的更多信息，请参见 **iPlanet Messaging Server Reference Manual** 和第 387 页 “监控磁盘空间”。

使用 stored 实用程序

stored 实用程序可在服务器上执行下列监控和维护任务：

- 后台及日常邮件传输任务。
- 死锁检测和死锁的数据库事务的重算。
- 启动时清理临时文件。
- 执行时限策略。
- 周期性监控服务器状态、磁盘空间、服务器响应时间等 （参阅第 394 页 “stored”）。
- 必要时发布报警。

stored 实用程序可自动于每天半夜执行清理和期满检测操作。可以选择进一步的清理和期满检测操作。

表 11-6 列示了 stored 的选项。表后列有几个常见用法的例子。有关详细的语法和使用要求，请参见 **iPlanet Messaging Server Reference Manual**。

表 11-6　stored 选项

选项	说明
-c	执行一次性的清理任务，删掉已清除邮件。运行一次，然后退出。 -c 选项是一次性的操作，因此无须指定 -1 选项。
-d	作为守护程序运行。执行系统检查并启动报警、死锁检测以及数据库修复。
-1	运行一次，然后退出。
-n	仅以试运行模式运行。并不真正对邮件进行时限或清理处理。运行一次，然后退出。
-v	详细输出。
-v -v	更详细的输出。

测试期满失效策略：

```
stored -n
```

执行一次性的时限和清理任务：

```
stored -l -v
```

如果要更改自动清理和期满失效操作的时间，须按下面的方式使用 configutil 实用程序：

```
configutil -o store.expirestart -v 21
```

偶尔也可能需要重启动 stored 实用程序，例如，当邮箱列表数据库损坏的时候。通过 UNIX 命令行重启动 stored 时，须使用下列命令：

server-root/msg-*instance*/stop-msg store
server-root/msg-*instance*/start-msg store

如果任何服务器守护程序出现崩溃，则须停止并重新启动包括 stored 在内的所有守护程序。

修复邮箱和邮箱数据库

如果一个或多个邮箱出现损坏现象，可用 reconstruct 实用程序重建邮箱或邮箱数据库，并修复任何不一致之处。

实用程序 reconstruct 可用来重建一个或多个邮箱，或主邮箱文件，修复任何不一致之处。可用此实用程序复原邮件存储库中的几乎任何形式的数据损坏。注意，低层的数据库修复（如完成的事务和重算未完成事务等）是通过 stored -d 进行的。

表 11-7 列示了 reconstruct 可用的各种选项。有关详细的语法和使用要求，请参见 **iPlanet Messaging Server Reference Manual**。

表 11-7　reconstruct 选项

选项	说明
-f	强制 reconstruct 针对一个或多个邮箱执行修正。
-m	修理并执行邮箱数据库的一致性检查。此选项检查在假脱机缓冲区找到的每个邮箱，适当地在邮箱数据库中添加或移除条目。每当在邮箱数据库中添加或删除条目时，就向标准输出文件输送可打印的邮件。
-n	只检查邮件存储库，不对一个或多个邮箱执行修正。 -n 选项不能被自己使用，除非提供一个邮箱名。在没有提供邮箱名的情况下， -n 选项必须与 -r 选项一起使用， -r 选项可以与 -p 选项相结合。例如，以下命令都是有效的： reconstruct -n user/dulcinea/INBOX reconstruct -n -r reconstruct -n -r -p primary reconstruct -n -r user/dulcinea/
-o	检查确定无主帐户。在当前 Messaging Server 主机中搜索在 LDAP 中没有对应条目的收件箱。例如， -o 选项可以发现已从 LDAP 删除或已移到另一个服务器主机中的收件箱所有者。对于所发现的每一个无主帐户，reconstruct 将把下面的命令写到标准输出中： mboxutil-d user/*userid*/INBOX
-o -d*filename*	如果 -d*filename* 指定有 -o 选项， reconstruct 则打开指定的文件并将 mboxutil -d 命令写入该文件。该文件随即可变为成为脚本文件，用于删除无主帐户。
-p *partition*	指定一个分区名，不使用全路径名。如果没有指定此选项， reconstruct 对所有分区都是默认的。
-q	修正配额系统中的任何不一致性，如邮箱带有错误配额根，或配额根带有错误的配额使用报告。 -q 选项在其他服务器进程运行时可以运行。
-r [*mailbox*]	对指定的一个或多个邮箱的分区进行修理并执行一致性检查。 -r 选项对指定邮箱内的所有子邮箱进行修理。如果指定 -r 时没有加带 “邮箱” 参数，实用程序则在必要时修复数据库中所有邮箱的假脱机缓冲区。

重建邮箱

重建邮箱时，请用 -r 选项。应该在下列情况下使用此选项：

- 访问邮箱时返回下面错误之一："System I/O error" or "Mailbox has an invalid format"。
- 访问邮箱时致使服务器崩溃。
- 文件已添加到假脱机目录，或从该目录删除。

5.0 版的 reconstruct -r 实用程序首先执行一致性检查。然后报告一致性情况并只在检测到问题时进行重建。因此在本版中 reconstruct 实用程序的执行已得到改善。

可以像下面例子所描述的那样使用 reconstruct：

若需重建用户 daphne 邮箱的假脱机缓冲区，请使用下面的命令：

```
reconstruct -r user/daphne
```

若需重建邮箱数据库中所有邮箱的假脱机缓冲区，请使用下面的命令：

```
reconstruct -r
```

但使用此选项时要谨慎，因为对于较大的邮件存储库，重建邮箱数据库中的所有邮箱的假脱机缓冲区需要花很长的时间。（参阅第 286 页“reconstruct 的操作性能”。）故障恢复的更好的方法是利用多个磁盘构建存储库。如果其中一个磁盘出了问题，不会影响整个存储库。如果某一磁盘损坏，只需像下例所示用 -p 选项重建存储库的一部分：

```
reconstruct -r -p subpartition
```

若需重建命令行参数中列示的邮箱 （但只有当其在 primary 分区中时），请输入下列：

```
reconstruct -p primary mbox1 mbox2 mbox3
```

如果确实需要重建所有的 primary 分区中的邮箱，请输入下列：

```
reconstruct -r -p primary
```

如果需强制 reconstruct 在不进行一致性检查的情况下重建文件夹，则须用 -f 选项。例如，下面的命令将强制重建用户文件夹 daphne：

```
reconstruct -f -r user/daphne
```

若需在不加以修正的情况下检查所有邮箱，可按下面的例子使用 -n 选项：

```
reconstruct -r -n
```

检查和修复邮箱

若需对邮箱数据库进行高层次的一致性检查并修复，请输入下列：

```
reconstruct -m
```

在下列情况下应使用 -m 选项：

- 从存储库假脱机缓冲区中删除了一个或多个目录，因此邮箱数据库条目也需删除。
- 一个或多个目录已恢复到存储库假脱机缓冲区中，因此邮箱数据库条目也需添加。

- `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，应按所示顺序执行下列步骤：

  - 关闭所有服务器。
  - 删除 *server-root*`/msg-`*instance*`/store/mboxlist` 中的所有文件。
  - 重新开始服务器进程。
  - 运行 `reconstruct -m`，依据假脱机缓冲区中的内容新建一个邮箱数据库。

移除无主帐户

搜寻无主帐户 （无主帐户即在 LDAP 中没有对应条目的邮箱）时，请输入：

```
reconstruct -o
```

命令的输出如下：

```
reconstruct: Start checking for orphaned mailboxes
mboxutil -d user/test/annie/INBOX
mboxutil -d user/test/oliver/INBOX
reconstruct: Found 2 orphaned mailbox(es)
reconstruct: Done checking for orphaned mailboxes
```

若需创建一个列示无主邮箱的名为 `orphans.cmd` 的文件 （该文件可转换为删除无主邮箱的脚本文件），请输入：

```
reconstruct -o -d orphans.cmd
```

命令的输出如下：

```
reconstruct: Start checking for orphaned mailboxes
reconstruct: Found 2 orphaned mailbox(es)
reconstruct: Done checking for orphaned mailboxes
```

reconstruct 的操作性能

`reconstruct` 一次操作所需的时间取决于若干因素，其中包括：

- 操作的种类及所选择的选项
- 磁盘性能
- 运行 `reconstruct -m` 时文件夹的数量
- 运行 `reconstruct -r` 时邮件的数量

- 邮件存储库的总容量
- 系统是否在运行其他进程以及系统的繁忙程度
- 是否有正在进行的 POP、 IMAP、 HTTP 或 SMTP 活动

`reconstruct -r` 选项首先进行一致性检查；此次检查可改善 `reconstruct` 的操作性能；操作性能的改善程度取决于须重建的文件夹数量。

举例来说，假定有大约 2400 个用户，一个 85GB 的邮件存储库，服务器中有并行的 POP、IMAP 或 SMTP 活动：

- `reconstruct -m` 需 1 小时
- `reconstruct -r -f` 需 18 小时

备注 如果服务器中没有正在进行的 POP、 IMAP、 HTTP 或 SMTP 活动，`reconstruct` 操作可能需要相当少的时间。

备份与恢复邮件存储库

备份与恢复是最常见、最重要的管理任务之一。必须为邮件存储库实施一套备份与恢复策略以确保出现问题时数据不致丢失；可能出现的问题包括：

- 将用户邮箱从一个服务器移动到另一个服务器
- 系统崩溃
- 硬件故障
- 意外地删除了邮件或邮箱
- 重新安装系统或升级时出现的问题
- 自然灾害 （例如，地震、火灾、飓风等）

在迁移用户时也需要备份数据。

Messaging Server 提供的命令行实用程序可用于备份和恢复邮件存储库。Messaging Server 还提供了一种与 Legato Networker 集成的解决方案。

Messaging Server 采用单副本备份方法。无论有多少包含特定邮件的用户文件夹，在备份过程中，邮件文件只备份一次，即所找到的第一个邮件文件。第二个邮件副本被备份为通往第一个邮件文件名的链接，其他类似。`backup` 实用程序以邮件文件的索引节或信息节点（inode）作为索引，将所有邮件列于一个散列表。但在恢复数据时，此方法会使操作复杂化。有关详细信息，请参阅第 290 页 “关于部分恢复的考虑”。

本节包含下列内容：

- 创建备份策略
- 创建备份组
- Messaging Server 备份和恢复实用程序
- 关于部分恢复的考虑
- 使用 Legato Networker

创建备份策略

建立备份策略时，需考虑到若干因素，诸如：

- 业务负载高峰
- 完整备份和递增备份
- 并行备份和串行备份

业务负载高峰

在为系统规划备份时需考虑到业务负载高峰这一因素。例如，备份最好安排在凌晨，如上午 2:00。

完整备份和递增备份

递增备份法可先扫描存储库以搜寻变更数据并只备份变更的数据。完整备份法则备份整个邮件存储库。需确定系统进行完整备份相对于递增备份的频次。可将递增备份作为每日维护作业加以实施。在需要移动或迁移数据时，进行完整备份是适宜的。

并行备份和串行备份

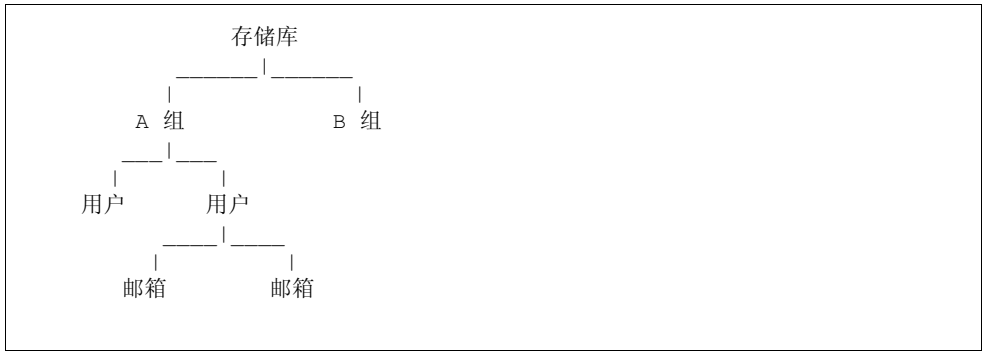
当用户数据存储于多个磁盘时，可选择以并行方法备份用户组。并行备份方法从总体上可加速备份过程，具体指标取决于系统资源。但也有需要串行备份的时候，例如，在不想影响服务器性能时。是用并行备份还是用串行备份取决于多方面的因素，如系统负载、硬件配置、可用的磁带机数量等等。

创建备份组

通过将用户划分为若干组，可改善备份管理。例如，可以为每个组分别指定备份作业时段。也可以选择以并行方式同时备份若干组。

假定用户邮件按用户的姓氏安排存储，字头为 A 的所有用户的邮件归为一个备份组，字头为 B 的所有用户的邮件归为另一个备份组。

邮件存储库的逻辑图可按下列划分：



通过将用户划分为若干组，可改善备份管理。例如，可以为每个组分别指定备份作业时段。也可以选择以并行方式同时备份若干组。有关创建备份组方面的详细信息，请参阅第 288 页“创建备份组”。

若需创建备份组，则要创建一个配置文件以存储组定义。该文件必须命名为 `backup-groups.conf` 而且必须存储在下列目录中：

server_root`/msg-`*instance*`/config/backup-groups.conf`

该文件的格式是：

```
groups=definitions
groups=definitions
.
.
.
```

例如，若将用户按用户 ID 的首字母分组，可用如下的定义：

```
groupA=a*
groupB=b*
groupC=c*
```

备份对象的命名采用如下的邮件存储库逻辑结构：

/server/group/user/mailbox

其中 *server* 是邮件存储库实例名。例如：siroe

Messaging Server 包含一个预定义备份组，可在没有创建配置文件 backup-groups 情况下使用。这个组称为 ALL，包含所有用户。

Messaging Server 备份和恢复实用程序

为了备份和恢复数据，可用 Messaging Server 提供的 imsbackup 和 imsrestore 两种实用程序。

请注意， imsbackup 和 imsrestore 这两种实用程序并不提供通用备份功能。这两种实用程序不具备 Legato Networker 这样的通用工具所具备的一些高级特性。例如，这两种实用程序只向自动换带机提供非常有限的支持。不能将单一的存储库写入多个并行设备中。要获得完善的备份功能须用如 Legato Networker 这样的通用化的外挂工具。有关 Legato Networker 的使用方面的详细信息，请参阅第 292 页 “使用 Legato Networker”。

imsbackup 实用程序

您可通过 imsbackup 实用程序将邮件存储库中选取的内容写到任何串行设备中，其中包括磁带、 UNIX 管道、无格式文件等。备份或备份中选取的部分可在以后用 imsrestore 实用程序恢复。 imsbackup 的输出可通过管道送往 imsrestore。

进行备份作业时，可按下例使用 imsbackup 命令，例中将 user1 备份到 backupfile：

```
imsbackup -f backupfile /mystore/ALL/user1
```

此命令采用默认的块因子 20。有关 imsbackup 命令的完整语法描述，请参阅 **iPlanet Messaging Server Reference Manual**。

imsrestore 实用程序

从备份设备中恢复备份数据时，可用 imsrestore 命令。例如，下面的命令可为 user1 从文件 backupfile 中恢复邮件。

```
imsrestore -f backupfile /mystore/ALL/user1
```

有关 imsbackup 命令的完整语法描述，参见 **iPlanet Messaging Server Reference Manual**。

关于部分恢复的考虑

这种单副本备份方法在恢复邮件时有下列需注意的地方：

- **完整恢复。**在完整恢复过程中，链接的邮件将继续指向它们所连接的邮件文件的同一信息节点上。
- **部分备份/恢复。**而在部分备份和部分恢复过程中，邮件存储库的单副本特性可能无法得到保持。

假定有三个邮件分别属于三个用户 A、 B 和 C，如下所示：

A/INBOX/1
B/INBOX/1
C/INBOX/1

例 1：在第一个例子中，系统执行一个部分备份和完整恢复作业，过程如下：

1. 备份用户 B 和 C。
2. 删除用户 B 和 C。
3. 从步骤 1 恢复备份数据。

在这个例子中， B/INBOX/1 和 C/INBOX/1 被赋予一个新的信息节点号，邮件数据写入磁盘中的一个新位置。仅有一个邮件副本被恢复，第二个邮件只是到第一个邮件的硬链接。

例 2：在这个例子中，系统执行完整备份和部分恢复，过程如下：

1. 执行完整备份。
2. 删除用户 A。
3. 恢复用户 A。

A/INBOX/1 被赋予一个新的信息节点号。

例 3：在这个例子中，部分恢复可能要尝试多次：

1. 执行完整备份。

   B/INBOX/1 和 C/INBOX/1 被备份为到 A/INBOX/1 的链接。
2. 删除用户 A 和 B。
3. 恢复用户 B。

   恢复实用程序请求管理员首先恢复 A/INBOX。
4. 恢复用户 A 和 B。
5. 删除用户 A （可选）。

备注 如果想确保所有邮件都以部分恢复方式恢复，可在运行 `imsbackup` 时使用 `-i` 选项。`-i` 选项使得必要时每个邮件可备份多次。此选项在 POP 环境下最有用。

使用 Legato Networker

Messaging Server 包含一个备份 API，可用来提供如 Legato Networker 这样的第三方备份工具的接口。邮件存储库的物理结构和数据格式被封装在备份 API 中。备份 API 与邮件存储库直接交互，为备份服务提供邮件存储库的逻辑界面。备份服务以邮件存储库的概念显示方式存储和检索备份对象。

Messaging Server 提供的 Application Specific Module （ASM）可被 Legato Networker 的 `save` 和 `recover` 命令调用，以便备份和恢复邮件存储库数据。 ASM 接着调用实用程序 Messaging Server `imsbackup` 和 `imsrestore`。

备注 本节提供的信息涉及如何将 Legato Networker 用于 Messaging Server 邮件存储库。有关 Legato Networker 界面方面的说明，请参阅 Legato 文挡。

用 Legato Networker 备份数据

在用 Legato Networker 对 Messaging Server 邮件存储库进行备份时，在援用 Legato 界面之前必须执行以下准备步骤：

1. 创建一个从 `usr/lib/nsr/imsasm` 到 *serverRoot*`/msg-`*instance*`/bin/imsasm` 的象征性的链接。
2. 从 Sun 或 Legato 处索取一份二进制文件 `nsrfile` 的副本并将之复制到下面的目录中：

   `/usr/lib/nsr/nsrfile`
3. 如果按组备份用户，请执行以下步骤：
   a. 遵照第 288 页 “创建备份组”中的说明创建备份组文件。
   b. 若需检查所做的配置，请运行 `mkbackupdir.sh`。

      查看在 *server_root*`/backup` 中的目录结构。该结构应与图 11-2 中展示的结构类似。

   注意，如果没有指定 `backup-groups.conf` 文件，备份进程将对所有用户使用默认的备份组 `ALL`。
4. 在目录 `/nsr/res/` 中为保存组创建一个 `res` 文件，以便在备份前调用脚本 `mkbackupdir.sh`。请见图 11-3 中的范例。

备注 Legato Networker 具有 64 个字符限制的保存集名称。默认情况下，`mkbackupdir.sh` 将在 *server_root*`/backup` 目录下创建存储映像。如果此目录名加上邮箱的逻辑名 （例如， `siroe/groupA/fred`）大于 64 个字符，则必须运行 `mkbackupdir.sh -p`。因此，应该为 `mkbackupdir.sh` 的 `-p` 选项使用一个短路径名。例如，下列命令将在 `/backup` 目录下创建备份映像：

`mkbackupdir.sh -p /backup`

重要提示：备份目录对于邮件存储库所有者必须是可写的（例如：`mailsrv`）。

图 11-2 所示为备份组目录结构的一个样板。

图 11-2 备份组目录结构

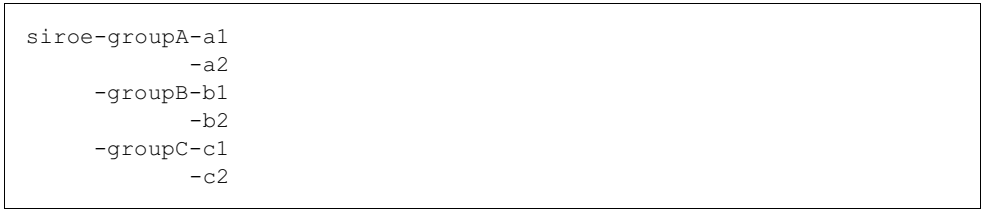


图 11-3 所示为一个在 /nsr/res 目录中的名为 IMS.res 的示例性 res 文件：

图 11-3 res 文件样板

```
type: savepnpc
precmd: "echo mkbackupdir started",
   "/usr/siroe/server5/msg-siroe/bin/mkbackupdir.sh -p /backup"
pstcmd: "echo imsbackup Completed";
timeout: "12:00 pm";
```

现在准备好按下面的步骤运行 Legato Networker 界面：

1. 如有必要，则先创建 Messaging Server 保存组。
   a. 然后运行 nwadmin。
   b. 选择 Customize | Group | Create。
2. 将 savepnpc 用作备份命令以创建一个备份客户：
   a. 将保存集设置为由 mkbackupdir 所创建的目录。

      对单一任务备份，请使用 *server_root*/backup

      对于平行备份，请使用 *server_root*/backup/*server*/*group*

      检查是否已经按第 288 页 “创建备份组”中的定义创建了 *group*。

      还必须按照备份作业时段数设置并行性。

      请参阅第 294 页 “范例：在 Networker 中创建备份客户”。

3. 选取 Group Control | Start 以测试备份配置。

范例：在 Networker 中创建备份客户 在 Networker 中创建备份客户时，从 `nwadmin` 中选择 Client | Client Setup | Create：

```
Name: siroe
Group: IMS
Savesets:/backup/siroe/groupA
   /backup/siroe/groupB
   /backup/gotmail/groupC
         .
         .
Backup Command:savepnpc
Parallelism: 4
```

用 Legato Networker 恢复数据

恢复数据时，可用 Legato Networker 的 `nwrecover` 界面或命令行实用程序 `recover`。下面的例子可用来恢复用户 a1 的 INBOX：

```
recover -a -f -s siroe /backup/siroe/groupA/a1/INBOX
```

接下来的例子可用来恢复整个邮件存储库：

```
recover -a -f -s siroe /backup/siroe
```

使用第三方备份软件 （Legato 除外）

iPlanet Messaging Server 提供两个存储库备份解决方案，命令行 `imsbackup` 和 Solstice Backup （Legato Networker）。对于大型邮件存储库，通过一次运行 `imbackup` 来备份整个邮件存储库会花费相当长的时间。 Legato 解决方案支持在多个备份设备上的并行备份会话。并行备份可以大大缩短备份时间 （已达到每小时备份 25 GB 的数据）。

如果使用另一个第三方并行备份软件（如，Netbackup），可以使用以下的方法将备份软件与 iPlanet Messaging Server 相整合。

1. 将用户分为若干组 （参见第 288 页 “创建备份组”）并在 *server_root*`/msg-<instance>/config/` 目录下创建 `backup-groups.conf` 文件。

   例如，对于 UID 标识的组用户，使用在 `/usr/iplanet/server5/msg-siroe/config/backup-groups.conf` 中的以下定义：

   ```
   groupA=a*
   groupB=b*
   groupC=c*
   . . .
   ```

备注	此备份解决方案要求更多的磁盘空间。为了并行备份所有的组，所要求的磁盘空间是邮件存储库空间的 2 倍。如果没有如此多的磁盘空间，可将用户分成更小的组，然后一次备份一批用户组。例如，组 1 - 组 5，组 6 - 组 10。备份后移除这些组数据文件。

2. 运行 `imsbackup` 将每个用户组备份到分段区下的文件中。

   命令格式是 `imsbackup -f <device> /<instance>/<group>`

   可以同时运行多个 `imsbackup` 进程。例如：

   ```
   # imsbackup -f- /siroe/groupA > /bkdata/groupA &
   # imsbackup -f- /siroe/groupB > /bkdata/groupB &
   ...
   ```

   `imsbackup` 不支持大型文件，如果备份数据大于 2 GB，就需要使用 `-f-` 选项以将数据写到 `stdout`（标准输出），然后使用管道输出到文件。

3. 使用第三方软件备份在分段区的组数据文件（在我们的例子中是 `/bkdata`）。

4. 若要恢复一个用户，请确定该用户的组文件名，从磁带上恢复该文件，然后使用 `imsrestore` 从数据文件中恢复该用户。

   请注意 `imsrestore` 不支持大型文件。如果数据文件大于 2 GB。请使用以下命令：

   ```
   # cat /bkdata/groupA | imsrestore -f- /siroe/groupA/andy
   ```

对邮件存储库进行故障诊断

本节提供对邮件存储库进行预见性维护的指导方针。此外，本节还描述在邮件存储库受损或意外关闭的情况下，可以使用的其他邮件存储库恢复程序。注意，本节关于其他邮件存储库恢复程序是对第 283 页 “修复邮箱和邮箱数据库”的扩充。

在阅读本节之前，强烈建议回顾本章和命令行实用程序以及 **iPlanet Messaging Server Reference Manual** 中的 `configutil` 各章。本章包含以下主题：

- 标准邮件存储库监控程序
- 常见问题和解决办法
- 邮件存储库恢复程序

标准邮件存储库监控程序

本节简述邮件存储库的标准监控程序。这些程序对于例行检查，测试和标准维护很有帮助。

有关详细信息，请参阅第 393 页 “监控邮件存储库”。

检查硬件空间

邮件存储库应具有足够的额外磁盘空间和硬件资源。当邮件存储库的接近磁盘空间和硬件空间的最大限额时，可能会在邮件存储库内产生问题。

磁盘空间不足是造成邮件服务器问题和失败的最常见的问题之一。如果邮件存储库没有要写的空间，邮件服务器将失败。另外，当可用的磁盘空间低于某阈值后，将出现与邮件传递、登录等等相关联的问题。当 stored 进程的清理功能失效，被删除的邮件不能从邮件存储库擦去时，磁盘空间可被迅速地耗尽。

有关监控磁盘空间的信息，请参见第 282 页“监控磁盘空间”和第 393 页“监控邮件存储库”。

检查日志文件

检查日志文件以确认邮件存储库进程是按照配置运行的。 Messaging Server 为每个主要协议或服务单独创建一批日志文件，所支持的协议或服务有：SMTP，IMAP，POP 和 HTTP。可以通过 Console 或在目录 *server-root*/msg-*instance*/log/ 中查看这些日志文件。日志文件的监控应当例行化。

应当意识到，日志记录会对服务器的性能产生影响。定义的日志记录越详细，在给定时间量内日志文件所占用的磁盘空间就越大。应对服务器定义有效而现实的日志记录轮换、失效和备份策略。有关对服务器定义日志记录策略的信息，参见第 13 篇，“日志记录和日志分析”。

检查 stored 进程

stored 功能执行多种重要任务，诸如邮件数据库的死锁和事务操作，强制时限策略，以及清除储存在磁盘上的邮件等。如果 stored 停止运行，则 Messaging Server 将最终陷入问题。如果 stored 在 start-msg 已运行后仍不启动，则其他进程将不能启动。

- 请检查确认 stored 进程正在运行。 pid 文件是由 stored（*server-root*/msg-*instance*/config/store.pid）创建和更新的。
- 每当 stored 进程试图实施以下功能之一时，请检查确认下列文件的时间戳（在 *server-root*/msg-*instance*/config/ 目录中）已更新：

表 11-8 stored 操作

储存操作	功能
stored.ckp	当启动一数据库检查点时被触及 （touched）。大约每 1 分钟打一次时间戳。
stored.lcu	每次数据库日志记录清理时被触及。大约每 5 分钟打一次时间戳。
stored.per	当根每次生成逐用户 db 写出时被触及。每小时打一次时间戳。

- 检查在 *server-root*/msg-*instance*/store/mailboxlist 中构建的日志文件。
- 检查在默认日志文件 *server-root*/msg-*instance*/log/default/default 中的 stored 邮件。

有关 stored 进程的更多信息，请参见第 282 页 “使用 stored 实用程序”和 **iPlanet Messaging Server Reference Manual** 的 “Messaging Server 命令行实用程序”一章的 stored 实用程序。

有关监控 stored 功能的其他信息，请参见第 393 页 “监控邮件存储库”。

检查数据库日志文件

数据库日志文件指 sleepycat 事务检查点日志文件 （在目录 *server-root*/msg-*instance*/store/mboxlist 中） 。如果日志文件累积，则不会发生对数据库检查点的检查。一般来说，在一个单一的时段内有两个或三个数据库日志文件。如果有更多的文件，则可能是出问题的信号。

检查用户文件夹

如果要检查用户文件夹，可以执行命令：
reconstruct -r -n （recursive nofix 递归 不修正），将对任何用户文件夹进行检查并报告错误。有关 reconstruct 命令的更多信息，请参见第 283 页 “修复邮箱和邮箱数据库”。

检查核心文件

只有当进程意外终止时，核心文件才会存在。检查这些文件很重要，特别是在邮件存储库发现问题时。

常见问题和解决办法

本节列出常见的邮件存储库问题和解决办法：

- 用户邮箱目录问题
- 全局性存储库问题

用户邮箱目录问题

用户邮箱问题是指当邮件存储库的损害仅限于少数用户而且没有对系统的全局造成损害时的情况。以下的指导方针对识别、分析和解决用户邮箱目录问题的处理过程提出了建议：

1. 查看日志文件、错误信息或用户观察到的任何不寻常行为。
2. 若要保留调试信息和历史，将整个 *server-root*/msg-*instance*/store/mboxlist/ 用户目录复制到邮件存储库以外的另一个位置处。
3. 要找出可能造成问题的用户文件夹，应当运行 reconstruct -r -n 命令。如果用 reconstruct 不能找到有问题的文件夹，则该文件夹可能不在 folder.db 中。

   如果用 reconstruct -r -n 命令不能找到有问题的文件夹，可使用 hashdir 命令确定其位置。有关 hashdir 的更多信息，请参见第 281 页 “hashdir 实用程序”和 **iPlanet Messaging Server Reference Manual** 的 “Messaging Server 命令行实用程序”一章的 hashdir 实用程序。

4. 一旦找到那个文件夹，检查其中的文件，检查权限，验证文件大小正确性。
5. 使用 `reconstruct -r`（没有 `-n` 选项）重建邮箱。
6. 如果 `reconstruct` 不能检测到已观察到的问题，可以使用 `reconstruct -r -f` 命令强制执行邮件夹的重建。
7. 如果这个文件夹不存在于 `mboxlist` 目录（*server-root*`/msg-`*instance*`/store/mboxlist`）中，而存在于 `partition` 目录 *server-root*`/msg-`*instance*`/store/partition`）中，则可能有全局性不一致问题。在这种情况下，应运行 `reconstruct -m` 命令。
8. 如果前面的步骤不起作用，可以移除 `store.idx` 文件并再次运行 `reconstruct` 命令。

注意	如果确信在该文件中有一个用 `reconstruct` 命令无法找到的问题，则只应移除 `store.idx` 文件。

9. 如果问题局限于有问题邮件，应将该邮件文件复制到邮件存储库以外的另一个位置处，然后针对 `mailbox/` 目录运行 `reconstruct -r` 命令。
10. 如果确定该文件夹在磁盘（的 *erver-root*`/msg-`*instance*`/store/mboxlist/partition/` 目录中）存在，而显然不在数据库（*server-root*`/msg-`*instance*`/store/mboxlist/` 目录）中，请运行 `reconstruct -m` 命令以确认邮件存储库的一致性。

有关 `reconstruct` 命令的更多信息，请参见第 283 页“修复邮箱和邮箱数据库”。

全局性存储库问题

如果可以确定邮件存储库失败是影响所有用户的问题或是系统全局性损害的结果，可以使用以下的指导方针恢复系统：

1. 停止邮件存储库进程。
   a. 一旦证实邮件存储库进程已被停止，可重新启动邮件存储库进程。
   b. 运行 `stored` 进程以恢复数据库。

   在许多情况下，数据库可以自动地从失败中恢复。因为当 `stored` 开始运行时，它启动一数据库恢复程序，该程序对照缓存文件和数据库文件分析数据库日志文件。该程序尝试将数据库置于一致状态。

2. 如果 msg-start 命令在 stored 进程命令试图启动一个邮件存储库时意外终止，则 stored 或是失败，或是尝试恢复存储库。

   如果当 stored 试图启动邮件存储库时，此处理过程反常地结束，则 stored 进程可能在检查大型日志文件以恢复数据库。

   a. 请检查 *server-root*/msg-*instance*/log/default/ 目录以查看 stored 已分析的信息。

   b. 此外，还可以检查配置和 pidfile.store 文件。

      pidfile.store 文件表明 pid 以及 stored 进程的状态。如果正在恢复中，pidfile 将该状态以 init 状态，如果 stored 进程完成数据库修理，则以 ready 表示。

3. 如果 pidfile 表示出 ready 状态，则数据库已恢复，邮件存储库的其余部分可以重新启动。

   a. 启动存储库进程并运行 reconstruct -m 命令。有关 reconstruct 的更多信息，请参见第 283 页 “修复邮箱和邮箱数据库”。

   b. 通过监控测试帐号和查看日志文件确定用户邮箱是否有效。

      如果个别用户邮箱损坏，请运行 reconstruct -r 命令。

   c. 如果对邮件存储库的损害是广泛的，可能有必要在邮件存储库进程停止的状态下进行修理。请参阅第 300 页 “邮件存储库恢复程序”。

4. 如果 pidfile 不能更改到 ready 状态，则 stored 进程或是在检查 mboxlist 日志文件，或是数据库不能恢复。

   a. 如果在 *server-root*/msg-*instance*/store/mboxlist 目录中有许多数据库日志文件，stored 进程可能不会脱离 init 状态。另外，数据库恢复可能需要过长的时间（例如，对于多数计算机上，20 到 30 个日志文件的处理时间就太长了。）如果此情况出现，应停止 stored 进程，移除在 *server-root*/msg-*instance*/store/mboxlist 目录中的文件，并启动快照或快速恢复程序。

   b. 如果 stored 进程不能恢复邮件存储库，则此数据库很有可能已经损坏。在这种情况下，需要恢复数据库的快照副本，或启动快速恢复技术。有关详细信息，请参阅第 300 页 “邮件存储库恢复程序”。

注意 当进程在访问数据库时，绝不要将其终止。如果将 stored 进程在 init 状态下终止，将不能从现有的 mboxlist 数据中恢复数据库。因此，这些数据必须移除。如果终止正在访问数据库的其他进程，该数据库可能会保持在不一致状态下，需要关闭整个邮件存储库并重新启动。

邮件存储库恢复程序

本节描述重建或修理邮件存储库的恢复程序。

- **执行快速恢复。**当数据库的损坏超出标准修理范围，请使用快速恢复。（有关标准邮箱修理的信息，请参见第 283 页 “修复邮箱和邮箱数据库”。）另外，快速恢复可使邮件存储库立即被调上来。当使用标准的邮件存储库恢复程序 （参见第 283 页 “修复邮箱和邮箱数据库”）时，还需要在快速恢复程序中使用 `reconstruct` 命令。
- **创建数据库快照备份和用数据库快照恢复邮件存储库。**如果数据库损坏，可恢复为前一个版本的数据库，这样较高比例的用户文件夹可立即恢复。在执行恢复后，可以使用带 `reconstruct` 命令的快速恢复程序以替代和重建数据库。

执行快速恢复

当数据库不一致时，可在标准恢复程序中使用 `reconstruct` 实用程序。（参阅第 283 页“修复邮箱和邮箱数据库”。）

如果数据库的损坏超出标准修理范围，可以通过以下这些步骤用 `reconstruct` 进行快速恢复：

1. 停止邮件存储库进程。
2. 验证所有存储库进程已被停止。
3. 把 *server-root*`/msg-`*instance*`/store/mboxlist/*` 这些文件复制到一个安全的位置，用于随后检查。
4. 移除 *server-root*`/msg-`*instance*`/store/mboxlist/` 目录中的所有文件。
5. 启动如 `stored`、 `imapd`、 `popd` 和 `mshttpd` 这样的邮件存储库进程。
6. 运行 `reconstruct -m` 实用程序重建 `folder.db`。

创建数据库快照备份

预见到邮件存储库的损坏，可预防性地创建邮箱数据库和日志文件的备份 （称为快照） 。这样，在数据库损坏的情况下，可以使用快照替代数据库，而不需要重建数据库。快照工具随时制成数据库的一致副本并可恢复。请确认有足够的磁盘空间保存这些备份。

备注	除非另有说明，否则在表 11-9 中列出的数据库快照参数只能用于 iPlanet Messaging Server 5.2。

表 11-9 描述了三个用于创建数据库快照的 configutil 参数。这些数据库快照在恢复过程中被 stored 进程所调用：

表 11-9　configutil 数据库快照参数

数据库快照参数	说明
local.store.snapshotpath	指定向其中复制 mboxlist 目录的路径。为邮件存储库所有者设置权限。快照将被放置在子目录中。
local.store.snapshotinterval	快照间的时间间隔。时间单位是分钟。建议一天至少执行一次此程序。
local.store.snapshotdirs	储存在磁盘上的不同快照数。最小值为 2，默认值为 3，建议这个数量足够确保在当前数据库的损害超出修理范畴时，具有很好的数据库支持。

创建数据库备份时，须用 configutil 命令为下列参数指定数值：

```
configutil -o local.store.snapshotinterval -v number
```

这里的 *number* 用于指定 stored 备份数据库的频次， *number* 表示以分为单位的时间间隔。

```
configutil -o local.store.snapshotpath -v path
```

其中 *path* 表示备份副本的位置。

注意　来自较早的 Messaging Server 版本的数据库快照实用程序与这些实用程序的功能不尽相同。因此，不赞同将快照实用程序的先期 Messaging Server 版本用于 Messaging Server 5.2。

用数据库快照恢复邮件存储库

为了用数据库快照恢复数据库，熟悉邮件存储库布局十分必要。有关详细信息，请参阅第 265 页 “邮件存储库目录布局”。

在数据库快照被创建后，（如在第 300 页 “创建数据库快照备份”中所解释的），它们被储存在 src 子目录中。这些文件最终将被移动到 dst *server-root*/msg-*instance*/store/mboxlist/ 目录中，那也是恢复的数据库驻留的地方。除了快照文件外，在创建快照时还要创建控制文件。表 11-10 描述的是数据库快照控制文件。注意，这些文件为邮件存储库所有者所拥有：

表 11-10　数据库快照控制文件

控制文件	说明
dst/.nosnap	禁用数据库快照处理，即使配置数据没有刷新。
dst/.snaprst	将所有先前的快照标记为无效。在生成第一个新快照后，此文件被移除。
dst/.catrecov	触发 stored 进程，以启动将快照恢复到可用格式的灾难性恢复。
src/.snaptime	表明目录中有一有效的快照。此文件的时间戳表明快照是何时完成的。

下列步骤解释如何通过使用数据库快照，控制文件， src/ 和 dst/ 目录执行手工恢复：

1. 在执行恢复前，请确认自己是邮件存储库的所有者。
2. 停止邮件存储库进程并验证所有进程是否已停止。
3. 将 *server-root*/msg-*instance*/store/mboxlist/ 目录中的文件复制到一个安全的位置以备以后查看。
4. 检查快照，确定哪一个（如果有的话）可以替代邮件存储库。有关详细信息，请参阅第 300 页 “创建数据库快照备份”。
   a. 使用 *.snaptime 文件确定备份的有效性和时间。如果一快照对应过多的日志文件，请查看另一个快照。
   b. 拾取最近的，没有捕获到数据库问题的有效快照。

      如果没有快照可用，请遵循快速恢复程序。有关详细信息，请参阅第 300 页 “执行快速恢复”。
5. 移除在 *server-root*/msg-*instance*/store/mboxlist/ 目录中的所有文件，因为它们已经损坏。
6. 将与选中快照对应的快照文件复制到 *server-root*/msg-*instance*/store/mboxlist/ 目录中，但请确认不要复制 *.snaptime 文件。
7. 用 touch 命令在 *server-root*/msg-*instance*/store/mboxlist/ 目录中创建 .catrecov 文件。

   一个 .catrecov 文件向邮件存储库发出需要执行灾难性恢复的信号。
8. 启动邮件存储库进程。
9. 监控 stored 进程。 stored 进程应恢复。
10. 在 stored 进程恢复后，确认文件 *server-root*/msg-*instance*/store/mboxlist/.catrecov 已移除，否则一旦启动，邮件存储库将认为需要进行灾难性恢复。
11. 运行 reconstruct -m 以修正 snaptime 文件和数据库失败间的任何不同。

第 12 篇

配置安全和访问控制

iPlanet Messaging Server 全方位支持灵活的安全功能，可以避免邮件被截取，防止来自假扮成用户或管理员的入侵者，而只允许指定的人员访问邮件系统的指定部分。

Messaging Server 的安全体系结构是 iPlanet 服务器整体安全体系结构的一部分。它是建立于工业标准和公共协议之上的体系结构，具有最强的互操作性和一致性。所以，要实现 Messaging Server 的安全策略，不仅需要参考本章，还需要参阅其他一些文档。特别是在设置 Messaging Server 安全功能时，您须使用 **Managing Servers with Netscape Console** 中提供的信息。

本章包括以下各节：

- 关于服务器安全
- 关于 HTTP 安全性
- 配置认证机制
- 用户登录口令
- 配置加密的和基于证书的认证
- 配置管理员的访问权限 Messaging Server
- 配置 POP、 IMAP 和 HTTP 服务的客户访问权
- 启用 POP Before SMTP
- 配置客户机访问 SMTP 服务

关于服务器安全

服务器安全包括的主题甚广。对于绝大多数企业而言，邮件系统应满足下述重大要求：确保只有授权的人员才能访问服务器，口令或身份不失密，通信时不会错误地以其他人的身份进行，通信过程保持必要的机密等，这些都是对邮件系统的重要要求。

由于服务器通信的安全性有可能受到多方面的危及，因此也需采用多种方法加强之。本章重点介绍加密、认证和访问控制方面的设置要求，并就 Messaging Server 的安全主题进行论述，所及内容包括下列：

- **用户 ID 与登录口令：**要求用户键入其用户 ID 和口令以登录到 IMAP、POP、HTTP 或 SMTP，并要求使用 SMTP 登录口令以将发件人认证信息传输给邮件收件人。

- **加密和认证：**对服务器进行设置，以使其通过 TLS 和 SSL 协议对通信及客户认证进行加密。
- **管理员访问控制：**用 Netscape Console 的访问控制工具以授权他人对 Messaging Server 及其某些单独任务的访问。
- **TCP 客户机访问控制：**使用过滤技术控制哪个客户机可以连接到服务器端的 POP、IMAP、 HTTP 和认证的 SMTP 服务。

本章并未涉及所有有关 Messaging Server 的安全性和访问控制问题。在其他地方讨论的安全主题如下：

- **物理安全：**若没有保持服务器物理安全的设备配置，软件安全恐怕毫无意义。
- **加密邮件（S/MIME）：**使用 S/MIME （安全多用途 Internet 邮件扩充协议），发件人可在发送邮件前将之加密，收件人可以在收到邮件后保存加密的邮件，只在阅读时才将之解密。使用 S/MIME 不需要特别的 Messaging Server 配置或任务，它仅仅是一项客户操作。有关设置方面的信息，请参阅客户程序文档。请注意，Messenger Express 客户界面不支持电子邮件的加密。
- **邮件存储库访问：**您可为 Messaging Server 定义一组邮件存储库管理员。这些管理员可以查看和监控邮箱并能够控制对它们的访问。有关详细信息，请参阅第 11 篇，“邮件存储库的管理”。
- **最终用户帐户配置：**最终用户帐户信息主要通过 Delegated Administrator 产品进行维护。有关详细信息，请参阅 Delegated Administrator 说明书。也可通过 Console 界面管理最终用户帐户。有关详细信息，请参阅附录 D，“管理邮件用户和邮件发送列表”。
- **过滤 UBE（大宗商业电子邮件，亦称垃圾邮件）：**参阅第 10 篇，“邮件过滤与访问控制”。

iPlanet 已具备大量的文档，这些文档分别涵盖各种有关安全性主题。有关本文提及的主题详细背景信息以及其他与安全有关的信息，请访问 iPlanet 文献网站，网址：http://docs.iplanet.com。

关于 HTTP 安全性

Messaging Server 支持用户 ID/ 口令认证和客户证书认证两种认证方法。但是，这两个协议在处理客户与服务器之间的网络连接上有所不同。

当 POP、 IMAP、或是 SMTP 客户登录到 Messaging Server 时，系统将为其建立连接和作业时段（会话）。在会话持续期间，即从登录到退出期间，将保持连接。当建立新连接时，客户必须重新认证到服务器。

当 HTTP 客户登录到 Messaging Server 时，服务器将为客户提供一个独特的作业时段或会话 ID。在会话持续期间，客户可用该会话 ID 多次建立连接。 HTTP 客户无需每次连接时重新认证。只有当会话被切断而且客户要建立新的会话时才需要重新认证。（若空闲的 HTTP 会话持续了一段时间后，服务器会自动切断此 HTTP 会话时段并注销该客户；默认时间段为 2 小时）。

以下方法用于改进 HTTP 会话的安全性：

- 会话 ID 现可捆定在特定的 IP 地址上。
- 每个会话 ID 都有与之关联的超时值，若在指定时间段未使用会话 ID，则该会话 ID 将无效。
- 服务器保留所有打开会话的数据库，所以客户无法伪造 ID。
- 会话 ID 存储在 URL 而不是 cookie 文件中。

有关为改进连接性能而指定配置参数方面的信息，请参阅第 3 篇，“配置 POP、 IMAP 和 HTTP 服务”。

配置认证机制

认证机制是客户向服务器证明其身份的一种特定方法。 Messaging Server 支持由 SASL （简单认证和安全层）协议定义的认证方法，并支持基于证书的认证。本节描述 SASL 安全机制。有关基于证书的认证的详细信息，请参阅第 308 页 “配置加密的和基于证书的认证”。

Messaging Server 支持下列基于口令认证的 SASL 认证方法。

- **PLAIN** - 这种机制在网络上传送用户的明文口令，因而可能被他人偷窥。

  注意 SSL 可用来减轻偷窥问题。有关详细信息，请参阅第 308 页 “配置加密的和基于证书的认证”。

- **DIGEST-MD5** - 是一种 challenge/response （问题与答案）认证机制，定义请见 RFC 2831。（Messaging Multiplexor 现还不能支持 DIGEST-MD5）。
- **CRAM-MD5** - 一种与 APOP 类似的 challenge/response 认证机制，但也适用于其他协议。定义见 RFC 2195。
- **APOP** - 一种 challenge/response 认证机制，只能与 POP3 协议配合使用。定义见 RFC 1939。

使用 challenge/response 认证机制时，服务器先向客户发送一个 challenge 字符串。客户以该 challenge 及用户口令的散列码应答。若客户的应答与服务器自身的散列码匹配，用户则通过认证。散列码是不可逆的，所以当用户的口令在网络中传送时不会失密。

备注	POP、IMAP 和 SMTP 服务程序支持所有 SASL 机制。HTTP 服务程序仅支持纯明文口令机制。

配置对明文口令的访问

CRAM-MD5、DIGEST-MD5 或 APOP SASL 认证方法工作时需要访问用户的明文口令。需要执行下述步骤：

1. 配置 Directory Server 以存储明码口令。
2. 配置 Messaging Server 使其知道 Directory Server 正在使用明码口令。

配置 Directory Server 的储存口令功能

若需启用 CRAM-MD5、 DIGEST-MD5 或 APOP 机制，则必须配置 Directory Server 按下述方式存储明码口令：

1. 从 Console 中打开需配置的 Directory Server。
2. 单击 “配置”选项卡。
3. 在左面板打开数据库。
4. 在右面板单击 “口令”。
5. 从 “口令加密”下拉列表中选择 “明码”。

备注	这项更改只对将来创建的用户有影响。现有用户在更改后需要转换或重置口令。

配置 Messaging Server

现在可以配置 Messaging Server 以使其知道 Directory Server 能够检索明码口令。这样就可使 Messaging Server 安全地通告 APOP、 CRAM-MD5 和 DIGEST-MD5：

```
configutil -o sasl.default.ldap.has_plain_passwords -v 1
```

可以把该值设置为 0 或空值 （""）来禁用 challenge/response SASL 机制。

备注	现有用户在他们的口令被重置或是转换 （请参阅 “转换用户” ）之前不能使用 APOP、 CRAM-MD5 或 DIGEST-MD5。

转换用户

可用 `configutil` 指定转换用户的信息。例如，若用户改变口令或一客户要用某种没有一适当条目的机制来认证。

```
configutil -o sasl.default.transition_criteria -v value
```

具体使用的值 （value），可以指定下列其中一个：

- `CHANGE` - 若用户改变口令，服务器将转换成明码。这是默认值。
- `CLIENT` - 若客户要使用某种没有一适当条目的机制来认证，服务器要求客户使用明文口令认证。然后服务器使用相同的口令值创建所需机制的条目。
- `PLAIN` - 若客户使用明文口令，则服务器将转换成明文。

为了保证成功地转换用户，必须在 Directory Server 中设置 ACI，以允许 Messaging Server 能够在用户口令属性中写入。为达此目的，请按下述步骤操作：

1. 从 Console 中打开需配置的 Directory Server。
2. 单击 “目录”选项卡。

3. 选择用户 / 组树的基后缀。
4. 从 “对象” 菜单中选择 “访问权”。
5. 在 “Messaging Server 最终用户管理员写权限” 中选择 （双击）“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”。

用户登录口令

对于登录到 Messaging Server 进行发送或接收邮件的用户来说，要求其提交口令是抵御未授权访问的第一道防线。Messaging Server 的 IMAP、POP、HTTP 和 SMTP 服务支持基于口令的登录。

IMAP、 POP 和 HTTP 口令登录

默认情况下，内部用户必须提交口令才能从 Messaging Server 检索他们的邮件。可以分别针对 POP、IMAP 和 HTTP 服务启用或关闭口令登录功能。有关 POP、IMAP 和 HTTP 服务的口令登录的更多信息，请参阅第 48 页 “基于口令的登录”。

用户口令可以从用户的客户软件以明码或者加密的形式 （除了 POP 以外）传输到服务器。若客户和服务器双方都配置启用 SSL，而且双方都支持所需强度的加密（如第 312 页 “启用 SSL 和选择密码” 中所说明的），系统则进行加密。

用户 ID 和口令存储在系统的 LDAP 用户目录中。口令安全性标准 （如最小长度）是由目录策略要求决定的，而不是 Messaging Server 管理的一部分。

基于证书的登录是基于口令之登录的备用方法。本章将在 SSL 部分中予以讨论，请参阅第 314 页 “设置基于证书的登录”。

Challenge/response SASL 机制是明文口令登录的另一种备用方法。

SMTP 口令登录

默认情况下，当用户连接到 Messaging Server 的 SMTP 服务以发送邮件时，不需要提交口令。但您可启用 SMTP 的口令登录功能以此启用经认证的 SMTP。

经认证的 SMTP 是 SMTP 协议的扩展，它允许客户认证到服务器。认证附带有邮件。经认证的 SMTP 之主要用途是允许那些在旅途中 （或使用本地 ISP）的本地用户提交邮件 （转发邮件），而无需创建可被他人滥用的开放式转发邮件。命令 AUTH 是客户程序认证服务器时使用的。

有关启用 SMTP 口令登录 （即启用经认证的 SMTP）的说明，请参阅第 182 页 “SMTP 认证、 SASL 和 TLS”。

使用经认证的 SMTP 时，可用也可不用 SSL 加密。

配置加密的和基于证书的认证

本节包含下列内容：

- 索取证书
- 启用 SSL 和选择密码
- 设置基于证书的登录
- 如何用 SMTP 代理优化 SSL 的性能

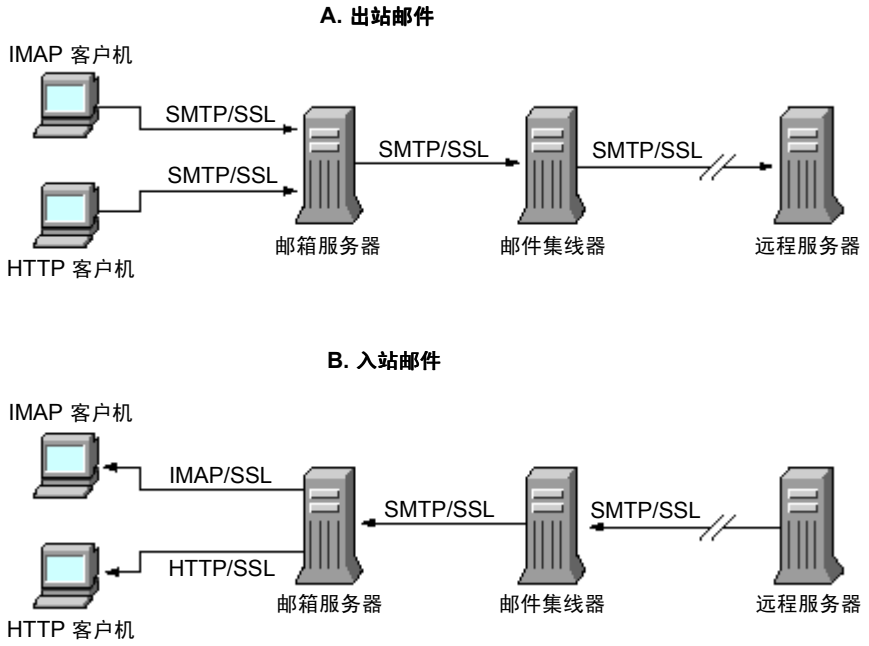
iPlanet Messaging Server 使用 TLS（传输层安全）协议，亦称 SSL（安全套接层）协议，主要用于加密通信和客户与服务器之间的基于证书的认证。 iPlanet Messaging Server 支持 SSL 3.0 和 3.1 版。 TLS 与 SSL 完全兼容并包含 SSL 中所有必要的功能。

有关 SSL 的背景信息，请参阅 *Introduction to SSL*（作为 **Managing Servers with Netscape Console** 的附录重新编排）。 SSL 是基于公钥密码术概念的技术，有关说明请见 *Introduction to Public-Key Cryptography*（也作为 **Managing Servers with Netscape Console** 的附录重新编排）。

若邮件在 Messaging Server 和其客户之间以及在各服务器之间的传输是加密的，则在通讯过程中使偷窥者几乎无机可乘。若连接的客户是经认证者，则对于假扮（欺骗）其身份的入侵者也几乎是无机可乘。

SSL 作为协议层运行于 IMAP4、HTTP 和 SMTP 的应用层之下。SMTP 和 SMTP/SSL 使用相同的端口； HTTP 和 HTTP/SSL 需要不同的端口； IMAP 和 IMAP/SSL 可以使用相同的或是不同的端口。 SSL 担负外发邮件和来件的特定通信阶段的工作，如图 12-1 所示。

图 12-1 与 Messaging Server 的加密通讯



SSL 提供连续转发加密功能，但是在每个中介服务器上邮件不加密。客户机需支持 S/MIME 才能获得端到端加密。

备注	若需启用对外发邮件的加密，必须修改通道定义以包含 `tls` 通道关键字，如 `maytls`、`musttls` 等。有关详细信息，请参阅 **iPlanet Messaging Server Reference Manual**。

请记住，设置过高的 SSL 连接可能给服务器的性能带来一定的负担。在设计邮件系统安装和分析性能时，可能需要依据服务器能力来权衡安全需求。

备注	所有 iPlanet 服务器都支持 SSL，而且在许多服务器上通过 Console 启用和配置 SSL 的界面也几乎是相同的，本节描述的一些任务的完整说明请参阅 **Managing Servers with Netscape Console** 中有关 SSL 的章节。本章仅就这些任务提供概要的说明。

索取证书

无论是用 SSL 加密还是认证，都需为 Messaging Server 获取服务器证书。此证书用于向客户机和其他服务器认证你处的服务器。

管理内部和外部模块

服务器证书可用于确定所有权和密钥对的有效性，即数据加密和解密所用的数字。服务器的证书和密钥对代表了服务器的身份。证书存放在证书数据库中，此数据库既可以是服务器的内部模块，也可以是外部的，即可移动的硬件卡 （智能卡）。

在密钥和证书数据库使用方面，iPlanet 服务器所用的模块与 PKCS（公共密钥加密系统）#11 API 相符。对于特定的硬件设备， PKCS #11 模块通常可以从供应商处获取，并须在 Messaging Server 使用此设备之前安装到 Messaging Server 中。预安装的“Netscape 内部 PKCS # 11 模块”仅支持单个内部软件标记，该标记使用服务器内部的证书数据库。

在服务器设置某证书时，您需创建该证书及其密钥的数据库并安装 PKCS #11 模块。若不使用外部硬件标记，可以在服务器上创建一个内部数据库，并使用默认的内部模块，该模块是 Messaging Server 的一部分。若需使用外部标记，则需连接到硬件智能卡阅读器并安装其 PKCS #11 模块。

无论使用内部还是外部 PKCS #11 模块，都可通过 Console 对其管理。安装 PKCS #11 模块时，请按下列步骤操作：

1. 将硬件读卡机连接到 Messaging Server 主机并安装驱动程序。
2. 通过 Console 中的 PKCS #11 管理界面为已安装的驱动程序安装 PKCS #11 模块。

（有关这方面的详细说明，请见 **Managing Servers with Netscape Console** 中的 SSL 章节。）

安装硬件加密加速器 若使用 SSL 加密，可通过安装硬件加密加速器来改进服务器加密和解密邮件的性能。加密加速器通常由一块永久安装在服务器中的硬件卡加上相应的软件驱动程序组成。iPlanet Messaging Server 支持符合 PKCS #11 API 的加速器模块。（加速器基本上是不存储其本身密钥而使用内部数据库的硬件标记。）安装加速器时，首先遵循制造商的说明安装硬件和驱动程序，然后以安装 PKCS #11 模块而结束安装，过程与硬件证书标记安装相同。

申办服务器证书

申办服务器证书时，请先在 iPlanet Console 中打开服务器，然后运行 “证书安装向导”程序。可通过“Console”菜单或 Messaging Server 的“加密”选项卡使用此向导。使用向导时需执行下述任务：

1. 生成证书请求。
2. 通过电子邮件将申报表发送到发行证书的证书管理机构或认证机构 （CA）。

当从 CA 收到回复的电子邮件后，将其保存为文本文件并使用 “证书安装向导”进行安装。

（有关这方面的详细说明，请见 **Managing Servers with Netscape Console** 中的 SSL 章节。）

安装证书

安装与请求是两个分开的过程。当从 CA 处收到申请证书的电子邮件回函并保存为文本文件时，即可再次运行 “证书安装向导”安装证书文件：

1. 请指定安装的证书是一个索取来的证书。
2. 看到有关提示时，请将证书的文本粘贴到相应的字段。

（有关这方面的详细说明，请见 **Managing Servers with Netscape Console** 中的 SSL 章节。）

备注 这一过程也可用来安装 CA 证书（见下），服务器可通过这一过程确定是否能信任客户机提交的证书。

安装委托 CA 证书

安装管理机构的证书时，也可使用 “证书安装向导”程序。 CA 证书用于验证 CA 自身的身份。服务器在认证客户和其他的服务器的过程中将使用这些 CA 证书。

例如，若您所在企业在基于口令认证的基础上还要设置基于证书的客户认证 （请参阅第 314 页 “设置基于证书的登录”一节），则需要安装客户提供的受托发布证书的所有 CA 机构的 CA 证书。这些 CA 机构可以是组织内部的，也可以是外部的，即代表商业或政府机构或其他企业。（有关通过 CA 证书认证方面的详细说明，请见 **Managing Servers with Netscape Console** 中的 “Introduction to Cryptography”相关章节。）

安装好后，Messaging Server 最初包含一些商业性 CA 机构的 CA 证书。若需要添加其它商业性的 CA 或是企业为内部使用开发的 CA （通过 iPlanet Certificate Server），则需索取并安装之。

备注 Messaging Server 自动提供的 CA 证书最初并未标记为委托的客户证书。若要监管这些由 CA 发行的客户证书，则需对委托设置进行某些编辑。有关说明，请见第 311 页 “证书和委托 CA 的管理”。

新 CA 证书的申办和安装有下列步骤：

1. 与证书管理机构联系 （可通过网站或电子邮件）并下载 CA 证书。
2. 将收到的证书文本保存为文本文件。
3. 如前一节所述，用 “证书安装向导”安装证书。

（有关这方面的详细说明，请见 **Managing Servers with Netscape Console** 中的 SSL 章节。）

证书和委托 CA 的管理

一服务器可拥有任意数量的用来认证客户的委托 CA 证书。

当您在 Console 中打开服务器并从“Console”菜单选取了“证书管理命令”后，便可查看、编辑委托设置，或删除已安装在 Messaging Server 中的任何证书。（有关说明，请见 **Managing Servers with Netscape Console** 中的 SSL 章节。）

创建口令文件

在任意 iPlanet 服务器上，当使用“证书安装向导”申请证书时，向导将创建一密钥对并将其存放在内部模块数据库或是一外部数据库（在智能卡上）中。然后向导提示您输入口令，即安装向导用于加密私钥的口令。此后只有与其相同的口令方可用于解该密钥。此向导部既不保留口令也不将其存储在任何地方。

对于绝大多数启用了 SSL 的 iPlanet 服务器而言，程序在启动时都会提示管理员提供解密钥对所需的口令。但在 Messaging Server 上，为了减少多次键入口令（至少三个服务器进程需要）的麻烦，并便利于服务器的自动重启动，口令将从口令文件读取。

口令文件名为 `sslpassword.conf`，位于 *server-instance*`/config/` 目录中。文件中的条目由若干单独的行组成，每一行的格式为

`moduleName:password`

这里的 *moduleName* 是要使用的（内部或外部）PKCS #11 模块的名字，而 *password* 则是解模块密钥对的口令。此口令以明码（非加密）保存。

Messaging Server 提供了一个默认版本的口令文件，其中只有一个条目（内部模块和默认口令）：

```
Internal (Software) Token:netscape!
```

在安装一内部证书时，若所有其它项都有所指定但未指定默认口令，则需编辑上述口令文件中的那一行以反映所指定的口令。若安装的是外部模块，则需在此文件中添加一行，在其中包含模块名和为其指定的口令。

注意	由于服务器启动时不提示管理员输入模块口令，所以确保服务器适当的管理员访问控制和适当的服务器主机及其备份的物理安全是特别重要的。

启用 SSL 和选择密码

可用 Console 启用 SSL 并选择一组加密密码，以便 Messaging Server 用来与客户机进行加密通讯。

关于密码

*密码*是加密过程中用于数据加密和解密的算法。某些密码比其他密码的加密程度更强，这意味着未授权的人对一加密邮件进行解码更为困难。

密码通过将密钥 - 一长串数字 - 作用于数据而对其进行加密。一般情况下，加密时密码使用的密钥越长，就越难于在无正确解密密钥情况下解开数据。

当客户机启动与 Messaging Server 的 SSL 连接时，客户机将通知服务器它贮备使用的加密密码和密钥长度。在任何加密通讯中，双方必须使用相同的密码。因为有一些密码和密钥的组合使用较为普遍，所以服务器在加密支持方面应灵活一些。iPlanet Messaging Server 可支持多达 6 种密码和密钥长度的组合。

表 12-1 列出了 Messaging Server 使用 SSL 3.0 时所支持的密码。有关该一览表汇总信息的详细资料，请参阅 **Managing Servers with Netscape Console** 中的“Introduction to SSL”一节。

表 12-1　Messaging Server 使用的 SSL 密码

密码	说明
128 位加密和 MD5 邮件认证的 RC4	最快的加密密码 （RSA 公司研制）和极严紧的密码密钥组合。
168 位加密和 SHA 邮件认证的三重 DES	较慢的加密密码 （美国政府标准），但具有最高严密度的密码密钥组合。
56 位加密和 SHA 邮件认证的 DES	较慢的加密密码 （美国政府标准）和中等严密度的密码密钥组合。
40 位加密和 MD5 邮件认证的 RC4	最快的加密密码 （RSA 公司研制）和严密度较低的密码密钥组合。
40 位加密和 MD5 邮件认证的 RC2	较慢的加密密码 （RSA 公司研制）和严密度较低的密码密钥组合。
不加密，只有 MD5 邮件认证	不加密，只用邮件摘要进行认证。

除非有特别的原因不使用某特定的密码，否则一般情况下应支持所有密码。但请注意，一些国家的出口法限制某些加密密码的使用。此外，还有一些客户软件产品是在美国出口控制法放宽之前开发的，这些产品不能使用严密度较高的加密法。请注意， 40 位密码只能防范一般的偷窥者，并不安全，因此不能防范有动机的攻击。

Console　若需通过 Console 启用 SSL 并选择加密密码，请按下述步骤操作：

1. 在 Console 中打开 Messaging Server，以修改其密码设定值。
2. 单击左面板中的 “配置”选项卡并选择 Services 文件夹。
3. 单击右面板中的 “加密”选项卡。
4. 选中 “启用 SSL”复选框以启用服务器上的 SSL。
5. 若要启用 RSA 密码功能，可选中 “RSA”复选框。
6. 从 “标记”下拉列表中选择要使用的标记。
7. 从 “证书”下拉列表中选择要使用的证书。

8. 单击 “密码首选项”打开可用的密码列表。
9. 单击有关的复选框以选择服务器需支持的加密密码。

若需完全关闭 SSL，取消 “启用 SSL”复选框的选中状态。

备注	若需为外发邮件启用 SSL 加密功能，则须修改通道定义以包含 `tls` 通道关键字，如 `maytls`、`musttls` 等。有关详细信息，请参阅 **iPlanet Messaging Server Reference Manual**。

命令行 也可在命令行启用 SSL 并选择密码，方法如下：

启用或关闭 SSL：

```
configutil -o nsserversecurity -v [ on | off ]
```

启用或关闭 RSA 密码：

```
configutil -o encryption.rsa.nssslactivation -v [ on | off ]
```

指定标记：

```
configutil -o encryption.rsa.nsssltoken -v tokenname
```

指定证书：

```
configutil -o encryption.rsa.nssslpersonalityssl -v certname
```

请注意，若启用 RSA 密码，还须指定标记和证书。

选择密码首选项：

```
configutil -o encryption.nsssl3ciphers -v cipherlist
```

其中， *cipherlist* 是以逗号分隔的密码列表。

设置基于证书的登录

除了基于口令的认证外， iPlanet 服务器还支持通过检查数字证书而对用户进行的认证。在基于证书的认证中，客户程序在建立了与服务器的 SSL 会话后，向服务器提交用户的证书。然后服务器鉴定提交的证书是否真实。若证书验证有效，用户则被认证通过。

在为基于证书的登录设置 Messaging Server 时，请按下列步骤操作：

1. 为服务器获取服务器证书。（有关详情，请参阅第 310 页 “索取证书”。）
2. 运行 “证书安装向导”以安装委托证书管理机构的证书，即服务器需要认证的由任意委托 CA 向用户颁发的证书。（有关详情，请参阅第 311 页 “安装委托 CA 证书”。）

   请注意，只要（至少）在服务器的数据库中有一个委托的 CA，服务器就可要求每一个连接客户机提供客户证书。
3. 打开 SSL。（有关详情，请参阅第 312 页 “启用 SSL 和选择密码”。）

4. （选项）编辑服务器的 `certmap.conf` 文件，以便服务器能按照提交的证书信息正确地搜索 LDAP 用户目录。

   若用户证书中的电子邮件地址与用户目录条目中的电子邮件地址相匹配，则不必编辑 `certmap.conf` 文件，也不必优化搜索或根据用户条目中的证书对提交的证书进行验证。

   有关 `certmap.conf` 的具体格式和可做的修改，请参阅 **Managing Servers with Netscape Console** 中 SSL 章节。

完成这些步骤后，客户机便可建立 SSL 会话以使用户能够登录到 IMAP 或 HTTP ；用户登录时，Messaging Server 将要求客户机提供用户的证书。如果客户程序提交的证书是 CA 发行的证书且该 CA 是服务器业已确定可信任的机构，而且证书中的身份与用户目录中的条目相匹配，则此用户将通过认证，并授予适当的访问权 （权限取决于管理该用户的访问控制规则）。

在启用基于证书的登录时没有必要禁止基于口令的登录。若允许基于口令的登录 （这是默认状态），而且已经执行了本节描述的任务，则基于口令和基于证书的登录二者都支持。因此，若客户建立了 SSL 会话并提供了证书，则使用基于证书的登录。若客户程序不使用 SSL 或不提供证书，则服务器要求提供口令。

有关设置 iPlanet 服务器整个系统和客户机使用基于证书认证方面的详细信息，请参阅 **Single Sign-On Deployment Guide**。

如何用 SMTP 代理优化 SSL 的性能

绝大多数网站不应使用 SMTP 代理，因为它可增加 SMTP 协议的等待时间。但经常使用 SSL 保护 SMTP 连接的大型网站可能需要最大限度地利用其在 SSL 加速器硬件方面的投资，其中一种优化方法便是在专门提供 SSL 和代理服务的服务器上，对所有协议实行全面的 SSL 操作。 SMTP 代理允许 SSL 通过一前端代理服务器得到处理，而邮件队列则可位于另一分开的 MTA 机器。这样，为没项任务优化的硬件设备便可分开配置和购置。

有关 SMTP 代理的安装说明，请见第 326 页 “安装 SMTP 代理程序”。

配置管理员的访问权限 Messaging Server

本节包含下列内容：

- Delegated Administration 的层次
- 提供对整个服务器的访问权
- 限制对指定任务的访问权

本节介绍如何控制服务器管理员在 Messaging Server 上的使用权限。对特定 Messaging Server 以及 Messaging Server 任务的访问均属在 Delegated Server Administration 环境下进行的管理性工作。

Delegated Server Administration 是绝大多数 iPlanet 服务器都具备的功能，这项功能指某管理员可有选择性地向其他管理员提供其访问某服务器和服务器功能的权限。本章将简要概述某些 Delegated Server 所涉及的任务。有关详细说明，请参见 **Managing Servers with Netscape Console** 中的 Delegating Server Administration 章节。还可参阅 **iPlanet**

Messaging Server Provisioning Guide 中的“Provisioning Messaging Server Administrators”一节的说明。**iPlanet Messaging Server Provisioning Guide** 介绍了服务器管理员 （可以配置 Messaging Server 的管理员）和 iDA 管理员 （可以在系统中添加、修改和删除用户和组的管理员）的职责。

Delegated Administration 的层次

当在网络上第一次安装 iPlanet 服务器时，安装程序在 LDAP 用户目录中自动创建一个组，称作 Configuration Administrators 组 （配置管理组）。默认情况下， Configuration Administrators 组的成员对网络上的所有主机和服务器的访问是无限制的。

Configuration Administrators 组位于访问层次的顶层，如下所示。您可为 Messaging Server 设置授权管理人员：

1. **配置管理员。** iPlanet 服务器网络的 “超级用户”。具有对所有资源的全面访问权。
2. **服务器管理员。**域管理员可以创建不同的组，负责管理每种类型的服务器。例如，您可创建 Messaging Administrators 组，负责其所在管理域或整个网络上管理所有 Messaging Server。该组成员在该管理域可访问所有的 Messaging Server（但不是其他服务器）。
3. **任务管理员。**最后一点，上述任何一类管理员都可在单一 Messaging Server 或一组 Messaging Server 中以有限权限创建组，或指定一名用户。您可允许这种任务管理员执行有限的具体服务器管理任务 （如只能启动或停止服务器或访问特定的服务日志）。

管理员可通过 Console 提供的界面执行下述任务：

- 授予组或个人以 “提供对整个服务器的访问权”中描述的访问权限，以使其能使用特定的 Messaging Server。
- 限制在指定 Messaging Server 上对指定任务的访问权，如第 317 页“限制对指定任务的访问权”所述。

提供对整个服务器的访问权

若需授予一个用户或组访问给定 Messaging Server 实例的权限，请按下列步骤操作：

1. 作为对 Messaging Server 有访问权的管理员登录到 Console，以便提供对该服务器的访问权。
2. 在 Console 窗口选择该服务器。

   从 “Console”菜单中选择 “对象”，然后选择 “设置访问权”。
3. 添加或编辑对该服务器具有访问权的用户和组的列表。

（有关详细说明，请参见 **Managing Servers with Netscape Console** 中的 Delegating Server Administration 章节。）

一旦设置了对特定 Messaging Server 有访问权的个人用户和组的列表，就可以像下面所描述的那样用 ACI 将特定服务器任务委派给列表中的特定的人员或组织。

限制对指定任务的访问权

管理员通常需连接到服务器执行一项或多项管理任务。常见的管理任务列于 Messaging Server Console 中的 “任务”窗体中。

默认情况下，对特定 Messaging Server 的访问意味着对其所有任务的访问。然而，在任务窗体中的每项任务都可以有一组附加的 ACI （访问控制指令）。在给予某连接的用户 （必须已经是对整个服务器有访问权的用户）以访问这些任务的权限之前，服务器将参考那些 ACI。实际上，服务器在 “任务”窗体中只显示用户具对其有访问权的那些任务。

如果有对 Messaging Server 的访问权，则可针对任何任务（即针对任何有访问权的任务）创建或编辑 ACI，以限制其他用户和组的对这些任务的访问。

若需限制连接的用户或组具有对该任务访问权，请按下列步骤操作：

1. 作为对 Messaging Server 有访问权的管理员登录到 Console，以便提供对该服务器的访问权。
2. 打开服务器，并在服务器的 “任务”窗体中单击相应的 “任务”文本将其选中。
3. 从 “编辑”菜单中选择 “设置访问权”，添加或编辑访问规则的列表，赋予一用户或组以预定的访问类型。
4. 对于其他任务可按需重复上述过程。

   （有关详细说明，请参见 **Managing Servers with Netscape Console** 中的 Delegating Server Administration 章节。）

Managing Servers with Netscape Console 中的 Delegating Server Administration 一章对 ACI 以及创建方法有详细的说明。

配置 POP、 IMAP 和 HTTP 服务的客户访问权

本节包含下列内容：

- 客户访问过滤器的工作原理
- 过滤器语法
- 过滤器示例
- 为服务创建访问过滤器
- 为 HTTP 代理认证创建访问过滤器
- 客户访问过滤器的工作原理

Messaging Server 支持针对 IMAP、POP 和 HTTP 服务的以服务为基础的复杂访问控制，以便您对哪些客户有权访问服务器进行广泛和细微的控制。

如果您在为某个大型企业或 Internet 服务供应商管理邮件服务，这些功能可以帮助您将垃圾邮件制造者和 DNS 欺骗者排斥在系统之外，从而改善网络的总体安全性。有关大宗商业电子邮件的特殊控制，请参阅第 10 篇，“邮件过滤与访问控制”。

备注 若通过 IP 地址控制访问对于企业*并不*重要，则不必创建本节所描述的任何过滤器。若所需要的仅仅是最小限度的访问控制，请参阅第 322 页 “允许大多数”一节中关于设置的说明。

客户访问过滤器的工作原理

Messaging Server 的访问控制工具是一个程序，它与所服务的 TCP 守护程序一样监听着同一端口，并通过访问过滤器确认客户身份，若客户通过过滤过程，则允许该客户程序访问守护程序。

作为处理过程的一部分，Messaging Server TCP 客户访问控制系统执行（必要时）下述对端点地址套接字的分析：

- 两个端点的反 DNS 查找 （以实施基于域名的访问控制）
- 两个端点的向前 DNS 查找 （以检测 DNS 电子欺骗）
- `Identd` 回叫 （以检查客户端是否为客户主机所知晓）

系统将这些信息与称作*过滤器*访问控制语句进行比较，以决定是授权访问还是拒绝访问。对于每项服务，可以分别设置 Allow 过滤器和 Deny 过滤器来控制访问。 Allow 过滤器明确授权访问， Deny 过滤器明确禁止访问。

当客户要求访问一项服务时，访问控制系统将客户的地址或名字信息按顺序与每个服务的过滤器进行比较，所采用的标准是：

- 在第一个匹配处停止搜索。因为 Allow 过滤器在 Deny 过滤器之前处理，所以 Allow 过滤器优先。
- 如果客户信息与一个服务的 Allow 过滤器匹配，则授权访问。
- 如果客户信息与一个服务的 Deny 过滤器匹配，则拒绝访问。
- 如果未与任何 Allow 过滤器 或 Deny 过滤器匹配，则授权访问 - 但若该处只有 Allow 过滤器而无 Deny 过滤器，则是例外，此情况下的无匹配意味着访问被拒绝。

这里描述的过滤器语法是非常灵活的，从而能够以简单、直观的方式实现许多不同种类的访问控制策略。尽管通常只要单独使用 Allow 过滤器或 Deny 过滤器即可以实现绝大多数策略，但实际上可以使用 Allow 过滤器和 Deny 过滤器的任意组合。

下面的各节详细地描述过滤器语法并给出了使用实例。第 323 页 “为服务创建访问过滤器”一节给出了创建访问过滤器的方法。

过滤器语法

过滤器语句既包含服务器信息又包含客户信息。服务信息包括服务名、主机名以及主机地址。客户的信息包括主机名、主机地址以及用户名。在服务信息和客户信息中都可以包括通配符名或模式。

过滤器最简单的形式是：

service:hostSpec

这里的 *service* 是服务的名字（如 smtp、 pop、 imap 或 http）而 *hostSpec* 表示客户要访问对象的主机名、 IP 地址或是通配符名或模式。在处理一过滤器时，如果客户寻求的访问对象与 *client* 匹配，则对 *service* 所指定的服务或者允许或者拒绝访问（取决于过滤器的类型）。这里是一些实例：

```
imap: roberts.newyork.siroe.com

pop: ALL

http: ALL
```

如果这些都是 Allow 过滤器，则第一个授予主机 roberts.newyork.siroe.com 访问 IMAP 服务的权限，而第二个和第三个则授予所有客户访问 POP 和 HTTP 服务的权限。如果它们是 Deny 过滤器，则拒绝这些客户程序访问那些服务。（关于通配符名 ALL 的说明，请参阅第 320 页 “通配符名”。）

过滤器中的服务器信息或客户信息有可能比这里的要复杂一些，其过滤器的更一般的形式如下：

serviceSpec:*clientSpec*

这里的 *serviceSpec* 可以是 *service* 或 *service@hostSpec*，而 *clientSpec* 可以是 *hostSpec* 或 *user@hostSpec*。*user* 是与客户主机查找访问相关联的用户名（或通配符名）。以下是两个例子：

```
pop@mailServer1.siroe.com: ALL

imap: srashad@xyz.europe.siroe.com
```

如果这些是 Deny 过滤器，则第一个过滤器拒绝所有的客户对主机 mailServer1.siroe.com 上的 SMTP 服务的访问。第二个过滤器拒绝户主机 xyz.europe.siroe.com 上的用户 srashad 对 IMAP 服务的访问。（有关何时使用这些扩展的服务器和客户规范，请参阅第 321 页 “服务器 - 主机描述”和第 321 页 “客户用户名描述”。）

最后，最一般的过滤器的形式如下：

serviceList:clientList

这里的 *serviceList* 由一个或多个 *serviceSpec* 条目组成，而 *clientList* 由一个或多个 *serviceSpec* 条目组成。在 *serviceList* 和 *clientList* 中各个条目由空格和 / 或逗号分隔。

这种情况下，当处理过滤器时，若客户查找的访问与 *clientSpec* 条目中的任意个 *clientList* 匹配，则对 *serviceList* 中指定的所有服务的访问或者被允许或者被拒绝 （取决于过滤器的类型）。下面是一个实例：

```
pop, imap, http: .europe.siroe.com .newyork.siroe.com
```

如果这是 Allow 过滤器，则授予在域 europe.siroe.com 和 newyork.siroe.com 中所有客户以访问 POP、IMAP 和 HTTP 服务的权限。有关使用前导点或其他模式指定域或子网的详细信息，请参阅第 320 页 “通配符模式”。

通配符名

可以使用下述通配符名来表示服务名、主机名或地址或是用户名：

表 12-2　通配符名

通配符名	说明
ALL	通用通配符。匹配所有名。
LOCAL	匹配任何本地主机 （其名字中不包含点字符的主机）。但是，若安装中使用的是规范的名字，即使是本地主机名也包含点，这样将不与此通配符匹配。
UNKNOWN	匹配任何未知的用户，或是任何未知名字或地址的主机。 请小心使用此通配符名： 由于临时的 DNS 服务器问题，主机名有可能是不可用的 - 在此种情况下，所有使用 UNKNOWN 通配符的过滤器将匹配所有客户主机。 当软件不能识别正与之通讯的网络类型时，其网络地址是不可用的 - 在此种情况下，所有使用 UNKNOWN 通配符的过滤器将匹配所有客户主机。
KNOWN	匹配任何已知其名字的用户，或是任何已知其名字*和*地址的主机。 请小心使用此通配符名： 由于临时的 DNS 服务器问题，主机名有可能是不可用的 - 所有使用 KNOWN 通配符的过滤器将对所有客户主机失效。 当软件不能识别正与之通讯的网络类型时，其网络地址是不可用的 - 所有使用 KNOWN 通配符的过滤器将对该网络中的所有的客户主机失效。
DNSSPOOFER	匹配任何其 DNS 名与其自身 IP 地址不匹配的主机。

通配符模式

在服务或客户地址中可以使用下述模式：

- 以点字符 （.）开头的字符串。若主机名的最后部分与指定的模式匹配，则该主机名匹配成功。例如，通配符模式 .siroe.com 匹配所有在域 siroe.com 中的主机。
- 以点字符 （.）结束的字符串。若主机地址的第一个数字域与指定的模式匹配，则该主机地址匹配成功。例如，通配符模式 123.45. 匹配子网 123.45.0.0 中的任意主机的地址。
- 形如 n.n.n.n/m.m.m.m 的字符串。此通配符模式可解释为 *net/mask* 对。若 *net* 等于地址与 *mask* 的 “按位与”，则该主机地址匹配成功。例如，模式 123.45.67.0/255.255.255.128 与 123.45.67.0 到 123.45.67.127 范围内的每个地址相匹配。

EXCEPT 操作符

访问控制系统支持一个操作符。若 *serceList* 或 *clientList* 中有多个条目，可使用 EXCEPT 操作符创建匹配名字或模式时的例外。例如，表达式：

list1 EXCEPT *list2*

意味着任何匹配 *list1* 的对象均已匹配，*除非*它同时还匹配 *list2*。

下面是一个实例：

```
ALL: ALL EXCEPT isserver.siroe.com
```

若这是 Deny 过滤器，将拒绝所有客户对服务的访问，但主机 isserver.siroe.com 上的客户例外。

EXCEPT 子句可以嵌套。表达式：

list1 EXCEPT *list2* EXCEPT *list3*

与下述表达式等价：

list1 EXCEPT (*list2* EXCEPT *list3*)

服务器 - 主机描述

可以通过在 *serviceSpec* 条目中包含服务器主机名或地址信息来进一步标识一过滤器中请求的指定服务。这时此条目的格式为：

service@hostSpec

当 Messaging Server 主机以不同的 Internet 主机名设置多重 Internet 地址时，可能需要此功能。对于服务提供商，可以使用此工具在单个服务器实例上通过不同的访问控制规则托管多个域。

客户用户名描述

对于支持 RFC 1413 中所描述的 identd 服务的客户主机，可以在过滤器中的 *clientSpec* 条目之中客户的用户名来进一步标识指定的客户请求服务。这时此条目的格式为：

user@hostSpec

这里的 *user* 是由客户的 identd 服务 （或通配符名）返回的用户名。

在过滤器中指定客户用户名可能是很有用的，但是请注意下述问题：

- identd 服务是不认证的，若客户系统已经失密，它返回的客户用户名是不可信赖的。一般来说，不要使用指定的用户名而只使用通配符名 ALL、 KNOWN 或 UNKNOWN。
- 大多数现代客户机都不支持 identd，所以在现代部署中价值不大。我们正在考虑在将来的版本中去除对 identd 的支持，如果该功能对您的网站有一定的价值，请通知 iPlanet。

- 用户名查找需要时间，执行针对所有用户的查找会降低不支持 identd 的客户的访问速度。选择性的用户名查找可以减轻该问题。例如，如下所示的规则：

  serviceList： @xyzcorp.com ALL@ALL

  将不执行用户名查找即匹配域 xyzcorp.com 中的用户，但对于其他所有系统将执行用户名查找。

用户名查找能力在一定程度上可以帮助抵御来自客户主机上的未授权用户的攻击。在某些 TCP/IP 实现中这是可能的，例如，对于使用 rsh （远程外壳服务）假扮委托的客户主机的入侵者就是如此。如果客户主机支持 identd 服务，可以使用用户名查找来检测这样的攻击。

过滤器示例

本节的示例显示了控制访问的多种方法在研究这些实例的过程中，请记住 Allow 过滤器在 Deny 过滤器之前处理，当匹配成功使搜索终止，若完全无法匹配，授予访问权。

这里列出的例子使用的是主机和域名而不是 IP 地址。请记住，在过滤器中可以包含地址和网络掩码信息，这样可以改善可靠性以防止域名服务失效。

拒绝大多数

这种情况下，按默认访问被拒绝。只有明确授权的主机被允许访问。

默认策略 （不访问）是用单个、无多大价值的拒绝文件实现的：

```
ALL: ALL
```

此过滤器拒绝所有的 Allow 过滤器未明确授予访问权的客户的所有服务。 Allow 过滤器则类似于：

```
ALL: LOCAL @netgroup1
```

```
ALL: .siroe.com EXCEPT externalserver.siroe.com
```

第一个规则允许来自本地域 （即所有主机名中没有点的主机）的所有主机和来自组 netgroup1 的成员的访问。第二个规则是用以点开头的通配符模式，它允许来自 siroe.com 域的访问，但主机 externalserver.siroe.com 除外。

允许大多数

这种情况下，按默认访问被允许。只有明确指定的主机被拒绝访问。

默认的策略 （授权访问）使得 Allow 过滤器成为不必要。不需要的客户在 Deny 过滤器中象这样明确列出：

```
ALL: externalserver.siroe1.com, .siroe.asia.com
```

```
ALL EXCEPT pop: contractor.siroe1.com, .siroe.com
```

第一个过滤器拒绝所有的服务器对特定主机和指定域的访问。第二个过滤器只允许来自特定主机和来自指定域的 POP 访问。

拒绝对被欺骗域的访问

可以在过滤器中使用通配符名 DNSSPOOFER 以检测主机名欺骗。当指定 DNSSPOOFER 时，访问控制系统执行正向的或反向的 DNS 查找以验证客户提供的主机名与其真实 IP 地址相匹配。下面是一个 Deny 过滤器的示例：

```
ALL: DNSSPOOFER
```

此过滤器拒绝针对所有其 IP 地址与 DNS 主机名不匹配的远程主机的所有服务。

控制对虚拟域的访问

若邮件系统的安装使用了虚拟域（从而可使一个单一的服务器实例与多个 IP 地址和域名相关联），则可以通过 Allow 过滤器和 Deny 过滤器的组合对每个虚拟域实施访问控制。例如，可以像下面这样使用 Allow 过滤器：

```
ALL@msgServer.siroe1.com: @.siroe1.com
ALL@msgServer.siroe2.com: @.siroe2.com
...
```

与一 Deny 过滤器配合如下：

```
ALL: ALL
```

每个 Allow 过滤器只允许 domain*N* 中的主机连接到其 IP 地址对应于 msgServer.siroe*N*.com 的服务。所有其他的连接都被拒绝。

为服务创建访问过滤器

可以为 IMAP、POP 或 HTTP 服务器创建 Allow 和 Deny 过滤器。您还可为 SMTP 服务创建过滤器，但价值不大，因为它们只能应用于认证的 SMTP 会话。有关对未认证的 SMTP 会话进行访问控制的说明，请见第 10 篇，“邮件过滤与访问控制”。

Console 要用 Console 创建过滤器，请按下述步骤：

1. 在 Console 中，打开要为其创建访问过滤器的 Messaging Server。
2. 单击 “配置”选项卡。
3. 在左面板中打开 Services 文件夹，并在 Services 文件夹下面选择 IMAP、 POP 或 HTTP。
4. 单击右面板中的 “访问”选项卡。

   在此选项卡中的 “Allow”和 “Deny”字段显示该服务器现有的 Allow 和 Deny 过滤器。字段中的每一行表示一个过滤器。可以分别对每个域指定下述操作：

   - 单击 “添加”以创建新的过滤器。于是 “Allow 过滤器”窗口或 “Deny 过滤器”窗口打开，在窗口中键入新过滤器的文本，然后单击 “确定”。
   - 选择一个过滤器并单击 “编辑”以修改此过滤器。于是 “Allow 过滤器”窗口或 “Deny 过滤器”窗口打开，在窗口中编辑显示的此过滤器的文本，并单击“确定”。
   - 选择一个过滤器并单击 “删除”以删除此过滤器。

请注意，如果需要重新排列 Allow 过滤器或 Deny 过滤器的顺序，可以执行一系列 “删除” 和 “添加” 操作。

有关过滤器语法的说明和各种实例，请参阅第 319 页 “过滤器语法”。有关详细信息，请参阅第 322 页 “过滤器示例”。

命令行 也可以在命令行指定 Access 和 Deny 过滤器，如下所示：

若需为服务创建或编辑访问过滤器，请按下列步骤操作：

```
configutil -o service.service.domainallowed -v filter
```

这里的 *service* 是 `pop`、`imap` 或 `http`，而 *filter* 遵循第 319 页 “过滤器语法” 中描述的语法规则。

若需为服务器创建或编辑 Deny 过滤器，请按下列步骤操作：

```
configutil -o service.service.domainnotallowed -v filter
```

这里的 *service* 是 `pop`、`imap` 或 `http`，而 *filter* 遵循第 319 页 “过滤器语法” 中描述的语法规则。

为 HTTP 代理认证创建访问过滤器

任意存储库管理员都可以代理对任何服务的认证。（有关存储库管理员方面的信息，请参阅第 267 页 “指定管理员的存储库访问权限”。）只对 HTTP 服务而言，若一客户主机的访问权是通过代理认证访问过滤器授予的，则它的用户可以代理对服务器的认证。

代理认证允许其他的像门户网站这样的服务，以认证用户并通过对 HTTP 登录服务的认证。例如，某个门户网站提供了若干服务，其中之一是 Messenger Express 基于站点的电子邮件。通过使用 HTTP 代理认证功能，终端用户只需要认证到入口服务器一次，当再次访问它们的电子邮件时不需要认证。门户网站必须配置登录服务器，它起着客户与服务器之间的接口的作用。为了帮助用户配置 Messenger Express 认证所需的登录服务器，iPlanet 特为 Messenger Express 提供了认证 SDK。

本节描述如何创建 Allow 过滤器以允许通过 IP 地址的 HTTP 代理认证。本节不描述如何设置登录服务器或如何使用 Messenger Express 认证 SDK。有关设置 Messenger Express 登录服务器和使用认证 SDK 的详细信息，请与 iPlanet 代表联系。

Console 要为 HTTP 服务的代理认证创建访问过滤器：

1. 在 Console 中，打开要为其创建访问过滤器的 Messaging Server。
2. 单击 “配置” 选项卡。
3. 在左面板中打开 Services 文件夹，并在 Services 文件夹下面选择 HTTP。
4. 单击右面板中的 “代理” 选项卡。

在此选项卡的 “Allow” 字段显示此代理认证现有的 Allow 过滤器。

5. 要创建新的过滤器，单击 “添加”。

   于是 “Allow”过滤器窗口打开。在窗口中键入新过滤器的文本，并单击 “确定”。

6. 要编辑现有的过滤器，选择此过滤器并单击 “编辑”。

   于是“Allow”过滤器窗口打开。在窗口中编辑显示的此过滤器的文本，并单击“确定”。

7. 要删除现有的过滤器，从 “Allow”字段中选择一项，然后单击 “删除”。

8. 当完成对 “代理”选项卡所做的修改后，单击 “保存”。

有关 Allow 过滤器语法的详细信息，请参阅第 319 页 “过滤器语法”。

命令行 也可以在命令行为 HTTP 服务器的代理认证指定访问过滤器，如下所示：

```
configutil -o service.service.proxydomainallowed -v filter
```

这里的 *filter* 遵循第 319 页 “过滤器语法”中描述的语法规则。

启用 POP Before SMTP

SMTP 认证，或 *SMTP Auth*（RFC 2554）是提供 SMTP 转接服务器安全功能的首选方法。SMTP Auth 只允许认证的用户通过 MTA 发送邮件。然而，有些老式的客户程序只能提供对 *POP before SMTP* 的支持。如果您管理的系统属于这种情况，您可按下列方法启用 POP before SMTP。然而在可能的情况下，请鼓励您的用户升级其 POP 客户程序，而不是使用 POP before SMTP。一旦在网站上部署了 POP before SMTP，用户就会依赖这些不符合因特网安全标准的认证方法，致使最终用户面临被窃之更大的风险，而且还会因不可避免的性能减退而使整个网站的运行速度减慢，这是因为系统不得不总是跟踪和协调 IP 地址的最近成功的 POP 会话情况。

iPlanet Messaging Server 所实现的 POP before SMTP 完全不同于 SIMS 或 Netscape Messaging Server。对 POP before SMTP 的支持，乃是通过配置 Messaging Multiplexor (MMP) 以使其具有 POP 和 SMTP 代理这两项认证方法而实现的。当 SMTP 客户机连接到 SMTP 代理时，代理服务器将检查内存高速缓存中最近的 POP 认证记录。如果能找到同一客户机 IP 地址的 POP 认证， SMTP 代理则会通知 SMTP 服务器，使其允许邮件定向至本地或非本地两地的收件人。

安装 SMTP 代理程序

1. 请按 **iPlanet Messaging Server Installation Guide** 中的说明安装 iPlanet Messaging Multiplexor (MMP)。
2. 在 MMP 上启用 SMTP 代理。

   请将下列字串：

   server_root/bin/msg/mmp/lib/SmtpProxyAService@25|587

   添加到 *server_root*/mmp-*hostname*/AService.cfg 文件中的 ServiceList 选项。该选项是一长行，且不能有折行。

备注 升级 MMP 后，将会有四个新文件，与现有的四个 MMP 配置文件相对应。这四个新文件是：

AService-def.cfg, ImapProxyAService-def.cfg, PopProxyAService-def.cfg, and SmtpProxyAService-def.cfg

这些文件是安装程序创建的，说明文件中描述的四个配置文件并不是在安装过程创建的，故不受其影响。当 MMP 启动时，它将查找正常的配置文件（如说明文件所述）。如果找不到正常的配置文件，MMP 将尝试把相关的 *AService-def.cfg 文件复制到相应的 *AService.cfg 文件名。

---

3. 在每一部 SMTP 转接服务器上的 SMTP 通道选项文件 tcp_local_option 中设定 PROXY_PASSWORD 选项。

   当 SMTP 代理与 SMTP 服务器建立连接时，它须通知 SMTP 服务器真正的客户机 IP 地址以及其它连接信息，以便 SMTP 服务器能正确地应用转接阻塞功能和其它安全策略（其中包括 POP before SMTP 认证）。这是一项对安全极为敏感的操作，因此必须得到认证。在 MMP SMTP 代理和 SMTP 服务器上配置的代理口令可确保任何第三方不会滥用此工具。

   范例：PROXY_PASSWORD *A_Password*

4. 配置 SMTP 代理对 POP before SMTP 的支持。

   a. 编辑 *server_root*/mmp-*instance*/SmtpProxyAService.cfg 配置文件。

      下列 SMTP 代理选项在操作方面与 IMAP 和 POP 代理选项相同 （见 **iPlanet Messaging Server Installation Guide** 标题为“Installing the Messaging Multiplexor”的附录说明，以及 **iPlanet Messaging Server Reference Manual** 中 “Encryption (SSL) Option”一节有关这些选项的说明或其它相关说明）：

      LdapURL, LogDir, LogLevel, BindDN, BindPass, Timeout, Banner, SSLEnable, SSLSecmodFile, SSLCertFile, SSLKeyFile, SSLKeyPasswdFile, SSLCipherSpecs, SSLCertNicknames, SSLCacheDir, SSLPorts, CertMapFile, CertmapDN, ConnLimits, TCPAccess

      上述文档中没有列出的其它 MMP 选项（其中包括 BacksidePort 选项），目前尚不能用于 SMTP 代理。

      增加下列五个选项：

      SmtpRelays 是以空格分隔的 SMTP 转接服务器主机名的列表 （具有选用端口），用于循环反复转接。这些转接设备必须要支持 XPROXYEHLO 扩展程序。这一选项是必需项，没有默认设置。
      范例：`default:SmtpRelays  manatee:485 gonzo mothra`

      SmtpProxyPassword 是一个口令，用于认证 SMTP 转接服务器上的源通道变更。这一选项是必需项，没有默认设置，且必须与 SMTP 服务器上的 PROXY_PASSWORD 选项匹配。
      范例：`default:SmtpProxyPassword` *A_Password*

      EhloKeywords 选项提供了一个 EHLO 扩展关键字列表，由代理传送给客户机。这是默认设置之外的选项。MMP 将从 SMTP 转接装置返回的 EHLO 列表中删除任何不能识别的 EHLO 关键字。 EhloKeywords 用于指定不应从该列表中删除的附加 EHLO 关键字。默认值是空的，但 SMTP 代理将支持下列关键字，所以没有必要将其列入该选项：8BITMIME, PIPELINING, DSN, ENHANCEDSTATUSCODES, EXPN, HELP, XLOOP, ETRN, SIZE, STARTTLS, AUTH

      那些使用 “TURN”扩展程序 （已很少有人使用）的网站，可使用下列范例：
      范例：`default:EhloKeywords  TURN`

      PopBeforeSmtpKludgeChannel 选项被设定为某一 MTA 通道的名称，以可用于 POP before SMTP 认证连接。默认值是空的，对于那些想启用 POP before SMTP 的用户而言，典型设置是 tcp_intranet。对于 SSL 性能优化而言，这一选项并非必需 （见第 315 页 “如何用 SMTP 代理优化 SSL 的性能”）。
      范例：`default:PopBeforeSmtpKludgeChannel  tcp_intranet`

      ClientLookup 选项会自动默认选用 no。如果设定为 yes， DNS 反向查找客户机 IP 地址之操作将会无条件地进行。这样， SMTP 转接器就无须承担这项操作。这一选项可在每一托管域的基础上进行不同的设置。
      范例：`default:ClientLookup  yes`

b. 设置 `PreAuth` 选项和 `PopProxyAService.cfg` 配置文件中的 `AuthServiceTTL` 选项。对于 SSL 性能优化而言，这一选项并非必需。（参阅第 315 页 “如何用 SMTP 代理优化 SSL 的性能”。）

备注 `AuthServiceTTL` 绝**不**能在 IMAP 或 SMTP 代理配置文件中设置。如此，才能确保 POP before SMTP 起到应有的功用。

这些选项用于指定当用户得到 POP 认证后，用户有多长时间 （以秒计算）可以提交邮件。典型的设置为 900 至 1800 （15-30 分）。

范例：

```
default:PreAuth     yes
default:AuthServiceTTL     900
```

c. 您也可通过选择而指定 MMP 将等待多少秒，以便 SMTP 转接程序作出响应，然后再尝试列表中的下一项任务。

默认值为 10 （秒）。如果不能与 SMTP 转接程序连接， MMP 将避免使用该转接程序，时间长短（分钟）相当于在线恢复之超时 （如果在线恢复超时是 10 秒，而且转接程序出现故障， MMP 则在 10 分钟内不会再使用该转接程序）。

范例：`default:FailoverTimeout  10`

配置客户机访问 SMTP 服务

有关配置客户机访问 SMTP 服务的详细说明，请参阅第 10 篇，“邮件过滤与访问控制”。

第 13 篇

日志记录和日志分析

iPlanet Messaging Server 可创建用来记录有关事件的日志文件，这些事件涉及管理、用服务器所支持的任何一种协议（SMTP、 POP、 IMAP 和 HTTP）的通信、以及由服务器所进行的其他处理。通过检查日志文件，可以监控服务器运行的许多方面。

因为 MTA 使用一个区别于其他服务的单独的日志工具，所以不能用 iPlanet Console 配置日志服务和查看日志。但是可以通过在配置文件中指定信息来配置 MTA 日志记录。因此，本章共分为三部分。第一部分提供总的介绍性信息；第二部分介绍邮件存储库与管理服务的日志记录问题；第三部分介绍 MTA 服务的日志记录问题。

第一部分：绪论

第二部分：服务日志（邮件存储库、 Administration Server 和 MTA）

第三部分：服务日志（MTA）

第一部分：绪论

您可自定义创建和管理 Messaging Server 日志文件的策略。本章介绍日志文件的类型和结构，并讨论如何管理和如何查看日志文件。这一部分由下列分节组成：

- 日志服务
- 用第三方工具分析日志

日志服务

Messaging Server 可为每一种所支持的主要协议或服务分别创建一组日志文件。这样就可单独制定、查看每一种类型日志文件。表 13-1 列出了可记录的服务，并对每一项服务的日志文件进行了说明。

表 13-1　日志服务

服务	日志文件说明
Admin	以 Administration Server 的方式，包含与 iPlanet Console 和 Messaging Server 之间通信有关的日志事件 （主要通过几个 CGI 进程）。
SMTP	包含与服务器的 SMTP 活动有关的日志事件
IMAP	包含与服务器的 IMAP4 活动有关的日志事件
POP	包含与服务器的 POP3 活动有关的日志事件
HTTP	包含与 HTTP 服务器活动有关的日志事件
Default	包含与服务器的其他活动有关的日志事件，例如命令行实用程序和其他进程

用第三方工具分析日志

对于超出了 iPlanet Messaging Server 能力的日志分析和报告生成事项，需要使用其他的工具。可以借助于文本编辑器或标准的系统工具自己操纵日志文件。

通过使用一种支持正则表达式分析的可使用脚本语言的文本编辑器，可以做到在本章所讨论的任何标准的基础上搜索和抽取日志条目，并可对结果进行分类，甚至生成合计或其他统计数据。

在 UNIX 环境下，您还能够修改和使用已有的、被开发来操纵 UNIX `syslog` 文件的报告生成工具。如果希望使用一个不受版权限制的 `syslog` 操纵工具，切记需要修改该工具以解决不同日期 / 时间格式问题和两个额外组件 （*facility* 和 *logLevel*）的问题，这两个组件在 Messaging Server 日志条目中显示，而不在 `syslog` 条目中显示。

第二部分：服务日志 （邮件存储库、 Administration Server 和 MTA）

本节对以下服务的日志记录进行了说明：POP、IMAP、HTTP、MTA、Admin 和 Default （参见表 13-1）。

对于这些服务，您可使用 iPlanet Console 指定日志设置并查看日志文件。所指定的设置影响到日志事件的种类和数量。当分析日志文件时，可使用这些设置和其他特性来改善对日志事件的搜索。有关 MTA 使用的服务日志方面的附加说明，请见第 339 页 “第三部分：服务日志 （MTA）”。

第二部分包含下面各节：

- 日志特性
- 日志文件格式
- 定义和设置日志记录选项
- 搜索并查看日志

日志特性

本节说明了下面这些邮件存储库和管理服务的日志特性：日志记录级别、日志事件的种类、日志文件名约定和日志文件目录。

日志记录级别

日志记录的级别，或称为优先级，定义了日志记录活动的详细程度（冗长度）。优先级较高意味着详细程度较低；这也意味着只有较高优先级（高重要性等级）的事件才记录到日志中。级别较低意味着详细程度较高；这也就意味着日志文件中记录了更多的事件。

您可分别为每一项服务 - 即 POP、IMAP、HTTP、Admin 和 Default - 分别设置日志记录的等级，方法是通过设置 `logfile.`*service*`.loglevel` 配置参数 （见第 334 页 “定义和设置日志记录选项”）。您还可用日志记录等级筛选通过搜索获得的日志事件。表 13-2 说明了这些可用的等级。这些日志记录级别是 UNIX `syslog` 功能的一个子集。

表 13-2　存储和管理服务的日志记录级别

级别	说明
Critical （致命）	最少细节的日志记录。每当发生严重问题或致命错误 （如服务器无法访问邮箱或需要调入并运行的程序库）时，可将事件写入日志。
Error （错误）	每当发生错误情况 （如在连接一个客户或另一个服务器时失败）时，可将事件写入日志。
Warning （警告）	每当发生警告情况 （如服务器无法理解来自客户的通信）时，可将事件写入日志。
Notice （通知）	每当产生一个通知 （一种普通但很重要的情况，如用户登录失败或一对话关闭）时，可将事件写入日志。
Information （信息）	每当进行重大操作 （如用户成功地登录、注销，或创建或重命名一个邮箱）时，可将事件写入日志。
Debug （调试）	最冗长的日志记录。仅对调试目的有用。对于每个进程或任务中的每一个单独的步骤，都可将事件写入日志，以用于查明问题。

一旦选择了一个特定的日志记录级别，对应于该级别，以及所有更高 （较不冗长）级别的事件都将记录到日志中。日志记录的默认级别为 `Notice`。

备注　设置的日志记录越冗长，日志文件所占用的磁盘空间就越大；关于这一问题的指导方针，参见第 334 页 “定义和设置日志记录选项”。

日志事件的种类

在每一个所支持的服务或协议中， Messaging Server 依据工具或事件所发生的功能区对日志事件进一步分类。所有记录事件都包含了生成该事件的工具的名字。依据这样的分类可在搜索时过滤事件。表 13-3 列出了 Messaging Server 能识别的日志事件种类。

表 13-3　日志事件种类

工具	说明
General （一般）	与本协议或服务相关的无差别操作
LDAP	与 Messaging Server 访问 LDAP 目录数据库有关的操作
Network （网络）	与网络连接 （套接字操作错误即属此类）有关的操作
Account （帐户）	与用户帐户 （用户登录即属此类）有关的操作
Protocol （协议）	与具体协议的命令 （由 POP、IMAP 或 HTTP 等功能返回的错误即属此类）有关的协议级操作
Stats （统计）	与收集服务器统计数据有关的操作
Store （存储库）	与访问邮件存储库 （读 / 写错误即属此类）有关的低级操作

有关在日志搜索中将事件种类用作过滤器的范例，请参见第 337 页 “搜索并查看日志”。

邮件存储库与管理日志的文件名约定

POP、IMAP、HTTP、Admin 和 Default 服务的日志文件使用相同的命名约定。每一个文件具有如下形式的文件名：

service.sequenceNum.timeStamp

表 13-4 列出了邮件存储库日志文件名的约定。

表 13-4　存储库与管理日志的文件名约定

组件	定义
service （服务）	记录的服务项：POP、 IMAP、 HTTP、 Admin、 Default。
sequenceNum （顺序号）	指定此日志文件创建顺序的整数，这是相对于日志文件目录中的其他日志文件而言的。较高顺序号的日志文件相对于较低顺序号的日志文件要更新一些。顺序号不循环使用，在服务器生命周期（从服务器安装开始）内单调增长。
timeStamp （时间戳）	指定文件创建的日期与时间的整数。（其数值以标准的 UNIX 时间表示：从 1970 年 1 月 1 日午夜开始的秒数。）

例如，一个名为 `imap.63.915107696` 的日志文件应该是 IMAP 日志文件目录中创建的第 63 个日志文件，它创建于 1998 年 12 月 31 日下午 12:34:56。

将末端开放的顺序计数方式与时间戳相结合，使得为分析而轮换、终止和选择文件更为便利。关于更多的相关建议，参见第 334 页 “定义和设置日志记录选项”。

日志文件目录

每一项日志服务被分配到一单个目录中，它的日志文件即存储于该目录中。如同所有的 POP 日志文件和其他服务中的日志文件一样，所有的 IMAP 日志文件存储在一起。要为每一个目录定义位置，还须定义目录的最大空间以及该空间中允许存储的日志文件的最大数量。

须确保存储容量足够容纳所有的日志文件。日志数据可占有相当大的空间，在较低的日志记录级别 （更冗长）情况下更是如此。

定义日志记录级别、日志轮换、日志终止以及服务器备份策略等也是很重要的。这可使所有的日志文件目录都能备份，而且不会出现超载情况；否则，会丢失信息。请参阅第 334 页 “定义和设置日志记录选项”。

日志文件格式

所有由 Messaging Server 创建的邮件存储库和管理服务日志文件具有相同的内容格式。日志文件为多行文本文件，其中的每一行中描述一个日志事件。对于每一种所支持的服务，所有事件描述都具有如下所示的通用格式：

```
dateTime hostName processName[pid]:category logLevel:eventMessage
```

表 13-5 列出了日志文件的各个组件。注意，除了日期 / 时间格式不同以及格式中包含了两个额外的组件 （*category* 和 *logLevel*）外，这里的事件描述格式与 UNIX 的 `syslog` 工具所定义的格式相同。

表 13-5　存储与管理日志文件组件

组件	定义
dateTime （日期时间）	事件被记录到日志的日期和时间，表示为 *dd/mm/yyyy hh:mm:ss* 格式，并有一时区字段，表示为 *+/-hhmm*，相对于 GMT。例如：`02/Jan/1999:13:08:21 -0700`
hostName （主机名）	运行服务器的主机的名字：例如， `showshoe`。 **注意：**如果主机中有一个以上的 Messaging Server 实例，您则可用进程 ID （pid）将不同实例的日志事件分隔开。
processName （进程名）	生成事件的进程名字：例如， `cgi_store`。
pid	生成事件的进程之标识：例如， `18753`。
category （种类）	事件所属类别：例如， `General` （参见第 332 页表 13-3）。
logLevel （日志记录级别）	事件所表现的日志记录级别： 例如， `Notice` （参见第 331 页表 13-2）。
eventMessage （事件消息）	可以是任何长度的针对一事件的解释性信息： 例如， `Log created(894305624)`。

下面是三个可用 iPlanet Console 查看的日志事件的例子：

```
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 事件条目的结尾可有三个数。上面的例子中有 0 115 0。第一个数是客户机发送的字节，第二个数是服务器发送的字节，第三个数是所选的邮箱 （POP 永远是 1）。

通过 “日志查看器”（Log Viewer）窗口查看一日志文件时，通过搜索事件中的任何指定的组件 （例如一个指定的日志记录级别、种类或一个指定的进程 ID），可限制显示出的事件的数量。有关详情，请参见第 337 页 “搜索并查看日志”。

每个日志条目的事件消息的格式都是该日志事件类型所特有的格式：也即，每一项服务定义了什么内容将出现在它的事件消息中。许多事件消息是简单明了的；但也有较复杂的消息。

定义和设置日志记录选项

可定义邮件存储库和和管理服务的日志记录配置以更好地满足管理上的需要。本节讨论的问题有助于就最佳配置和策略做出决策，并解释如何实现。

灵活的日志记录体系

日志文件 （*service.sequenceNum.timeStamp*）的命名方案有助于设计一个灵活的日志轮换和备份策略。事实上，由于不同服务的事件被写入不同的文件中，使得快速分离问题变得更容易。另外，由于文件名中的顺序号总是递增的，而且时间戳总是唯一的，因此后创建的日志文件不会因耗尽了有限数量的顺序号而简单地覆盖先创建的日志文件。反之，只有到达时限、文件数量或总存储空间这些更为灵活的限制时，老日志文件才被覆盖或删除。

Messaging Server 支持日志文件的自动轮换，这简化了管理，方便了备份。无须手工废除当前日志文件并创建一个新日志文件以容纳随后的日志事件。可随时对目录中除当前日志文件以外的所有文件进行备份，而无须停止服务器或手工通报服务器去启动一个新的日志文件。

在确立了日志记录策略后，可设置选项 （对于每一项服务而言）以控制总日志存储空间、日志文件的最大数量、单个文件大小、文件最大时限以及日志文件轮换频率等限制。

规划所需的选项

需要注意的是，必须设置若干种限制，而且其中不止一个可使日志文件被轮换或被删除。哪个限量先到达，哪个限量就是起控制作用的限制条件。例如，若最大日志文件空间为 3.5MB，而且指定每天创建一个新日志文件，则当日志数据增长速率大于每 24 小时 3.5MB 时，实际创建日志文件的速率大于每天一个。因此，若日志文件的最大数量为 10，日志文件的最大时限为 8 天，就有可能永远无法达到该时限。这是因为，较快的日志文件轮换速率意味着在不到 8 天的时间内要创建 10 个日志文件。

为 Messaging Server 的管理日志提供的下列默认值，可能是规划的一个合理的出发点：

目录中日志文件的最大数量：10
最大日志文件空间：2 MB
所有日志文件总的最大空间：20 MB
最小可用磁盘空间：5 MB
日志轮换时间：1 天
最大时限：7 天
日志记录级别：Notice （通知）

可以看出，这种配置是基于这样的假定：服务器管理日志数据预计以每天 2MB 的速率积累，备份为每周一次，而分配给总管理日志的存储空间至少为 25MB。（若日志记录级别更为冗长，这些设置可能不够充分。）

对于 POP、IMAP 或 HTTP 日志而言，采用与默认同样的值也许是合理的开端。如果所有服务都具有与前面列出的默认值几乎相同的日志存储需求，则一开始可按 150MB 的估计值安排总日志存储空间。（需要注意的是，这仅仅是一个大概的存储空间需求；实际存储空间需求可能有很大的不同。）

设置日志记录选项

您可用 iPlanet Console 或命令行来设置选项以控制邮件存储库日志记录配置文件。

这些选项的最优设置取决于日志数据累积的速率。这个速率可能是每 4000 到 10000 个日志条目占用 1MB 存储空间。在更冗长的日志记录级别 （如 Notice）情况下，一个适度繁忙的服务器每周可生成几百兆字节的日志数据。下面是一个可采用的方案：

- 设置一个与存储空间限制相一致的日志记录级别，也就是这样一种日志记录级别，它使得估计的日志数据累积速率与用以估计存储空间限制的速率大致相同。
- 定义日志文件的空间，以便执行搜索不受影响。还需进一步调整，使之与轮换空间安排和总存储空间限制协调一致。对于给定的日志条目累积速率，应设置一个比预期略大的最大值，以适应轮换自动发生时的累积。文件的最大空间乘以文件的最大数量应大致等于总存储空间限制。

  例如，若 IMAP 日志设置为每天轮换一次，则所预期的 IMAP 日志数据累积速率为每天 3MB，而 IMAP 日志的总存储空间限制为 25MB，则可将 IMAP 日志文件的最大空间设置为 3.5MB。（在这个例子中，若累积太快，以至于所有的日志文件都达到最大空间，且达到日志文件最大数量，则仍会丢失一些日志数据。）
- 若服务器每周备份一次， IMAP 日志文件每天轮换一次，则需将 IMAP 日志文件的最大数量指定为大约 10 个 （考虑到由于单个文件达到存储空间限制而使轮换加速的情况），最大时限为 7 或 8 天。
- 在硬盘容量范围内挑选一个总存储空间限制，使之与为服务器所规划的备份时间安排协调一致。估计出日志数据累积的速率，加上安全因素，即可定义总存储空间限制，使到达该限制的时间不至于超过两次备份之间的时间。

  例如，若预期 IMAP 日志文件数据的平均累积速率为每天 3MB，服务器备份每周一次，则应当为 IMAP 日志设置一个 25-30MB 等级的存储空间限制（假定磁盘存储空间足够大）。

- 为安全起见，挑选一个在保存日志文件的卷中容许的最小自由磁盘空间容量。用这种方法，若是由除日志文件空间以外的因素导致卷空间被充满，则在把日志文件写入已满磁盘而导致失败之前，老日志文件将被删除。

需要注意的是，可以选择将日志信息发送给 syslog 工具，而非服务器所支持的日志文件。通过按如下方式设置 `syslogfacility` 选项以将日志信息发送到 syslog：

```
configutil -o logfile.service.syslogfacility -v value
```

其中，*service* 是 `admin`、`pop`、`imap`、`imta` 或 `http` 和 *value* 是 `user`、`mail`、`daemon`、`local0` 至 `local7`，或为无。

若设置了“值”，邮件被记录到对应与设置值的 syslog 工具，而其他日志文件服务选项均被忽略。若没有设置选项，或值被设置为 `none`，日志记录将使用 Messaging Server 的日志文件。

Console 使用 iPlanet Console 设置日志记录选项：

1. 打开要设置其日志文件选项的 Messaging Server。
2. 单击“配置”选项卡，打开左面板中的 Log Files 文件夹，选择一项服务（例如 IMAP、HTTP 或 Admin 等）的日志文件。
3. 从“详细程度”下拉列表中挑选一日志记录级别。
4. 在“日志文件目录路径”字段中输入保存日志文件目录的名称。
5. 在“每个日志的文件大小”字段中，输入最大日志文件大小。
6. 在“创建一个新日志，每隔：”字段中，为日志轮换计划输入一个数。
7. 在“每个目录的日志数量”和“如果一个日志生成时间超过”这两个字段中，输入与备份时间安排相协调的最大日志文件数和最大时限。
8. 在“如果超出总日志大小”字段中输入您需要的总的存储限量。
9. 在“如果磁盘空间小于”字段中，输入所需保留的最小自由磁盘空间的大小。

命令行 在命令行中设置选项须使用 `configutil` 命令，如下例所示：

设置日志记录级别：

```
configutil -o logfile.service.loglevel -v level
```

其中，*service* 是 `admin`、`pop`、`imap`、`imta` 或 `http` 和 *loglevel* 是 `Nolog`、`Critical`、`Error`、`Warning`、`Notice`、`Information` 或 `Debug`。

指定日志文件目录路径：

```
configutil -o logfile.service.logdir -v dirpath
```

指定每个日志文件的最大空间：

```
configutil -o logfile.service.maxlogfilesize -v size
```

这里的 *size* 用于指定字节数。

指定日志轮转时间安排：

```
configutil -o logfile.service.rollovertime -v number
```

这里的 *number* 用于指定秒数。

指定每目录中日志文件的最大数量：

```
configutil -o logfile.service.maxlogfiles -v number
```

指定存储空间限制：

```
configutil -o logfile.service.maxlogsize -v number
```

这里的 *number* 用于指定字节数。

指定所需保留的最小自由磁盘空间：

```
configutil -o logfile.service.minfreediskspace -v number
```

这里的 *number* 用于指定字节数。

指定日志文件存活的时限：

```
configutil -o logfile.service.expirytime -v number
```

这里的 *number* 用于指定秒数。

搜索并查看日志

iPlanet Console 提供了一个查看邮件存储和管理日志数据的基本界面。通过它可以选择单个日志文件，并可对文件中的日志条目进行灵活的带过滤的搜索。

对于一个给定的服务，日志文件是按日期时间顺序列出的。一旦选定一个日志文件进行搜索，通过指定搜索参数，可缩小单个事件的搜索范围。

搜索参数

下面是可用于指定来查看日志数据的搜索参数：

- **时间段**。可以指定一特定时间段的起始和结束时间以便从该时间段中检索事件，也可以指定一个 （在此之前的）日数来搜索。当发生了服务器崩溃或其他类似事件而且知道发生时间时，通常可以设置一个范围来找到相关的事件。或者也可以指定日范围，仅查看当前日志文件中当天发生的事件。
- **日志记录级别**。可设置一个日志记录级别（参见第 331 页“日志记录级别”）。应选择一个特定的级别来发现一个特定的问题；例如， Critical 可用来寻找服务器崩溃的原因，Error 可用于定位失败的协议调用。
- **工具。**可指定一个工具（参见第 332 页“日志事件的种类”）。如果知道包含问题的功能区，可选择一个特定的工具；例如，如果认为服务器崩溃是由磁盘错误引起的，则应选择 Store ；如果问题的产生是由于 IMAP 协议的命令错误，则应选择 Protocol。

- **文本搜索模式。**可提供一个文本搜索模式以进一步缩小搜索范围。在定义要检索的事件时，可以包含事件的任何部件（参见第 333 页“日志文件格式”），只要它能在通配符类型的搜索中表示出来，诸如事件时间、进程名、进程 ID 以及事件消息的任何部分（例如远程主机名、功能名、错误号等等）。

  搜索模式中可以包含下列特殊字符和通配符：

  * 任何字符集 （例如：*.com）
  ? 任何单字符 （例如， 199?）
  [*nnn*]*nnn* 集里的任何字符 （例如：[aeiou]）
  [^*nnn*] 不在集合 *nnn* 中的任何字符 （例如：[^aeiou]）
  [*n-m*] 范围 *n-m* 中的任何字符 （例如：[A-Z]）
  [^*n-m*] 不在范围 *n-m* 中的任何字符 （例如：[^0-9]）
  \ 转换参数：置于 *、 ?、 [或] 之前以将它们用做常值 （即字符本身）。

注释：搜索须区分大小写的。

关于将日志记录级别与工具相结合以查看日志，请参见下面的例子：

- 指定 Account 工具 （以及 Notice 级别）来显示失败的登录，这对于调查潜在的安全缺口是很有用的。
- 指定 Network 工具 （以及所有日志记录级别）来调查连接问题。
- 设置所有工具 （以及 Critical 日志记录级别）来查看服务器运行中的基本问题。

指定搜索项和查看结果

遵循以下步骤，用属于一个给定服务的指定特性来搜索日志事件：

1. 在 iPlanet Console 中，打开要对其日志文件进行检查的 Messaging Server。
2. 按两种步骤中的任何一种，显示一给定日志服务中的日志文件内容选项卡：
   - 单击“任务”选项卡，然后单击“查看*服务*日志”选项，这里的*服务*与是日志记录服务的名称 （如 “IMAP 服务”或 “管理”）。
   - 单击“配置”选项卡，然后打开左面板中的 Log Files 文件夹，选择一项服务的日志文件 （例如 IMAP 或 Admin）。然后单击右面板中的 “内容”选项卡。
3. 该日志服务的 “内容”选项卡完整显示出来。
4. 在 “日志文件名”字段中，选择要检查的日志文件。
5. 单击 “查看选中日志”按钮，打开日志查看窗口。
6. 在 “日志阅读器”窗口中，指定所需的搜索参数 （在前节已有说明，“搜索参数”）。
7. 单击 “更新”执行搜索并通过 “日志条目”字段显示结果。

第三部分：服务日志 （MTA）

MTA 提供的工具可记录每一封入队和出队的邮件。此外，它还可提供调度程序出错和调试输出。第二部分包含以下各节：

- 启用 MTA 的日志记录功能
- 指定其它 MTA 日志记录选项
- MTA 日志条目格式
- 管理 MTA 日志文件
- MTA 邮件日志记录示例
- Dispatcher 调试和日志文件

可逐个通道控制日志记录，也可设定对所有通道上活动的邮件都进行日志记录。在初次配置中，日志记录在所有通道上都被禁用。

启用了日志记录后，每当邮件通过 MTA 通道时， MTA 都会把一个条目写入 `mail.log*` 文件中。若希望获得有多少邮件通过 MTA（或特定的通道）的统计数据，或者调查一邮件是否或何时被发送或传递之类的问题时，这些日志条目是很有用的。

如果您感兴趣的只是在若干特定 MTA 通道上通过的邮件数这样的统计数据，则可以只在那些感兴趣的 MTA 通道上启用日志记录通道关键字。许多站点更喜欢在所有 MTA 通道上启用日志记录。特别地，如果试图跟踪问题，则诊断问题的第一步就是注意到邮件并没有通过预期的或预定的通道，而针对所有通道启用日志记录有助于调查此类问题。

注意 如果启用了记录功能，`mail.log` 会逐渐增大，若任其增大而不管，该文件会消耗所有可用磁盘空间。因此，必须监控这个文件的大小，定期删除不需要的内容。您也可删除整个文件，然后根据需要创建另一个版本。

启用 MTA 的日志记录功能

若需为一特定通道启用日志记录，须将关键字 `logging` 添加到 MTA 配置文件的通道定义中，如下例所示：

channel-name keyword1 keyword2 `logging`

此外，您还可设置一些配置参数，如日志文件的目录路径、日志级别等。请参阅第 330 页“第二部分：服务日志 （邮件存储库、 Administration Server 和 MTA）”。

如果希望所有通道的日志消息对日志文件都是活动的，则只需简单地将一 defaults 通道块添加在 MTA 配置文件的通道块节的开头部分即可。例如：

```
defaults logging

l defragment charset7 us-ascii charset8 iso-8859-01
siroe.com
```

defaults 通道将紧跟在 MTA 配置文件中的在第一个空白行后出现。defaults logging 所在行的前一行和后一行都应当是空白行，这一点十分重要。

每个邮件都按入、出队列的方式记入日志。所有的日志条目都放在 MTA 日志目录的 mail.log_current 文件中：msg-*instance*/log/imta/mail.log_current。

邮件退回工作，主要在半夜时分运行，将任何存在的 mail.log_yesterday 添加到累积日志文件 mail.log 中，再将当前的 mail.log_current 文件更名为 mail.log_yesterday，然后启用一个新的 mail.log_current 文件。系统对任何 connection.log* 文件也执行类似的操作。

您可将 MTA 邮件记录发送到 syslog (UNIX) 或 event log (Windows NT)，方法是将 LOG_MESSAGES_SYSLOG 选项设置为 1。0 是默认设置，用于指示系统不进行 syslog (event log) 记录。

指定其它 MTA 日志记录选项

除了当日志记录被启用时总是提供的基本信息以外，通过设置 MTA 选项文件中的各种 LOG_* MTA 选项，还可将指定额外的、可选的信息字段包含于其中。关于选项文件的完整细节，请参见 **iPlanet Messaging Server Reference Manual**。

- LOG_MESSAGE_ID。此选项可用来确立条目与邮件的关联关系。
- LOG_FILENAME。此选项使获得传递一特定邮件文件的重试次数更为容易，而且对于理解邮件分割（MTA 有可能将一邮件分割为多个收件人并存入磁盘中的不同邮件文件拷贝中）是很有用的。
- LOG_CONNECTION。该选项致使 MTA 对 TCP/IP 连接和邮件流通量进行日志记录。连接日志条目按默认值方式写入 mail.log* 文件，也可选择将其写入 connection.log* 文件；参见 SEPARATE_CONNECTION_LOG 选项。
- SEPARATE_CONNECTION_LOG。此选项用于指定将连接日志条目写入文件 connection.log。
- LOG_PROCESS. 与 LOG_CONNECTION 结合使用时，此选项建立由进程 ID 标识的连接条目与邮件条目的对应关系。
- LOG_USERNAME。 此选项控制与一个处理邮件队列的进程相关联的用户名是否保存在文件 mail.log 中。由于 SMTP 规范中使用了 SASL （SMTP AUTH），因此用户名字段中应是经过认证的用户名 （以星号为前缀）。

MTA 日志条目格式

MTA 日志文件以 ASCII 码文本写入。在默认状态下，每一个日志文件条目包含八九个字段，如图 13-1 所示。

图 13-1 MTA 日志条目格式

```
19-Jan-1998 19:16:57.64 l tcp_local E 1 adam@sesta.com
 rfc822;marlowe@siroe.com marlowe@siroe.com
```

日志条目显示：

1. 生成条目的日期和时间。
2. 源通道的通道名 （例中的 `l`）。
3. 目标通道的通道名 （例中的 `tcp_local`）。（对于 SMTP 通道，当 `LOG_CONNECTION` 被启用时，用加号 + 表示入站到 SMTP 服务器；用减号 - 表示经由 SMTP 客户机出站)。
4. 条目类型 （E）；参见表 13-6。
5. 邮件大小 （1）。默认单位为千字节，可通过使用 MTA 选项文件中的 `BLOCK_SIZE` 关键字改变这个默认单位。
6. 信封发件人：地址 （`adam@sesta.com`） 。注意有的邮件其信封发件人：地址是空的，例如通知邮件，该字段就是空的。
7. 信封收件人：地址的原格式 （`marlowe@siroe.com`）。
8. 信封发件人：地址的现用 （当前）格式 （`marlowe@siroe.com`）。
9. 传递状态 （只对 SMTP 通道而言）。

表 13-6 说明日志记录条目代码。

表 13-6 日志记录条目代码

条目	说明
D	成功出列
DA	通过 SASL （认证）成功出列
DS	通过 TLS （安全）成功出列
DSA	通过 TLS 和 SASL （安全与认证）成功出列
E	入列
EA	通过 SASL （认证）成功入列

表 13-6　日志记录条目代码（接上页）

条目	说明
ES	通过 TLS （安全）成功入列
ESA	通过 TLS 和 SASL （安全与认证）成功入列
J	拒收入列尝试 （通过从属通道程序拒收）
Q	出列暂时失败
R	拒收出列尝试的收件人地址 （通过主通道程序拒收），或一个失败 / 退回邮件的生成。
W	针对一尚未传递邮件而生成的警告消息。
Z	有些是成功的收件人中，但此收件人暂时不成功；所有收件人原邮件文件出列，取而代之的是，一个为此受件人以及其他不成功收件人而创建的新邮件文件将立即入列。
SMTP 通道的 LOG_CONNECTION + 或 - 条目	
C	连接已关闭
O	连接已打开
X	连接已拒收
Y	在建立连接之前，连接尝试失败
I	ETRN 命令已收到

在 LOG_CONNECTION、 LOG_FILENAME、 LOG_MESSAGE_ID、 LOG_NOTARY、 LOG_PROCESS 以及 LOG_USERNAME 都启用的情况下，格式改变情况如图 13-2 所示。（由于印刷上的原因，日志条目行被折行；实际的日志条目应显示在一个物理行上。）

图 13-2　带附加字段的日志格式

```
19-Jan-1998 13:13:27.10 HOSTA   2e2d.2.1 tcp_local   l
 E 1 service@siroe.com rfc822;adam@sesta.com
 adam 276 /imta/queue/l/ZZ01IWFY9ELGWM00094D.00
 <01IWFVYLGTS499EC9Y@siroe.com> inetmail
 siroe.com (siroe.com [192.160.253.66])
```

除了上面已经讨论过的字段外，这些附加字段是：

1. 通道进程得以运行的节点的名称 （例中的 HOSTA）。
2. 进程 ID （以十六进制表示），后跟一逗号 （点）和一计数。如果它是一个多线程通道条目（例如，tcp_* 通道条目），就会在进程 ID 和计数之间出现一个线程 ID。在示例中，进程 ID 为 2e2d.2.1。
3. 邮件的 NOTARY （传递收到的请求）标记，以整数表示 （例中的 276）。
4. MTA 队列区中的文件名（例中的 /imta/queue/l/ZZ01IWFY9ELGWM00094D.00）。
5. 邮件 ID （例中的 <01IWFVYLGTS499EC9Y@siroe.com>）。
6. 执行中的进程名 （例中的 inetmail）。在 UNIX 系统中，对于象 SMTP 服务器这样的调度程序进程，这个进程名通常为 inetmail （除非使用了 SASL）。
7. 连接信息（例中的 siroe.com (siroe.com [192.160.253.66])）。连接信息包含发送系统或通道名，例如由发送系统在 HELO/EHLO 行中呈现的名字（对于到访 SMTP 邮件），或入列通道的正式主机名 （对于其他类型的通道）。对于 TCP/IP 通道而言，发送系统的 “真”名，即通过 DNS 反向查找发现的象征性名字和 / 或 IP 地址，也可在通道关键字 ident* 的控制下呈现在括弧内；参见第 179 页 “IDENT 查找”。在这个例子中，假定使用其中的一个关键字，以默认关键字 identnone 为例，它意味着显示从 DNS 中找到的名字和 IP 地址。

管理 MTA 日志文件

邮件退回工作，主要在半夜时分运行，将任何存在的 mail.log_yesterday 添加到累积日志文件 mail.log 中，再将当前的 mail.log_current 文件更名为 mail.log_yesterday，然后启用一个新的 mail.log_current 文件。对于任何 connection.log* 文件也执行类似的操作。

MTA 自动执行轮换以维护当前文件，但必须针对备份文件、截断文件、删除文件等等任务确定一个策略，以便管理累积文件 mail.log。

在考虑如何管理日志文件的问题时，需要注意的是，MTA 的周期性回复工作将执行网站提供的 *server-instance*/imta/bin/daily_cleanup 程序，如果存在的话。因此，某些站点可能选择提供自己的清理程序更名旧的 mail.log 文件，例如每周一次 （或每月一次，等等）。

MTA 邮件日志记录示例

作为日志记录在 MTA 邮件文件中的字段格式和字段列表是多样化的，确切情况完全取决于对日志记录选项所做的设置。本节展示一些解释典型的日志条目类型的例子。对于其它可选的字段的说明，参见第 340 页 “指定其它 MTA 日志记录选项”。

备注 由于印刷上的原因，日志文件条目会呈现在多行中。在实际环境中，每个日志文件条目只占用一行。

检查日志文件时需要注意的是，在一个典型的系统中，许多邮件会被同时处理。具有代表性的是，与一个特定邮件有关的条目会散布于与其他邮件有关的条目中，而这些“其他邮件”也正在相同的时间里被处理。通过基本日志信息可获得经由 MTA 移动的邮件总数的大致情况。

如果希望将与同一邮件有关的特定条目与同一收件人相关联，可能需要启用 LOG_MESSAGE_ID。如果希望将 MTA 队列区内的特定邮件与特定文件相关联，或希望通过查看条目了解某尚未成功出队的邮件尝试传递的次数，可能需要启用 LOG_FILENAME。对于（通过 TCP/IP 通道进行处理的）SMTP 邮件，如果需要将往来于远程系统的 TCP 连接与发送的邮件相关联，可能需要启用 LOG_PROCESS 以及 LOG_CONNECTION 的某些级别。

图 13-3 展示了一个相当基本的涉及某些类型的日志条目的例子。如果一个本地用户通过一个外发 TCP/IP 通道发送一邮件到 Internet，即可见到例子中的条目类型。在本例中，LOG_CONNECTION 被启用。标有 （1）和 （2）的行是一个条目，在实际的日志文件中该条目出现在一个物理行中。类似地，标有 （3）-（7）的行也是一个条目，也应出现在一个物理行中。

图 13-3 日志记录：一本地用户发送一外发邮件

```
19-Jan-1998 19:16:57.64 l            tcp_local    E 1 (1)
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com (2)

19-Jan-1998 19:17:01.16 tcp_local                 D 1 (3)
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com (4)
 dns;thor.siroe.com
 (TCP|206.184.139.12|2788|192.160.253.66|25) (5)
 (THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694]) (6)
 smtp;250 2.1.5 marlowe@siroe.com and options OK. (7)
```

1. 此行表明，从 l 通道到 tcp_local 通道的入列 （E）日期和时间。
2. 这是 （1）中日志文件的同一物理行的一部分，只是为了印刷上的方便才另行显示。它显示了信封发件人：地址，在此例中为 adam@sesta.com，以及原始版本和当前版本的收件人：地址，在此例中为 marlowe@siroe.com。
3. 此行表明，一组 （1）邮件从 tcp_local 通道出列 （D），即由 tcp_local 通道成功发送到远程 SMTP 服务器的日期与时间。
4. 此行表明，信封发件人：地址，原信封收件人：地址，以及当前格式的收件人：地址。
5. 此行表明，连接得以建立的 DNS 中的实际系统被命名为 thor.siroe.com；本地发送系统具有 IP 地址 206.184.139.12，发送端口为 2788；远程目标系统具有 IP 地址 192.160.253.66，远程目标系统上的连接端口为 25。
6. 此行显示了远程 SMTP 服务器的 SMTP 标志区行。
7. 此行表明了为此地址返回的 SMTP 状态码； 250 是基本的 SMTP 成功代码，而且，这个远程 SMTP 服务器以扩展 SMTP 状态码和一些附加文本加以响应。

图 13-4 所示为类似于图 13-3 中的日志记录条目，不同的是，通过设置 LOG_FILENAME=1 和 LOG_MESSAGE_ID=1 而显示文件名和邮件 ID 等附加的日志信息；参见（1）和（2）。特别是邮件 ID 可用于建立条目与邮件的关联。

图 13-4 日志记录：包含可选日志记录字段

```
19-Jan-1998 19:16:57.64 l            tcp_local    E 1
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
 /imta/queue/tcp_local/ZZ01ISKLSKLZLI90N15M.00
   <01ISKLSKC2QC90N15M@sesta.com> (1)

19-Jan-1998 19:17:01.16 tcp_local                 D 1
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
 /imta/queue/tcp_local/Z01ISKLSKLZLI90N15M.00
   <01ISKLSKC2QC90N15M@sesta.com> (2)
 dns;thor.siroe.com (TCP|206.184.139.12|2788|192.160.253.66|25)
 (THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694])
 smtp;250 2.1.5 marlowe@siroe.com and options OK.
```

图 13-5 说明了如何通过启用 LOG_FILENAME=1、 LOG_MESSAGE_ID=1 和 LOG_CONNECTION=1 而发送给多个收件人。在此处，用户 adam@sesta.com 已发送到 MTA 邮件列表 test-list@sesta.com 中，该列表扩展到 bob@sesta.com、carol@varrius.com 和 david@varrius.com 中。需要注意的是，对于每个收件人，原信封收件人：地址都是 test-list@sesta.com，尽管当前信封收件人：地址是各不相同的地址。注意，尽管涉及到两个不同的文件（一个针对 l 通道，而另一个针对外发的 tcp_local 通道），邮件 ID 却始终保持不变。

图 13-5 日志记录：发送到列表

```
19-Jan-1998 20:01:44.10 l            l            E 1
 adam@sesta.com rfc822;test-list@sesta.com bob
 imta/queue/l/ZZ01ISKND3DE1K90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:44.81 l            tcp_local    E 1
 adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:44.81 l            tcp_local    E 1
 adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:50.69 l                         D 1
 adam@sesta.com rfc822;test-list@sesta.com bob
 imta/queue/l/ZZ01ISKND3DE1K90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:57.36 tcp_local                 D 1
 adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>
 dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
 (gw.varrius.com -- SMTP Sendmail)
 smtp;250 OK.

19-Jan-1998 20:02:06.14 tcp_local                 D 1
 adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>
 dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
 (gw.varrius.com -- SMTP Sendmail)
 smtp;250 OK.
```

图 13-6 说明了试图向一个不存在的域 （在此为 `very.bogus.com`）发送邮件；也即，发送到一个未被 MTA 重写规则宣布为不存在的域名而且 MTA 匹配到一个外发 TCP/IP 通道。此例假定 MTA 选项设置为 `LOG_FILENAME=1` 和 `LOG_MESSAGE_ID=1`。

当 TCP/IP 通道运行并检查 DNS 中的域名时， DNS 返回的错误讯息表明该名字不存在。请注意“rejection”条目 （R），见 （5），以及 DNS 返回的出错讯息，说明此乃一非法域名，见 （6）。

由于地址被拒收是发生在邮件被提交后，所以 MTA 生成一个退回到原发件人的邮件。 MTA 将新的拒收邮件入列到原发件人 （1）处，在删除原出站邮件 （显示于 （5）中的 R 条目）之前，发送给 Postmaster （4）一个副本。

通知类邮件，如退回邮件，具有空的信封发件人：地址，如（2）和（8）中所见到的，其中的信封发件人：字段显示为空白。由 MTA 生成的退回邮件的初始入列显示新通知邮件的邮件 ID，后跟一个原邮件（3）的邮件 ID。（这样的信息对于 MTA 并不总是可用的，但当可被日志记录时，可用于建立对应于出站失败邮件的日志条目与对应于结果通知邮件的条目之间的关联。）这样的通知邮件入列到进程通道中，然后再次入列到适当的目标通道（7）中。

图 13-6 日志记录：发送到不存在的域

```
19-JAN-1998 20:49:04 l            tcp_local    E 1
 adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
 imta/queue/tcp_local/ZZ01ISKP0S0LVQ94DU0K.00
 <01ISKP0RYMAS94DU0K@SESTA.COM>

19-JAN-1998 20:49:33 tcp_local    process      E 1 (1)
 rfc822;adam@sesta.com adam@sesta.com  (2)
 imta/queue/process/ZZ01ISKP0S0LVQ94DTZB.00
 <01ISKP22MW8894DTAS@SESTA.COM>,<01ISKP0RYMAS94DU0K@SESTA.COM> (3)

19-JAN-1998 20:49:33 tcp_local    process      E 1 (4)
 rfc822;postmaster@sesta.com postmaster@sesta.com
 imta/queue/process/ZZ01ISKP0S0LVQ94DTZB.00
 <01ISKP22MW8894DTAS@SESTA.COM>,<01ISKP0RYMAS94DU0K@SESTA.COM>

19-JAN-1998 20:50:07 tcp_local                 R 1 (5)
 adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
 imta/queue/tcp_local/ZZ01ISKP0S0LVQ94DU0K.00
 <01ISKP0RYMAS94DU0K@SESTA.COM>
 Illegal host/domain name found (6)

19-JAN-1998 20:50:08 process      l            E 3 (7)
 rfc822;adam@sesta.com adam (8)
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:08 process      l            E 3
 rfc822;postmaster@sesta.com postmaster
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:12 l                         D 3
 rfc822;adam@sesta.com adam
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:12 l                         D 3
 rfc822;postmaster@sesta.com postmaster
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SIROE.COM>
```

图 13-7 说明了试图发送错误的地址到远程系统。这个例子假定 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。注意拒收条目（R），参见（1）。相对于图 13-6 中的拒收条目，对这里的拒收条目需要注意的是，它表明到远程系统的连接已建立，并显示了远程 SMTP 服务器所生成的 SMTP 错误码，参见（2）和（3）。显示在（2）中的信息内容是由通道选项设置 LOG_BANNER=1 和 LOG_TRANSPORTINFO=1 决定的。

图 13-7 日志记录：发送到不存在的远程用户

```
20-JAN-1998 13:11:05 l            tcp_local    E 1
 adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
 imta/queue/tcp_local/ZZ01ISLNBB1JOE94DUWH.00
 <01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:08 tcp_local    process      E 1
 rfc822;adam@sesta.com adam@sesta.com
 imta/queue/process/ZZ01ISLNBB1JOE94DSGB.00
 <01ISLNBFKIDS94DUJ8@sesta.com>,<01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:08 tcp_local    process      E 1
 rfc822;postmaster@sesta.com postmaster@sesta.com
 imta/queue/process/ZZ01ISLNBB1JOE94DSGB.00
 <01ISLNBFKIDS94DUJ8@sesta.com>,<01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:11 tcp_local                 R 1   (1)
 adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
 imta/queue/tcp_local/ZZ01ISLNBB1JOE94DUWH.00
 <01ISLNBAWV3094DUWH@sesta.com>
 dns;thor.siroe.com
 (TCP|206.184.139.12|2788|192.160.253.66|25)          (2)
 (THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694])
 smtp; 553 unknown or illegal user: nonesuch@siroe.com   (3)

20-JAN-1998 13:11:12 process      l            E 3
 rfc822;adam@sesta.com adam
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:12 process      l            E 3
 rfc822;postmaster@sesta.com postmaster
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:13 l                         D 3
 rfc822;adam@sesta.com adam@sesta.com
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:13 l                         D 3
 rfc822;postmaster@sesta.com postmaster@sesta.com
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>
```

图 13-8 说明了当 MTA 拒收一远程端试图 提交的一邮件时，所产生的那一类日志文件条目。（在这个例子中，假定没有任何可选的 LOG_* 选项被启用，因此仅有基本字段被记录到日志条目中。应特别注意，启用 LOG_CONNECTION 选项，会导致在这样的 J 条目中包函额外的信息字段。）在这种情况之下，这个例子是为了说明已经以 ORIG_SEND_ACCESS 映射设置了 SMTP 转发阻塞的 MTA （参见第 247 页 “配置 SMTP 转发阻塞”），该映射包含：

```
ORIG_SEND_ACCESS

! ...numerous entries omitted...
!
   tcp_local|*|tcp_local|*   $NRelaying$ not$ permitted
```

且该处的 alan@very.bogus.com 不是内部地址。因此，远程用户 harold@varrius.com 通过 MTA 系统向远程用户 alan@very.bogus.com 转发的尝试被拒收。

图 13-8 日志记录：拒收远程端提交邮件的尝试

```
28-May-1998 12:02:23 tcp_local                J 0      (1)
 harold@varrius.com rfc822; alan@very.bogus.com        (2)
 550 5.7.1 Relaying not permitted: alan@very.bogus.com (3)
```

1. 这个日志显示了 MTA 拒收一远程端试图提交一邮件的日期和时间。拒收是通过一个 J 记录标明的。（对于 MTA 通道试图发送一个被拒收的邮件的情况，由 R 记录表明，如图 13-6 和图 13-7 所示）。
2. 显示试图提交邮件的信封发件人：地址和收件人：地址。在这种情况下，没有原始信封收件人：信息，因此字段是空的。
3. 该条目中包含 MTA 发往远程 （试图发件的人）端的 SMTP 错误消息。

图 13-9 说明了这样因下面的原因而产生的那一类日志文件条目：一邮件在初次尝试时不能传递，所以 MTA 试图多次发送该邮件。这个例子假定选项设置为 LOG_FILENAME=1 和 LOG_MESSAGE_ID=1。

图 13-9 日志记录：多次传递尝试

```
15-Jan-1998 10:31:05.18 tcp_internal   tcp_local  E 3 (1)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZZ01IS3D2ZP7FQ9UN54R.00
 <01IRUD7SVA3Q9UN2D4@sesta.com>

15-Jan-1998 10:31:10.37 tcp_local                Q 3 (2)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZZ01IS3D2ZP7FQ9UN54R.00         (3)
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 TCP active open: Failed connect()    Error: no route to host (4)

 ...several hours worth of entries...

15-Jan-1998 12:45:39.48 tcp_local                Q 3 (5)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZY01IS3D2ZP7FQ9UN54R.00         (6)
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 TCP active open: Failed connect()    Error: no route to host

 ...several hours worth of entries...

15-Jan-1998 16:45:24.72 tcp_local                Q 3
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZX01IS67NY4RRK9UN7GP.00         (7)
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 TCP active open: Failed connect() Error: connection refused (8)

 ...several hours worth of entries...

15-Jan-1998 20:45:51.55 tcp_local                D 3 (9)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZX01IS67NY4RRK9UN7GP.00
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 dns;host.some.org (TCP|206.184.139.12|2788|192.1.1.1|25)
 (All set, fire away)
 smtp; 250 Ok
```

1. 进入 `tcp_internal` 通道的邮件，无论来自 POP 或 IMAP 客户，还是来自使用 MTA 作为 SMTP 转发的组织内的另一个主机， MTA 均将之入列到外发的 `tcp_local` 通道中。
2. 如 Q 条目所示，初次传递尝试失败。
3. 可从 `ZZ*` 文件名中看出这是初次传递尝试。
4. 当 TCP/IP 包无法找到一个通往远程用户的路由时这次传递尝试失败。与图 13-6 不同的是，DNS 并不拒绝目标域名 `some.org`；相反，“no route to host”错误表明，是在发送方和接收方之间出现了一个网络方面的问题。

5. 当 MTA 作为定期工作下一次运行它时，再次尝试传递，但再次失败。
6. 文件名现在是 ZY*，表明这是第二次尝试。
7. 对于这第三次不成功的尝试，文件名是 ZX*。
8. 下一次定期工作再次尝试传递时，传递又失败，尽管这次 TCP/IP 包没有抱怨它不能通往远程 SMTP 服务器，而实际原因是远程 SMTP 服务器没有接受连接。（或许远程端已经确定了问题之所在，但他们的 SMTP 服务器尚未恢复；或者该 SMTP 服务器正忙于处理其他邮件而没有在 MTA 试图连接时接受连接。）
9. 最终邮件出列。

图 13-10 说明邮件经过转换通道而进行路由选择的情况。站点假定有一个如下所示的 CONVERSIONS 映射表：

```
CONVERSIONS

  IN-CHAN=tcp_local;OUT-CHAN=l;CONVERT    Yes
```

这个例子假定选项的设置为 LOG_FILENAME=1 和 LOG_MESSAGE_ID=1。

图 13-10 日志记录：到访 SMTP 邮件通过转换通道路由

```
04-Feb-1998 00:06:26.72 tcp_local     conversion    E 9 (1)
 amy@siroe.edu rfc822;bert@sesta.com bert@sesta.com
 imta/queue/conversion/ZZ01IT5UAMZ4QW98518O.00
 <01IT5UALL14498518O@siroe.edu>

04-Feb-1998 00:06:29.06 conversion    l             E 9 (2)
 amy@siroe.edu rfc822;bert@sesta.com bert
 imta/queue/l/ZZ01IT5UAOXLDW98509E.00
 <01IT5STUMUFO984Z8L@siroe.edu>

04-Feb-1998 00:06:29.31 conversion                  D 9 (3)
 amy@siroe.edu rfc822;bert@sesta.com bert
 imta/queue/conversion/ZZ01IT5UAMZ4QW98518O.00
 <01IT5UALL14498518O@siroe.edu>

04-Feb-1998 00:06:32.62 l                           D 9 (4)
 amy@siroe.edu rfc822;bert@siroe.com bert
 imta/queue/l/ZZ01IT5UAOXLDW98509E.00
 <01IT5STUMUFO984Z8L@siroe.edu>
```

1. 来自外部用户 amy@siroe.edu 的邮件到达，所标注的地址是 l 通道收件人 bert@sesta.com。然而，CONVERSIONS 的映射条目致使邮件初始入列到转换通道（而不是直接到 l 通道）。
2. 转换通道运行并将邮件入列到 l 通道。
3. 接着，转换通道可将邮件出列 （删除老邮件文件）。
4. 最后 l 通道将邮件出列 （传递）。

图 13-11 说明了当连接日志记录通过选项设置 LOG_CONNECTION=3 而被启用时，一外发邮件的日志输出。本例还假定 LOG_PROCESS=1，LOG_MESSAGE_ID=1 和 LOG_FILENAME=1。本例显示了这样一种情况：用户 adam@sesta.com 发送同一邮件 （注意，所有邮件副本的邮件 ID 都是相同的）给三个收件人的情况，这三个收件人是 bobby@hosta.sesta.com，carl@hosta.sesta.com 和 dave@hostb.sesta.com。本例假定邮件输出到一个标有（正如这类通道的通常情况那样） single_sys 通道关键字的 tcp_local 通道中。因此，磁盘上将为每一个不同主机名上的收件人分别创建一个邮件文件，如（1）、（2）以及（3）所示，其中收件人 bobby@hosta.sesta.com 和 carl@hosta.sesta.com 存储于同一邮件文件中，但收件人 dave@hostb.sesta.com 则存储于另一个邮件文件中。

图 13-11 日志记录：出站连接日志记录

```
19-Feb-1998 10:52:05.41 1e488.0 l            tcp_local    E 1
 adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00  (1)
  <01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:05.41 1e488.0 l            tcp_local    E 1
 adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00  (2)
  <01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:05.74 1e488.1 l            tcp_local    E 1
 adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7C11FU000FCN.00  (3)
  <01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:10.79 1f625.2.0 tcp_local    -            O (4)
 TCP|206.184.139.12|5900|206.184.139.66|25
 SMTP/hostb.sesta.com/mailhub.sesta.com          (5)

19-Feb-1998 10:52:10.87 1f625.3.0 tcp_local    -            O (6)
 TCP|206.184.139.12|5901|206.184.139.70|25
 SMTP/hosta.sesta.com/hosta.sesta.com            (7)

19-Feb-1998 10:52:12.28 1f625.3.1 tcp_local                 D 1
 adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00
  <01ITRF7BDHS6000FCN@SESTA.COM>
 hosta.sesta.com dns;hosta.sesta.com          (8)
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 (hosta.sesta.com -- Server ESMTP [iMS V5.0 #8790])
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 smtp;250 2.1.5 bobby@hosta.sesta.com and options OK.

19-Feb-1998 10:52:12.28 1f625.3.1 tcp_local                  D 1
 adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00
  <01ITRF7BDHS6000FCN@SESTA.COM>
 hosta.sesta.com dns;hosta.sesta.com
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 (hosta.sesta.com -- Server ESMTP [iMS V5.0 #8790])
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 smtp;250 2.1.5 carl@hosta.sesta.com and options OK.

19-Feb-1998 10:52:12.40 1f625.3.2 tcp_local     -            C (9)
 TCP|206.184.139.12|5901|206.184.139.70|25
 SMTP/hosta.sesta.com/hosta.sesta.com
```

```
19-Feb-1998 10:52:13.01 1f625.2.1 tcp_local                   D 1
 adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7C11FU000FCN.00
  <01ITRF7BDHS6000FCN@SESTA.COM>
 mailhub.sesta.com dns;mailhub.sesta.com
 (TCP|206.184.139.12|5900|206.184.139.66|25)
 (MAILHUB.SESTA.COM -- Server ESMTP [iMS V5.0 #8694])
 (TCP|206.184.139.12|5900|206.184.139.66|25)
 smtp;250 2.1.5 dave@hostb.sesta.com and options OK.

19-Feb-1998 10:52:13.05 1f625.2.2 tcp_local     -             C (10)
 TCP|206.184.139.12|5900|206.184.139.66|25
 SMTP/hostb.sesta.com/mailhub.sesta.com
```

1. 邮件入列到第一个收件人
2. .... 和第二个收件人 ...
3. .... 以及第三个收件人。
4. 设置 LOG_CONNECTION=3 使 MTA 写入该条目。减号 - 表示该条目涉及到一个外发连接。O 意味着该条目对应连接的打开操作。还需注意的是，这里的进程 ID 是相同的，即 1f625，这是因为针对这些不同连接的打开操作，多线程 TCP/IP 通道所使用的是同一个进程，尽管这里的打开操作是由线程 2 及线程 3 所实施。
5. 由于有两个不同的远程系统需要连接，在不同线程中的多线程 SMTP 客户机分别打开一个每个系统的连接，第一个在此条目中，第二个见 7 中所示。条目这部分显示了发送方和目标方的 IP 地址和端口号，同时也显示了初始主机名，以及通过执行 DNS 查寻找到的主机名。在 SMTP/*initial-host*/*dns-host* 子句中，注意初始主机名和在初始主机名上执行 DNS MX 记录查询找到的主机名的显示：mailhub.sesta.com 显然是 hostb.sesta.com 处的 MX 服务器。
6. 在不同的线程 （通过同一个进程）中，多线程 SMTP 客户打开到第二个系统的连接。
7. 由于有两个不同的远程系统需要连接，在不同线程中的多线程 SMTP 客户机分别打开一个与每个系统的连接，第二个在此条目中，第一个见 5 中所示。条目这部分显示了发送方和目标方的 IP 地址和端口号，同时也显示了初始主机名，以及通过执行 DNS 查寻找到的主机名。在本例中，系统 hosta.sesta.com 显然是直接收邮件的。
8. 除了产生具体的连接条目中外，LOG_CONNECTION=3 也使与连接有关的信息包含在常规邮件条目中，如例中所示。
9. LOG_CONNECTION=3 致使 MTA 写入此条目。在所有邮件 （本例中的 bobby 和 carl）出列后，连接被关闭，如此条目中的 C 所示。
10. LOG_CONNECTION=3 致使 MTA 写入此条目。在所有邮件 （本例中的 dave）出列后，连接被关闭，如此条目中的 C 所示。

图 13-12 说明了通过 LOG_CONNECTION=3 启用连接日志记录时，到访 SMTP 邮件的日志输出情况。

图 13-12 日志记录：入站连接日志记录

```
19-Feb-1998 17:02:08.70 tcp_local    +            O    (1)
 TCP|206.184.139.12|25|192.160.253.66|1244 SMTP        (2)

19-Feb-1998 17:02:26.65 tcp_local    l             E 1
 service@siroe.com rfc822;adam@sesta.com adam
 THOR.SIROE.COM (THOR.SIROE.COM [192.160.253.66])      (3)

19-Feb-1998 17:02:27.05 tcp_local    +             C    (4)
 TCP|206.184.139.12|25|192.160.253.66|1244 SMTP

19-Feb-1998 17:02:31.73 l                          D 1
 service@siroe.com rfc822;adam@sesta.com adam
```

1. 远程系统打开一个连接。字符 O 表明此条目与打开的连接有关；字符 + 表明此条目与一个到访的连接有关。
2. 显示了连接的 IP 地址和端口号。在此条目中，接收系统（生成日志文件条目的系统）的 IP 地址为 206.184.139.12，连接到端口 25；发送系统的 IP 地址为 192.160.253.66，从端口 1244 发送。
3. 在此条目中，对于从到访 TCP/IP 通道（tcp_local）到 l 通道收件人的邮件入列，由于启用了 LOG_CONNECTION=3，故包括有默认以外的信息，应注意。特别是，发送系统在 HELO 或 EHLO 行中声明的名字，基于连接的 IP 地址的 DNS 反向查找所发现的发送系统名，以及发送系统 IP 地址，均有记录；参见第 8 篇，“配置通道定义”中关于影响此行为的通道关键字的讨论。
4. 入站连接关闭。字符 C 表明此条目与连接的关闭有关；字符 + 表明此条目与到访连接有关。

Dispatcher 调试和日志文件

Dispatcher 的错误和调试输出（如果启用的话）将被写入 MTA 日志记录目录中的 dispatcher.log 文件。

调试输出可用 Dispatcher 配置文件中的 DEBUG 选项启用，或用 IMTA_DISPATCHER_DEBUG 环境变量（UNIX）在每一进程上启用。

DEBUG 选项或 IMTA_DISPATCHER_DEBUG 环境变量（UNIX）以十六进制定义了 32 位的调试掩码。若需启用所有调试项，可将该选项设置为 -1，或将全系统的逻辑或环境变量定义为值 FFFFFFFF。每一比特的实际意义请见表 13-7。

表 13-7　Dispatcher 调试比特

比特	十六进制值	十进制值	用途
0	x 00001	1	基本服务 Dispatcher 主模块调试。
1	x 00002	2	附加服务 Dispatcher 主模块调试。
2	x 00004	4	服务 Dispatcher 配置文件记录。
3	x 00008	8	基本服务 Dispatcher 其它调试。
4	x 00010	16	基本服务调试。
5	x 00020	32	附加服务调试。
6	x 00040	64	与进程有关的服务调试。
7	x 00080	128	未用。
8	x 00100	256	基本服务 Dispatcher 和进程通信调试。
9	x 00200	512	附加服务 Dispatcher 和进程通信调试。
10	x 00400	1024	信息包级通信调试。
11	x 00800	2048	未用。
12	x 01000	4096	基本 Worker Process 调试。
13	x 02000	8192	附加 Worker Process 调试。
14	x 04000	16384	其它 Worker Process 调试，特别是连接跨区转接
15	x 08000	32768	未用。
16	x 10000	65536	基本 Worker Process 至 Service Dispatcher I/O 调试。
17	x 20000	131072	附加 Worker Process 至 Service Dispatcher I/O 调试。
20	x 100000	1048576	基本统计调试。
21	x 200000	2097152	附加统计调试。
24	x 1000000	16777216	将 PORT_ACCESS 拒绝情况记录到 dispatcher.log 文件。

Solaris 上的系统参数

系统的堆大小（datasize）必须足以容纳 Dispatcher 的线程栈用量。因为每项 Dispatcher 服务都计算 STACKSIZE*MAX_CONNS，然后总计每项服务的计算值。系统的堆大小至少需为此数的两倍。

Dispatcher 配置文件中提供的 Dispatcher 服务可影响对各种系统参数的要求。

若需显示堆大小 （即默认的 datasize），可用 csh 命令：

```
# limit
```

或用 ksh 命令

```
# ulimit -a
```

或实用程序

```
# sysdef
```

第 14 篇

MTA 故障诊断

本章介绍邮件传送代理 （MTA）故障诊断的常用工具、方法和程序。本章包括下列各节：

- 故障诊断概述
- 标准 MTA 故障诊断程序
- 常见 MTA 问题和解决方案
- 一般出错讯息
- 修复邮箱和邮箱数据库 （不同章节）

与之相关的监视程序内容可在第 15 篇，“监控 iPlanet Messaging Server”中查找。

备注	在阅读本章之前，应阅读本指南中的第 10 篇到第 6 篇以及 **iPlanet Messaging Server Reference Manual** 中有关 MTA 配置和命令行实用程序的章节。

故障诊断概述

对 MTA 进行故障诊断的首要步骤之一就是确定从何处开始诊断。视问题情况，可在日志文件中寻找出错信息。在其他情况下，可检查所有标准 MTA 处理，查看 MTA 配置，或启动和停止单个通道。不管使用什么方法，在对 MTA 进行故障诊断时需考虑如下问题：

- 配置或环境问题是否会防碍邮件的接受 （如磁盘空间或配额问题）？
- 邮件进入邮件队列时诸如 dispatcher 和作业控制器的 MTA 服务是否存在？
- 网络连通性问题或路由问题是否会引起邮件在远程系统上被滞粘或错误路由？
- 问题是在邮件进入邮件队列之前还是之后出现的？

本章将在下列小节中讨论这些问题。

标准 MTA 故障诊断程序

本节概括了 MTA 的标准故障诊断程序。如果问题没有生成出错信息或出错信息不能提供足够的诊断依据，或者只想对 MTA 进行一般的运行状态检查、测试和标准维护，可遵循使用这些程序步骤。

- 检查 MTA 配置
- 检查邮件队列目录
- 检查关键文件的所有权
- 检查确认作业控制器和 dispatcher 的运行状态
- 检查日志文件
- 手工运行通道程序
- 启动和停止单个通道
- MTA 故障诊断实例

检查 MTA 配置

使用 `imsimta test -rewrite` 实用程序检查地址配置。运用此实用程序，不实际发送邮件即可测试 MTA 的地址重写和通道映射。详细信息，请参阅 **iPlanet Messaging Server Reference Manual** 中“MTA 命令行实用程序”一章。

该实用程序通常显示将要应用的地址重写以及邮件将要入队的那个通道。然而，MTA 配置中的句法错误会使实用程序产生出错信息。如果输出不是所预期的话，则需更正配置。

检查邮件队列目录

检查邮件是否在 MTA 邮件队列目录中，典型情况下这个目录就是 */server-root*`/msg-`*instance*`/imta/queue/`.使用诸如 `imsimta qm` 这样的命令行实用程序检查 MTA 邮件队列目录下预期邮件文件的存在。有关 `imsimta qm` 的详细说明，请参阅 **iPlanet Messaging Server Reference Manual** 和第 401 页“imsimta qm 计数器”中的“MTA 命令行实用程序”一章。

如果 `imsimta test -rewrite` 的输出看起来是正确的，检查确认邮件确实位于 MTA 邮件队列子目录中。要做到这一点，需启用邮件日志记录（有关 MTA 的详细说明，请参阅第 339 页“第三部分：服务日志（MTA）”）。然后应查看 */server-root*`/msg-`*instance*`/log/imta/` 目录中的 `mail.log_current` 文件。可根据邮件 ID 跟踪一个特定邮件，以证实该邮件确放置在 MTA 邮件队列的子目录中。如果找不到该邮件，可能是文件磁盘空间或目录权限出现问题。

检查关键文件的所有权

在安装 iPlanet Messaging Server 时，应当已经选择了一个邮件服务器用户帐户 （默认 nobody）。下列目录、子目录和文件应属于此帐户：

/*server-root*/msg-*instance*/imta/queue/
/*server-root*/msg-*instance*/log/imta/
/*service-root*/msg-*instance*/imta/tmp

如下面 UNIX 系统示例中那样的命令可用于检查这些目录的保护和所有权：

ls -l -p -d /usr/iplanet/server5/msg-budgie/imta/queue

```
drwx------ 6 nobody bin 512 Feb 7 09:32
/usr/iplanet/server5/msg-budgie/imta/queue
```

ls -l -p -d /usr/iplanet/server5/msg-budgie/log/imta

```
drwx------ 2 nobody bin 1536 Mar 10 09:00
/usr/iplanet/server5/msg-budgie/log/imta
```

ls -l -p -d /usr/iplanet/server5/msg-budgie/imta/tmp

```
drwx------ 2 nobody bin 512 Feb 7 10:00
/usr/iplanet/server5/msg-budgie/imta/tmp
```

使用如下面 UNIX 系统示例中那样的命令检查确认 /*server-root*/msg-*instance*/imta/queue 中的文件属于 MTA 帐户：

ls -l -p -R /usr/iplanet/server5/msg-budgie/imta/queue

检查确认作业控制器和 dispatcher 的运行状态

MTA 作业控制器负责处理 MTA 处理作业的执行，包括大多数外发 （主）通道任务。

有些 MTA 通道，如 MTA 的多线程 SMTP 通道，包含处理进入邮件的驻留服务器进程。这些服务器为通道处理从属（进入）目录。MTA dispatcher 处理这样的 MTA 服务器的创建。dispatcher 配置选项控制服务器的有效性，已创建服务器的数量以及每个服务器可处理的连接的个数。

要检查确认作业控制器和 dispatcher 的存在和 MTA 服务器和处理作业的运行，需使用命令 `imsimta process`。在空闲条件下，该命令可使 `job_controller` 和 `dispatcher` 工作。例如：

```
imsimta process

USER      PID S   VSZ    RSS    STIME     TIME   COMMAND
mailsrv  9567  S  18416   9368   02:00:02    0:00 /opt/iplanet/
  server5/bin/msg/imta/bin/tcp_smtp_server

mailsrv  6573  S  18112   5720   Jul_13      0:00 /opt/iplanet/
  server5/bin/msg/imta/bin/job_controller

mailsrv  9568 S  18416   9432   02:00:02   0:00 /opt/iplanet/
  server5/bin/msg/imta/bin/tcp_smtp_server

mailsrv  6574 S  17848   5328   Jul_13     0:00 /opt/iplanet/
  server5/bin/msg/imta/bin/dispatcher
```

如果作业控制器不存在，于，*/server-root*/*msg*-`instance/imta/queue` 目录中的文件将得以备份，邮件也不会被传递。如果没有 dispatcher，那么将无法接受任何 SMTP 连接。

关于 `imsimta process` 的详细说明，请参阅 **iPlanet Messaging Server Reference Manual**。

如果作业控制器和 dispatcher 都不存在，应查看 */server-root*/`msg`-*instance*/`log/imta/` 目录中的 `dispatcher.log-*` 文件或 `job_controller.log-*` 文件。

如果日志文件不存在或没指示有错误，则需通过使用 `imsimta start` 命令启动进程。详细信息，请参阅 **iPlanet Messaging Server Reference Manual** 的文件 “MTA 命令行实用程序” 一章。

备注 在运行 `imsimta process` 时，不应有 Dispatcher 或作业控制器的多重实例。

检查日志文件

如果 MTA 处理作业运行正常而邮件却停留在邮件队列目录中，可检查日志文件确定问题所在。所有 MTA 日志文件均创建在 */server-root*/msg-*instance*/log/imta 目录中。各种 MTA 处理作业的日志文件名格式见表 14-1。

表 14-1　MTA 日志文件

文件名	日志文件内容
*channel*_master.log-*uniqueid*	*通道*的主程序输出 （通常为客户机）
*channel*_slave.log-*uniqueid*	*通道*的从属程序输出 （通常为服务器）
dispatcher.log-*uniqueid*	Dispatcher 调试。不管 Dispatcher 的 DEBUG 选项是否已设置，都将创建此日志。尽管如此，若想得到详细的调试信息，还是需将 DEBUG 选项设置为一个非零值。
imta	ims-ms 在传递有误处的通道出错信息。
job_controller.log-*uniqueid*	作业控制器日志记录。不管作业控制器的 DEBUG 选项是否已设置，都将创建此日志。尽管如此，若想得到详细的调试信息，还是需将 DEBUG 选项设置为一个非零值。
tcp_smtp_server.log-*uniqueid*	tcp_smtp_server. 调试。此日志中的信息只针对服务器，而不针对邮件。
return.log-*uniqueid*	针对定期 MTA 退回作业的调试输出； 如果 return_debug 选项用于 option.dat， 则创建此日志。

备注　每个日志文件在创建时都有唯一的 ID （*uniqueid*）以防覆盖用同一通道创建的早期日志文件。要找到特定的日志文件，可使用 imsimta view 实用程序。还可通过使用 imsimta purge 命令清除旧的日志文件。详细信息，请参阅 **iPlanet Messaging Server Reference Manual** 中的 “MTA 命令行实用程序” 一章。

channel _master.log-*uniqueid* 和 *channel* _slave.log-*uniqueid* 的日志文件将在下列任何一种情况下创建：

- 当前配置中有错误。
- master_debug 或 slave_debug 关键字设置在 imta.cnf 文件的通道上。
- 如果 mm_debug 被设置为一个非 0 值 （mm_debug > 0）于文件 option.dat 中 （在目录：*/server-root*/*msg*-instance/imta/config/）。

有关调试通道主代理和从属程序的详细说明，请参阅 **iPlanet Messaging Server Reference Manual**。

手工运行通道程序

在诊断 MTA 传递问题时，手工运行一个 MTA 传递任务是很有用的，特别是在为一个或多个通道启用了调试功能之后。

`imsimta submit` 命令会通知 MTA 作业控制器运行通道。如果为有问题的通道启用了调试功能，`imsimta submit` 将在 */server-root*`/msg-`*instance*`/log/imta` 目录下生成一个日志文件，如表 14-1 所示。

`imsimta run` 命令将为当前活动进程下的通道执行输出指向终端机的出站传递。这可能比提交一个任务更简便，尤其在问题可能存在于任务提交本身时。

备注	为了手工运行通道，作业控制器必须处于运行状态。

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 **iPlanet Messaging Server Reference Manual** 一章中的 “MTA 命令行实用程序”。

启动和停止单个通道

在某些情况下，停止和启动单个通道也许会使邮件队列问题更容易诊断和调试。停止邮件队列能检查列队邮件，以确定是否有循环或垃圾邮件攻击的存在。

停止一个特定通道的出站处理 （出队）

1. 使用 `imsimta qm stop` 命令停止一个特定通道。这样做可不必停止作业控制器，也不必重新编译配置。在下面的例子中， `conversion` 通道被停止：

   `imsimta qm stop conversion`

2. 要继续执行处理，需使用 `imsimta qm start` 命令重新启动通道。在下面的例子中，`conversion` 通道被启动：

   `imsimta qm start conversion`

有关 `imsimta qm start` 和 `imsimta qm stop` 命令的详细说明，请参阅 **iPlanet Messaging Server Reference Manual** 中关于 MTA 命令行实用程序的那一章。

停止来自特定域或 IP 地址 （入列到一通道的）的入站处理

在将临时 SMTP 的错误返回客户主机时，若想停止针对一个特定域或 IP 地址的入站邮件处理，可运行下列程序之一。这样邮件将不会保留在系统内。请参阅第 235 页 “第一部分：映射表”。

- 要想停止一特定主机或域名的入站处理，需在 MTA 映射文件中的 ORIG_SEND_ACCESS 映射表 （特别是 */server-root*/msg-*instance*/imta/config/mappings）中添加下列访问规则：

```
ORIG_SEND_ACCESS

    *|*@sesta.com|*|*              $X4.2.1|$NHost$ blocked
```

  通过使用此程序，发件人的远程 MTA 会在它们的系统中保留邮件，并继续定期的重新发送这些邮件，直到重新启动入站处理为止。

- 要停止一特定 IP 地址的入站处理，需在 MTA 映射文件中的 PORT_ACCESS 映射表（特别是 */server-root*/msg-*instance*/imta/config/mappings）中添加下列访问规则：

```
PORT_ACCESS

    TCP|*|25|IP_address_to_block|*                $N500$ unable$ to$ \
    connect$ at$ this$ time
```

若要重新启动来自域或 IP 地址的入站处理，需确保将这些规则从映射表中移出并重新编译配置。此外，您可能希望为每个映射表创建唯一的出错信息。这样做可以确定正在使用的是哪个映射表。

MTA 故障诊断实例

本节介绍如何一步一步地对特定的 MTA 问题进行故障诊断。在本例中，收件人没有收到邮件的附件。注意：为了和 MIME 协议术语保持一致，本节中将 “附件”称为 “邮件部分”。上述故障诊断技术用于识别邮件部分在何处和为何消失。（请参阅第 360 页“标准 MTA 故障诊断程序”）。通过使用下列步骤，可确定邮件通过 MTA 的路径。此外，也可确定邮件部分是在邮件进入邮件队列之前还是之后消失的。要做到这一点，需以手动方式停止和运行通道，捕获相关文件。

备注 用手动方式启动的邮件通过通道时，必须运行作业控制器。

识别邮件路径中的通道

通过识别邮件路径中有那些通道，可将 `master_debug` 和 `slave_debug` 两个关键字用于相应的通道。这些关键字在通道的主日志文件和从属日志文件中生成调试输出；而主程序和从属程序的调试信息又反过来有助于识别邮件部分的消失点。

1. 把 `log_message_id=1` 添加到 `/`*server-root*`/msg-`*instance*`/imta/config.` 目录下的 `option.dat` 文件中。使用这个参数，就可以查看邮件 ID：在 `mail.log_current` 文件中的标题行。
2. 运行 `imsimta cnbuild` 来重新编译配置。
3. 运行 `imsimta restart dispatcher` 来重新启动 SMTP 服务器。
4. 让最终用户重发带邮件部分的邮件。
5. 确定邮件经过的通道。

   尽管有不同方法识别通道，建议使用如下方法：

   a. 在 UNIX 平台上，用 `grep` 命令查找邮件 ID：在目录 `/`*server-root*`/msg-`*instance*`/log/imta/` 中的 `mail.log_current` 文件中的标题行。在 Windows NT 平台上，使用 `find` 命令。

   b. 一旦找到邮件 ID：标题行，寻找 E （入队）和 D （出队）记录以确定邮件路径。有关记录日志条目代码的详细说明，请参阅第 341 页 “MTA 日志条目格式”。有关此例，请参阅下列 E 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 ...
```

左侧通道是源通道，右侧通道是目标通道。此例中， E 和 D 记录表示邮件路径是从通道 `tcp_local` 到通道 `conversion`，最后到通道 `tcp_intranet`。

手工启动和停止通道以收集数据

本节介绍如何手工启动和停止通道。有关详情，请参阅第 364 页“启动和停止单个通道”。通过手工启动和停止邮件路径中的通道，可在 MTA 处理的不同阶段保存邮件和日志文件。这些文件以后用于第 368 页 “识别邮件崩溃点”。

1. 在 */server-root*/msg-*instance*/imta/config 目录下的 option.dat 文件中设置 mm_debug=5，以提供详实的调试信息。
2. 把 slave_debug 和 master_debug 这两个关键字添加到 */server-root*/msg-*instance*/imta/config 目录下的 imta.cnf 文件中的相应通道中。
   a. 从发送带有邮件部分的邮件的远程系统将 slave_debug 关键字用于入站通道 （或邮件在初始会对话过程中切换到的任何通道）上。在此例中，slave_debug 关键字被添加到 tcp_local 通道。
   b. 把 master_debug 关键字添加到其他邮件经过并在第 366 页“识别邮件路径中的通道”被识别的通道上。在此例中，master_debug 关键字应添加到 conversion 和 tcp_intranet 通道上。
   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 这两个命令手工启动和停止特定的通道。有关使用这些关键字的详细说明，请参阅第 364 页 “启动和停止单个通道”。
4. 启动捕获邮件文件的进程，并让最终用户重发带邮件部分的邮件。
5. 在邮件进入一个通道时，如果已被 imsimta qm stop 命令停止则会在通道中停止。有关详细信息，请参阅 3。
   a. 在手工运行邮件路径的下一个通道之前，复制并重新命名邮件文件。请看下面这个 UNIX 平台的例子：

      # cp ZZ01K7LXW76T7O9TD0TB.00 ZZ01K7LXW76T7O9TD0TB.KEEP1

      邮件文件通常驻留在类似于 */server-root*/msg-*instance*/imta/queue/*destination_channel*/001 等目录中。 *destination_channel* 是邮件要通过的下一个通道 （例如：tcp_intranet）。如果希望在 *destination_channel* 目录中创建子目录（如 001， 002 等），需将关键字 subdirs 添加到通道。
   b. 建议每次捕获和复制邮件时利用扩展名对邮件进行编号，以便识别邮件处理的顺序。
6. 重新执行通道中邮件处理，并入队到下一个邮件路径的目标通道。要实现此步骤，需使用 imsimta qm start 命令。
7. 复制并保存相关通道的日志文件（例如：tcp_intranet_master.log-*），日志文件位于 */server-root*/msg-*instance*/log/imta/. 目录下。选择具备所跟踪邮件数据的适当的日志文件。确保所复制的文件与邮件进入通道时的时间戳和主题标题相匹配。
   以 tcp_intranet_master.log-* 为例，可将文件保存为 tcp_intranet_master.keep，这样文件就不会被删除。

8. 重复步骤 5 ~ 7 直到邮件到达其最终目的地。

   在步骤 7 中复制的日志文件应与在步骤 5 中复制的邮件文件相关联。假设停止了所有丢失邮件部分的通道，则应保存 conversion_master.log-* 和 tcp_intranet_master.log-* 文件。还应保存源通道日志文件 tcp_local_slave.log-*。此外，应在每个目标通道保存相关邮件文件的副本：来自 conversion 通道的 ZZ01K7LXW76T7O9TD0TB.KEEP1 和来自 tcp_intranet 通道的 ZZ01K7LXW76T7O9TD0TB.KEEP2。

9. 邮件文件和日志文件一经复制就移除调试选项。

   a. 将 slave_debug 和 master_debug 关键字从 /*server-root*/msg-*instance*/imta/config 目录下 imta.cnf 文件中的相应通道中移除。

   b. 重新设置 mm_debug=0，并将 /*server-root*/msg-*instance*/imta/config 目录下 option.dat 文件中的 log_message_id=1 移除。

   c. 用 imsimta cnbuild 重新编译配置。

   d. 运行命令 imsimta restart dispatcher 重新启动 SMTP 服务器。

识别邮件崩溃点

1. 当完成启动和停止通道程序后，应已具备下列可用来对问题进行故障诊断的文件：

   a. 来自每个通道程序的所有邮件副本 （例如：ZZ01K7LXW76T7O9TD0TB.KEEP1）。

   b. tcp_local_slave.log-* 文件

   c. 每个目标通道的一套 *channel*_master.log-* 文件

   d. 表示邮件路径的一套 mail.log_current 记录

   所有文件都应具有与邮件 ID 相匹配的时间戳和邮件 ID 值：mail.log_current 记录中的标题行。注意当邮件退回发件人时例外，这些退回的邮件会具有与原邮件不同的邮件 ID 值。

2. 检查 tcp_local_slave.log-* 文件以确定邮件在进入邮件队列时是否有邮件部分。

   观察 SMTP 对话和数据以发现从客户机发送来的是什么。

   如果邮件部分没有在 tcp_local_slave.log-* 文件中出现，那么问题出在邮件进入 MTA 之前。这就造成邮件在没有邮件部分的情况下入队。如果是这种情况，问题可能已出现在发件人的远程 SMTP 服务器上或发件人的客户机上。

3. 调查邮件文件副本以发现邮件部分在何处被更改或丢失。

   如果任何邮件文件显示邮件部分被更改或丢失，需检查上一个通道的日志文件。例如，如进入到 tcp_intranet 通道的邮件的邮件部分被更改或丢失，则应查看 conversion_master.log-* 文件。

4. 查看邮件的最终目的地。

   如果邮件部分看上去在 tcp_local_slave.log，邮件文件（例如：ZZ01K7LXW76T7O9TD0TB.KEEP1），以及 *channel*_master.log-* 文件中没有改变的话，那么 MTA 没有更改邮件，邮件部分在通向最终目的地路径的下一个步骤时消失。

   如果最终目的地是 ims-ms 通道（邮件存储库），那么可从服务器下载邮件到客户机，以此确定邮件部分是否在这一传输过程中或在这之后丢失。如果目标通道是 tcp_* 通道，那么应转到邮件路径中的 MTA。假设它是一个 iPlanet Messaging Server MTA，则应重复整个故障诊断过程。（请参阅第 366 页 “识别邮件路径中的通道”，第 367 页 “手工启动和停止通道以收集数据”，和本节）如果那个 MTA 不在管理范围内，那么报告问题的用户应与该特定网站联系。

常见 MTA 问题和解决方案

本节列出了 MTA 配置和操作的常见问题和解决方案。

- 更改对配置文件或 MTA 数据库不生效
- MTA 可发送外发的邮件但不接收入站邮件
- 外来 SMTP 连接超时
- 邮件未入队
- MTA 邮件未传递
- 循环邮件
- 接收的邮件为编码邮件
- 服务器端规则 （SSR）不生效

更改对配置文件或 MTA 数据库不生效

如果对配置、映射、转换、安全、选项或别名文件的更改不生效，则应检查是否执行了下列步骤：

1. 重新编译配置 （通过运行 imsimta cnbuild）。
2. 重新启动相应进程 （例如 imsimta restart dispatcher）。
3. 重新创建任何客户连接

MTA 可发送外发的邮件但不接收入站邮件

大多数 MTA 通道依靠从属程序（或称通道程序）接收入站邮件。有关 MTA 支持的一些传输协议（比如 TCP/IP 和 UUCP），应确保传输协议激活 MTA 从属程序而不是它的标准服务器。将自带的 `sendmail` SMTP 服务器替换为 MTA SMTP 服务器作为 iPlanet Messaging Server 安装的一部分来执行。详细信息，请参阅针对 **UNIX 的 iPlanet Messaging Server Installation Guide**。

对于多线程 SMTP 服务器来说， SMTP 服务器的启动受 Dispatcher 控制的。如果 Dispatcher 配置使用的 `MIN_PROCS` 值大于或等于 SMTP 服务的那个值，那么总应有至少一个 SMTP 服务器进程在运行（可能更多，这取决于 SMTP 服务的 `MAX_PROCS` 值）。`imsimta process` 命令也可用于检查 SMTP 服务器进程的存在。详细说明，请参阅 **iPlanet Messaging Server Reference Manual** 中关于 MTA 命令行实用程序一章。

外来 SMTP 连接超时

外来 SMTP 连接超时常常与系统资源及其分配相关。下列技术可用语识别外来 SMTP 连接超时的原因：

1. 检查可允许多少外来 SMTP 连接同时存在。这是由 `MAX_PROCS` 和 `MAX_CONNS` 这两个 SMTP 服务的 dispatcher 设置控制的；允许同时存在的连接数量即为 `MAX_PROCS*MAX_CONNS`。若可提供系统资源，在使用效率过低的情况下可考虑增加该连接数量。
2. 另一个可使用的技术是打开 TELNET 会话。在下面的例子中，用户连接到 `127.0.0.1` 端口 25。一旦连接上， 220 标志区即被退返回。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 (iPlanet Messaging Server 5.1
(built May 7 2001))
```

如果已连接上并接收了一个 220 标志区，但附加命令（如 `ehlo` 和邮件发件人）没有响应，那么应运行 `imsimta test -rewrite` 以保证配置正确。若正在使用 `imsimta dirsync` 命令，应确保此命令最近运行过。有些情况下，假设 `dirsync` 失败， SMTP 服务器中的命令不接收响应。在这种情况下，只要首先移除 `dirsync` 锁定文件，运行 `imsimta dirsync -F` 就会解决问题。

3. 如果 220 标志区的响应时间较慢，并且在 SMTP 服务器上运行 pstack 命令显示以下 iii_res* 功能 （这些功能表明正在执行一名字解析查找。）：

```
febe2c04 iii_res_send (fb7f4564, 28, fb7f4de0, 400, fb7f458c,
fb7f4564) + 142c
febdfdcc iii_res_query (0, fb7f4564, c, fb7f4de0, 400, 7f) + 254
```

那么主机很可能按相反顺序进行名字解析查找，即使是在像 localhost/127.0.0.1 的常见名字对。要防止类似的性能降低，应重新排列 /etc/nsswitch.conf 文件中的主机查找。这需要更改来自 /etc/nsswitch.conf 文件中的下列各行，从：

```
hosts: dns nis [NOTFOUND=return] files
```

到：

```
hosts: files dns nis [NOTFOUND=return]
```

在 /etc/nsswitch.conf 文件中进行这种更改可提高性能。让较少的 SMTP 服务器不得不处理邮件，而不是让太多的 SMTP 服务器不得不执行不必要的查找。

4. 也可将 slave_debug 关键字放置在处理跨越 TCP/IP 的外来 SMTP 邮件的通道上，通常就是 tcp_local 和 tcp_intranet。这样做之后，查看最新的 tcp_local_slave.log-*uniqueid* 文件以识别超时邮件的任何特殊特征。例如，若带有大量收件人的来件超时，可考虑在通道上使用 expandlimit 关键字。

记住，如果系统超过负荷并过度扩展，超时是难以完全避免的。

邮件未入队

在 TCP/IP 传递中遇到的错误通常是瞬时的； MTA 在遇到问题时一般会保留邮件并定期重试。在某些主机上经历周期性中断的同时其他主机连接工作良好，这对于大型网络是很常见的。要想验证此问题，需检查日志文件中与传递尝试相关的错误。可看到诸如 “Fatal error from smtp_open” 之类的出错信息。类似错误并非罕见并通常与瞬时性网络问题相关。若需调试 TCP/IP 网络问题，可使用诸如 PING、 TRACEROUTE 和 NSLOOKUP 这类的实用程序。

下面的例子显示的的步骤可用来发现为何一邮件滞留在队列中等待传递到 xtel.co.uk。要确定邮件为何没有出队，可重新创建 MTA 用来跨越 TCP/IP 传递 SMTP 的步骤。

```
% nslookup -query=mx xtel.co.uk  (1)

Server: LOCALHOST
Address: 127.0.0.1

Non-authoritative answer:
XTEL.CO.UK  preference = 10, mail exchanger = nsfnet-relay.ac.uk (2)

% telnet nsfnet-relay.ac.uk 25 (3)
Trying... [128.86.8.6]
telnet: Unable to connect to remote host: Connection refused
```

1. 使用 NSLOOKUP 实用程序检查本主机存在什么 MX 记录，如果有的话。如果不存在 MX 记录，那么应尝试直接连接到主机。如果存在 MX 记录，则必须连接到指定的 MX 转发上。 MTA 首先满足首选的 MX 信息，除非明确配置不这样做。还可参阅第 180 页“TCP/IP MX 记录支持”。
2. 在此例中，DNS（域名服务）返回 xtel.co.uk 的指定 MX 转发的名称。这是 MTA 实际连接的主机。如果列出不止一个 MX 转发，MTA 会依次尝试每个 MX 记录，最先尝试带有最小的首选值的记录。
3. 如果确实已连接到远程主机，则应检查该主机是否通过使用 TELNET 接受入站 SMTP 连接到 SMTP 服务器端口 25。

备注 如果在没有指定端口的情况下使用 TELNET，将发现远程主机接受普通的 TELNET 连接。这并不表明该主机也接受 SMTP 连接；很多系统都接受常规的 TELNET 连接但却拒绝接受 SMTP 连接，反之亦然。因此，应对 SMTP 端口进行不可缺省的测试。

在上一个例子中，远程主机拒绝接受到 SMTP 端口的连接。这就是 MTA 无法传递邮件的原因。连接被拒绝可能是由于远程主机的错误配置或远程主机上的某种资源耗尽。在这种情况下，无法在本地解决问题。通常应让 MTA 继续重试传递邮件。

如果在不使用 DNS 的 TCP/IP 网络上运行 iPlanet Messaging Server，可省略步骤 （1）和（2）。作为替代，可使用 TELNET 直接访问有问题的主机。注意应使用与 MTA 所用相同的主机名。查看从 MTA 最后一次尝试开始的相关日志文件以确定主机名。如果正在使用主机文件，则应确保主机名信息是正确的。我们强烈建议您使用 DNS 而不是主机名。

注意如果在使用交互式测试检测 TCP/IP 主机连通性时没有遇到问题，那么很可能在 MTA 的最后尝试传递邮件的过程中问题就已经解决了。可在适当通道上重新运行 imsimta submit tcp_channel 以查看邮件是否正在出队。

MTA 邮件未传递

除了邮件传输问题，还有两个常见可造成邮件队列邮件不被处理的问题：

1. 队列缓存与队列目录中的邮件不同步。等待传递的 MTA 队列子目录中的邮件文件被输入到内存中的队列缓存中。通道程序在运行时会参考这个队列缓存来确定要传递队列中的哪些邮件。也会有这样的情况：队列中有邮件文件，但却没有相应的队列缓存条目。

   a. 要检查证实一特定文件是否存在于队列缓存中，可使用 `imsimta cache -view` 实用程序；如果文件不在队列缓存中，那么队列缓存就需要进行同步。

   队列缓存通常每四个小时同步一次。如有必要，可使用 `imsimta cache -sync.` 命令手工重新同步缓存。一经同步，通道程序就会在处理完新邮件之后处理原先未处理的邮件。如果希望更改默认同步间隔时间 （4 小时），则应修改 */server-root*`/msg-`*instance*`/imta/config` 目录下的 `job_controller.cnf` 文件，在文件中添加 `sync_time=`*timeperiod*，其中 *timeperiod* 反映了进行队列缓存同步的频度。注意 *timeperiod* 必须大于 30 分钟。在下面的例子中，通过把 `sync_time=02:00` 添加到 `job_controller.cnf` 中的 global defaults（全局默认设置）节，队列缓存间隔时间被修改为 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
```

   可在运行 `imsimta cache -sync` 后运行 `imsimta submit` *channel* 清除待处理邮件。请注意如果待处理邮件过大（大于 1000）的话，清除过程可能需要较长时间，这一点很重要。

   要获取队列缓存的概括信息，可运行 `imsimta qm -maint dir -database -total`。

   b. 如果在将队列缓存同步后，邮件仍未传递，则应重新启动作业控制器。这就需要运行 `imsimta restart job_controller` 命令。

   重新启动作业控制器会导致邮件数据结构在磁盘邮件队列上的重建。

注意 重新启动作业控制器是一较极端的步骤，应在所有其他方法全部试过无效之后方可执行。

有关作业控制器的详细说明，请参阅第 88 页 “作业控制器”。

2. 由于不能创建其处理日志文件，通道处理程序无法运行。请查看访问权限，磁盘空间和配额。

循环邮件

如果 MTA 检测出一邮件是循环的，该邮件将被退出作为 .HELD 文件。请参阅第 374 页“诊断和清理 .HELD 邮件”。某些情况可导致产生 MTA 无法检测的邮件循环。

第一步是确定邮件为何循环。应当在有问题邮件文件还在 MTA 队列区域时查看该文件的一个副本，查看与有问题邮件相关的 MTA 邮件日志条目 （如果在有问题通道的 MTA 通道配置文件中启用了 `logging` 通道关键字的话），以及查看有问题通道的 MTA 通道调试日志文件。确定有问题邮件的发件人：和收件人：地址，查看收件箱：标题行，并查看邮件结构（邮件内容封装类型），均可帮助查明所遇到的邮件循环属于哪种类型。

一些更常见的情况包括：

1. Postmaster 地址损坏

   MTA 要求 Postmaster 地址是一个可接收邮件的功能地址。如果发送给邮件管理员的邮件是循环的，需查看配置中是否具有一个指向可接收邮件的帐户的正确 Postmaster 地址。

2. 剥离收件箱：标题行是为了防止 MTA 检测循环邮件。

   常规邮件循环的检测是基于收件箱标题行的。如果收件箱标题行被剥离 （显式地针对 MTA 系统自身，或针对类似与防火墙的另一系统），则会干扰邮件循环的正确检测。在这些情况下，需检查是否有不希望的收件箱标题行剥离的发生。还要检查邮件发生循环的深层原因。可能的原因包括：系统名分配问题或系统未配置为能辨识其自有名称的变体，DNS 问题，有问题系统缺少可靠的地址信息，用户地址转发错误等。

3. 其他邮件系统对通知邮件的错误处理正在生成再包装邮件以响应通知邮件。

   Internet 标准要求通知邮件（正在传递或退回邮件的报告）具有一个空的信封发件人：地址以防邮件循环。然而，一些邮件系统没有正确处理这样的通知邮件。在转发或退回通知邮件时，这些邮件系统可能会插入一个新的信封发件人：地址。这就会导致邮件循环。解决方法是修正错误处理通知邮件的那个邮件系统。

诊断和清理 .HELD 邮件

如果 MTA 检测出邮件在服务器和通道之间正进行退回处理，传送将被暂停，邮件将被储存在 */server-root*`/msg-`*instance*`/imta/queue/`*channel* 中的后缀为 .HELD 的文件中。通常，邮件循环的出现是因为每个服务器或通道都认为另外的服务器有责任传送邮件。

例如，一个最终用户可能会设置一选项把两个不同邮件主机上的邮件相互转发。在其 `sesta.com` 帐户上，最终用户启用目标为他的 `varrius.com` 帐户的邮件转发。然后，在忘了已启用了这一设置的情况下，该最终用户又在其 `varrius.com` 帐户上设置目标为 `sesta.com` 帐户的邮件转发。

MTA 的错误配置也可能导致循环。例如， MTA 主机 X 认为 `mail.sesta.com` 的邮件发给了主机 Y，但是主机 Y 认为主机 X 应该处理 `mail.sesta.com` 的邮件 ；结果就是，主机 Y 把邮件退回给主机 X。

在这种情况下，邮件被 MTA 忽略且不会继续尝试传送。出现这种问题时，查看邮件的标题行以确定哪个服务器或通道退回了邮件。必要时可修改条目。

可以按下列步骤重试 .HELD 邮件：

1. 将扩展名 .HELD 重命名为除 00 外的任意两个数字。例如，把 .HELD 改成 .06。

备注 在重命名 .HELD 文件前，确定邮件已经停止循环。

2. 运行 `imsimta cache -sync`。运行这一命令可以更新缓存。
3. 运行 `imsimta submit` *channel* 或 `imsimta run` *channel*。

也许要重复执行这些步骤，因为邮件有可能再次被标记为 .HELD，原因是收件箱：标题行的累积。

接收的邮件为编码邮件

MTA 发出的邮件以编码格式接收。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?=
```

在用 MTA 解码器命令 `imsimta decode` 读取时，这些邮件在显示时为未编码邮件。有关详情，请参阅 **iPlanet Messaging Server Reference Manual**。

RFC 821 规定，SMTP 协议只允许 ASCII 字符（一种七位字符集）的传输。事实上，在未经协调的情况下通过 SMTP 传输八位字符是非法的，并且都知道会给 SMTP 服务器带来一系列问题。例如，SMTP 服务器可能产生计算限制循环。邮件会一遍一遍地被发送。八位字符可以使 SMTP 服务器崩溃。最后，八位字符集将使不能处理八位字符数据的浏览器和邮箱崩溃。

过去，SMTP 客户在处理包含八位数据的邮件时只有三种选择：将其作为无法传递邮件退回发件人，将邮件编码，或者将其发送造成对 RFC 821 的直接违规。但是有了 MIME 和对 SMTP 的扩展，现在有标准编码方法，可以用来利用 ASCII 字符集给八位数据编码。

在上面的例子中，收件人接收到一个其 MIME 内容类型为 TEXT/PLAIN 的编码邮件。远程 SMTP 服务器（MTA SMTP 客户机向其传输邮件）不支持八位数据的传输。由于原邮件包含八位字符， MTA 不得不对邮件进行编码。

服务器端规则 （SSR）不生效

一过滤器是由一个或多个应用于邮件的条件操作组成的。由于过滤器是在服务器上储存和检测的，因而常常被称为服务器端规则 （SSR）。

目录同步命令 （imsimta dirsync）用有关用户过滤器的信息更新 MTA 的 SSR 数据库。SSR 数据库存放短过滤器 （小于 1016 字节）而一个 LDAP DN 则用于长过滤器。请注意，只有在 imsimta dirsync 命令更新了目录服务器之后，MTA 才能识别用户过滤器的更改。有关 SSR 的详细说明，请参阅第 255 页 “第二部分：邮箱过滤器”。

这一部分包括有关以下 SSR 主题的信息：

- 测试 SSR 规则
- 故障诊断程序
- 常见语法问题

测试 SSR 规则

- 要检查 MTA 的用户过滤器，用命令：

```
# imsimta test -rewrite -debug -filter user@domain
```

在输出内容中寻找以下信息：

```
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，可以把关键字 slave_debug 添加在 tcp_local 通道上以观察过滤器是如何应用的。结果将显示在 tcp_local_slave.log 文件中。一定要把 mm_debug=5 添加到 */server-root*/msg-*instance*/imta/config 目录下的 option.dat 文件中，以便获得足够的调试信息。

故障诊断程序

在诊断 SSR 问题时一定要遵循下列程序：

- 使用 `imsimta dirsync` 命令时，一定要确认 `ims-ms` 通道是有标记的过滤器。
  `ssrd:$a`
  和
  `fileinto $u+$s@$d`
  在 */server-root*`/msg-`*instance*`/imta/config` 目录下的 `imta.cnf` 文件中。
- 使用 `imsimta dirsync` 命令时，确认 `imsimta dirsync` 命令能正确同步过滤器信息。这需要从 */server-root*`/msg-`*instance*`/.` 目录执行以下命令。一定要作为邮件服务器用户来执行这些命令：

```
# configutil -l -o service.imta.ssrenabled -v true
OK SET
# configutil | fgrep ssr
local.imta.ssrenabled = yes
service.imta.ssrenabled = true
```

常见语法问题

- 如果过滤器出现了语法问题，查看 `tcp_local_slave.log-*` 文件中的下列信息：
  `Error parsing filter expression:...`
  - 如果过滤器正常，过滤器信息在输出的末尾。
  - 如果过滤器不正常，以下出错信息将出现在输出的末尾：
    ```
    Address list error -- 4.7.1 Filter syntax error:
        desdaemona@sesta.com
    ```
    而且，如果过滤器不正常， SMTP RCPT TO 命令将返回一个临时性出错应答代码：

```
RCPT TO:user@domain
452 4.7.1 Filter syntax error
```

一般出错讯息

MTA 不能启动时，一般出错讯息出现在命令行上。在这部分中介绍和诊断一般出错讯息。

备注	要诊断 MTA 配置须，使用 `imsimta test -rewrite -debug` 实用程序来检查 MTA 的地址重写和通道映射处理。使用这一实用程序可以在不发送邮件的情况下检查配置。请参阅第 360 页 “检查 MTA 配置”。

MTA 的副组件也可能导致本章中没有介绍的出错讯息的产生。请参阅 **iPlanet Messaging Server Reference Manual** 中有关 MTA 命令行实用程序和配置的章节，有关各个副组件的详细说明，参见第 6 篇到第 10 篇各章。这章包括下列出错类型：

- mm_init 中的错误
- 编译的配置版本不匹配
- 交换空间错误
- 文件打开或创建错误
- 非法主机 / 域错误
- SMTP 通道中的错误：os_smtp_* errors

mm_init 中的错误

mm_init 中的错误通常表明 MTA 配置有问题。运行 `imsimta test -rewrite` 实用程序这些错误就会被显示出来。如 `imsimta cnbuild` 这样其他实用程序，通道、服务器或浏览器也都可能返回这样的错误。

常见的 mm_init 错误包括：

- 错误别名等价
- 不能打开别名文件
- 发现重复别名
- 在通道表里的重复主机
- 发现重复映射名
- 映射名过长
- 初始化 ch_facility 时出错：编译的字符集版本不匹配
- 初始化 ch_facility 时出错：无空间
- 本地主机别名或固有名称对系统过长
- 别名没有等价地址
- 通道没有正式主机名
- 正式主机名过长

错误别名等价

别名文件条目的右侧格式错误。

不能打开别名文件

包含于别名文件内的文件无法打开。

发现重复别名

两个别名文件条目左侧一样。须找到并取消复制。寻找如下出错讯息：`error line #XXX` 其中 `XXX` 是行号。修正这一行上的重复别名。

在通道表里的重复主机

出错讯息说明 MTA 配置有两个正式主机名相同的通道定义。

注意，MTA 配置文件（`imta.cnf`）中的重写规则（上半部分）里的多余的空行可使 MTA 把配置文件的剩余部分视为通道定义。一定要保证文件的第一行不是空行。因为很多重写规则有相同的模式（左侧），MTA 据此把它们视为有着非唯一正式主机名的通道定义。检查 MTA 配置，看是否存在任何有重复正式主机名的通道定义以及文件上半（重写规则）部分是否有不正确的空行。

发现重复映射名

这个讯息说明两个映射表有相同的名称，其中一个重复映射表应移除。但是映射表中的格式错误有可能使 MTA 把别的内容误认为是映射表名。例如，对映射表条目的错误缩排会让 MTA 认为条目左侧其实是映射表名。检查映射文件的一般格式和映射表名。

备注	应以一空行打头，后随任何带映射表名的行。但是映射表条目之间不得有任何空行。

映射名过长

这个错误表示映射名太长应该缩短。映射文件格式错误可能会使 MTA 把其他内容误认为是映射表名。例如，对映射表条目的错误缩排会让 MTA 认为条目左侧其实是映射表名。检查映射文件和映射表名。

初始化 ch_facility 时出错：编译的字符集版本不匹配

这一讯息说明，需要用命令 `imsimta chbuild`. 重新编译并重新安装编译的字符集表。有关详情，请参阅 **iPlanet Messaging Server Reference Manual**。

初始化 ch_facility 时出错：无空间

这一出错讯息一般表示需调整 MTA 字符集内部表的大小然后重建编译的字符集表，需使用的命令如下：

```
imsimta chbuild -noimage -maximum -option
imsimta chbuild
```

请核实，进行此更改之前没有重新编译或重新启动任何别的内容。参考 **iPlanet Messaging Server Reference Manual** 中 “MTA 命令行实用程序”一章可获得更多的关于 `imsimta chbuild` 的信息。

本地主机别名或固有名称对系统过长

这一错误说明本地主机别名或固有名称太长 （在一通道块的第二个及随后的名称中的可选右侧） 。但是 MTA 配置文件里早先的一些语法错误 （比如重写规则里的多余的空行）可能使 MTA 把其它内容误认为是通道定义。除了检查配置文件里所提到的那行外，也要检查这一行以上的内容以便找到其他语法错误。特别是当 MTA 发现错误的那一行原本是一条重写规则时，一定要检查在它上面是否有多余的空行。

别名没有等价地址

别名文件的条目没有右侧 （翻译值）部分。

通道没有正式主机名

这一错误说明，一通道定义块缺少必需的第二行（正式主机名行）。有关通道定义块的详细信息，请见 **iPlanet Messaging Server Reference Manual** 和第 8 篇，“配置通道定义”中的有关 MTA 配置和命令行实用程序的章节。每个通道定义块的前后都必需有一空行。但是在块通道名和通道定义的正式主机名行之间不能出现空行。还要注意，MTA 配置文件的重写规则部分不允许有空行。

正式主机名过长

通道的正式主机名 （通道定义块的第二行）长度限制在四十字节内。如想让通道的正式主机名超过这个长度，把它缩短成一个占位名称，然后用重写规则使长名称和短正式名称匹配。这种情况在处理 `l` （本地）通道主机名时可能出现。例如：

原始通道 1：

```
!delivery channel to local /var/mail store
l subdirs 20 viaaliasrequired maxjobs 7 pool LOCAL_POOL
newt.salamander.lizard.gecko.komododragon.com
```

创建占位名：

```
!delivery channel to local /var/mail store
l subdirs 20 viaaliasrequired maxjobs 7 pool LOCAL_POOL
newt
```

创建重写规则：

```
newt.salamander.lizard.gecko.komododragon.com    $U%$D@newt
```

注意，当使用 `l` （本地）通道时，需要使用反向映射表。有关用法和语法的信息，请参阅 **iPlanet Messaging Server Reference Manual** 中的 “MTA 配置”一章。

MTA 配置文件中早期的一些语法错误（例如，重写规则里多余的空行）可能使 MTA 把其他内容误认成通道定义。这可能导致一原本为重写规则的文本被误认成正式主机名。除了检查配置文件里所提到的那行外，也要检查这一行以上的内容以便找到其他语法错误。特别是当 MTA 发现错误的那一行原本是一条重写规则时，一定要检查在它上面是否有多余的空行。

编译的配置版本不匹配

`imsimta cnbuild` 实用程序的功能之一就是把 MTA 配置信息编译成可以快速装载的图像。编译格式定义得十分严格并且在不同的 MTA 版本之间经常更改。小的更改可能作为补丁版的一部分出现。

当进行这种更改时，一内部版本字段也被更改，以便检测出不相容的格式。当检测出不相容格式时， MTA 组件就会中断并显示上面的错误。解决这个问题的办法就是用命令 `imsimta cnbuild` 生成一个新的编译的配置。

另一个不错的办法是用 `imsimta restart` 命令来重新启动任何驻留的 MTA 服务器进程，这些进程即可获取更新了的配置信息。

交换空间错误

为了确保正确操作，应在邮件传输系统上配置足够的交换空间。配置不同，必需的交换空间大小也不同。一个一般适用的建议是：交换空间至少应为主要内存的三倍。

下面的出错信息表明缺少交换空间：

```
jbc_channels: chan_execute [1]: fork failed: Not enough space
```

在作业控制器的日志文件可能会看到这样的出错信息。其他交换空间错误因配置不同而有所不同。

使用下列命令可以确定还剩多少交换空间和已经用了多少交换空间：

- Solaris 系统：`swap -s`（当 MTA 进程忙碌时）， `ps -elf`，或 `tail /var/adm/messages`
- HP-UX 系统：`swapinfo` or `tail /var/adm/syslog/syslog.log`
- Windows NT 系统：如果在别处需要更大空间或速度更快的驱动器，可以在默认硬盘之外的驱动器上设置页面调度文件大小（例如 `C:\`）。检查可用空间或设置新的页面调度文件大小，遵循以下步骤：
  - 转至控制面板单击 System Properties （系统属性）或 System （系统）。
  - 单击 Performance （性能）选项卡。
  - 单击 Change in the Virtual Memory （在虚拟内存中更改）节。
  - Virtual Memory （虚拟内存）窗口将提供每个驱动器的页面调度文件大小。

文件打开或创建错误

为了发送一封邮件，MTA 读取配置文件并在 MTA 邮件列队目录中创建邮件文件。对于 MTA 或其他用非 MTA 的 SDK 写的程序，配置文件都必须是可读的。在安装过程中，已给这些文件赋予了适当的权限。可创建配置文件的 MTA 实用程序和其他程序也赋予权限。如果文件受系统管理者、其他授权用户或通过针对站点的程序的保护，MTA 可能就不能读配置信息了。这会导致“打开文件”错误或其他无法预计的结果。在读取配置文件遇到问题时，`imsimta test -rewrite` 实用程序还会报告其他信息。请参见 **iPlanet Messaging Server Reference Manual** 的 MTA 有关章节中的 `imsimta test -rewrite` 说明文档。

如果 MTA 象是从授权帐户而不是从非授权帐户发挥功能，MTA 表目录中的文件权限很可能是产生问题的原因。检查配置文件及其目录的权限。请参阅第 361 页“检查关键文件的所有权”。

“文件创建”错误通常表明在 MTA 邮件列队里创建邮件文件时出了问题。有关诊断文件创建问题请参见第 360 页 “检查邮件队列目录”。

非法主机 / 域错误

当地址通过浏览器提供给 MTA 时可能会出现这种错误。或者，此错误可能会作为出错退回邮件而被延迟并退回。在这两种情况下，这种出错讯息都表明 MTA 不能把邮件传递给指定的主机。要确定邮件为何不能送到特定的主机，需要遵循下面的故障诊断程序：

- 证实有问题的地址没有拼错、没有被错误转录以及没有使用已经不存在的主机名或域名。
- 通过 `imsimta test -rewrite` 实用程序运行有问题的地址。如果实用程序仍然返回“illegal host/domain （非法的主机 / 域）”错误，说明 MTA 在 `imta.cnf` 文件和其他文件中没有处理这一地址规则。证实 MTA 的配置是正确的，即正确地回答了所有配置问题，而且一直保持配置信息及时更新。
- 如果 `imsimta test -rewrite` 没有在地址上发生错误， MTA 可以确定如何处理地址，但是网络传输将不接受该地址。欲获得其他详细信息可以查阅相关的日志文件。瞬时网络路由或名字服务错误不会导致返回出错讯息，尽管严重错误配置的域名服务器可能引起这些问题。
- 如已连接到 Internet，检查证实已正确配置了 TCP/IP 通道以支持 MX 记录查找。很多域地址不能从 Internet 上直接访问，而是需要邮件系统正确解析 MX 条目。如已连接到 Internet，并且 TCP/IP 被配置为支持 MX 记录，则 MTA 也应配置为启用 MX ；参见 TCP/IP 连接和 DNS 查找支持第 176 页 “TCP/IP 连接和 DNS 查找支持”以获得详细说明。如果 TCP/IP 包没有配置为支持 MX 记录查找，则将无法达到只针对 MX 的域。

SMTP 通道中的错误：os_smtp_* errors

下列错误不一定是 MTA 错误：如 os_smtp_open，os_smtp_read 以及 os_smtp_write 这样的 os_smtp_* 错误。这些错误是在 MTA 报告在网络层遇到问题时生成的。例如，os_smtp_open 错误意味着网络对远程端的连接无法打开。由于地址错误或通道配置错误，MTA 可能被配置成与一个无效系统连接。os_smtp_* 错误通常是由于 DNS 或网络连接问题引起的，尤其是这是先前使用的通道或地址时。os_smtp_read 或 os_smtp_write 错误通常表明连接被另一端中止或网络引起了问题。

网络和 DNS 问题的本质常常是瞬时性的。偶然出现的 os_smtp_* 错误一般不用太担心。但是如果这些错误常常出现，这可能说明存在一潜在的网络问题。

要获取有关特定 os_smtp_* 错误的详细说明，可以启用有问题通道上的调试功能。查看调试通道的日志文件，可以显示有关 SMTP 对话的详细内容。尤其要查看 SMTP 对话过程中网络问题出现的时间。这个时间可能暗示网络问题或远程端问题。在某些情况下，可能还需要进行网络层调试 （例如 TCP/IP 信息包跟踪），以确定发送和接收了什么。

第 15 篇

监控 iPlanet Messaging Server

在大多数情况下，规划且配置良好的服务器可以在不需要管理员过多干预下执行。然而，作为管理员仍有责任监控服务器以便发现问题征兆。本章描述 iPlanet Messaging Server 的监控，包括如下几部分：

- 日常监控任务
- 监控系统性能
- 监控 MTA
- 监控邮件访问
- 监控 LDAP Directory Server
- 监控邮件存储库
- 监控使用的实用程序和工具

故障诊断程序，请见第 14 篇，“MTA 故障诊断”。

日常监控任务

日常执行的基础操作中最重要的包括检查 Postmaster 邮件、监控日志文件以及设置 `stored` 实用程序。这些任务在下文中描述。

检查 Postmaster 邮件

Messaging Server 有一个为 Postmaster 电子邮件设置的预定义的管理性邮件发送列表。任何此邮件发送列表中的用户将自动收到发送给 Postmaster 的邮件。

Postmaster 邮件的规则在 RFC822 中定义，它要求每个邮件站点接受寄给名为 postmaster 的用户或邮件发送列表的每个邮件，并且发送到此地址的邮件被传递给一个真实的人。所有发送到 postmaster@host.domain 的邮件被发送到 Postmaster 帐户或邮件发送列表。

Postmaster 地址通常是用户发送关于其邮件服务的电子邮件的地址。作为 Postmaster，可能会收到来自本地用户的关于服务器响应时间的邮件，或来自其他服务器管理员的关于遇到无法发送邮件至你的服务器的问题等等。 Postmaster 应当每日检查 Postmaster 邮件。

也可以配置服务器发送一些出错信息邮件到 Postmaster 地址。例如，当 MTA 不能够路由或传递一封邮件时，可以通过发送到 Postmaster 地址的邮件而得到通知。也可以给 Postmaster 发送例外情况警告 （磁盘空间不足，服务器响应迟缓等）。

监控及维护日志文件

iPlanet Messaging Server 为每一种它所支持的主要协议或服务分别创建一组日志文件，即 SMTP、IMAP、POP 和 HTTP。应当例行监控日志文件，特别是当服务器出现问题的时候。

请注意日志记录能够影响服务器性能。日志记录越详细，在一给定时间段内日志文件会占用的磁盘空间就越多。应当为服务器定义有效且实际的日志轮换、期满检测及备份策略。关于为服务器定义日志记录策略的信息请参阅第 13 篇，“日志记录和日志分析”。

设置 stored 实用程序

`stored` 实用程序为服务器执行自动监控及维护任务，例如：

- 后台及日常邮件传输任务。
- 死锁检测和死锁的数据库事务的回卷。
- 启动时清理临时文件。
- 执行时限策略。
- 周期性监控服务器状态、磁盘空间、服务器响应时间等。
- 必要时发布报警。

`stored` 实用程序可自动于每天半夜执行清理和期满检测操作。有关详细信息，请参阅第 394 页 “stored”。

监控系统性能

本章关注于 iPlanet Messaging Server 的监控，然而，也需要监控服务器所驻留的系统。一个配置良好的服务器无法在缺乏性能调整的系统上很好地运行，一些服务器失败的表象可能表明硬件功能不足以服务于电子邮件负荷。本章不提供关于系统性能监控的所有细节，因为许多程序是针对特定平台的，可能需要参阅针对特定平台的系统文档。下面的程序描述性能监控：

- 监控端到端的邮件传递时间
- 监控磁盘空间
- 监控 CPU 的使用情况

监控端到端的邮件传递时间

电子邮件需要及时传递。这或许是服务协议所要求的，但尽可能快速地传递邮件也是一种好策略。缓慢的端到端时间可能说明许多问题。可能是服务器工作不正常，或者一天中的某段时间经历了过量的邮件负荷，或者现有的硬件资源在超负荷运转。

漫长的端到端传递时间的表象

邮件的传递花费比通常更多的时间。

监控端到端邮件传递时间

使用任何可以发送和接收邮件的工具。比较服务器转发间的报头时间以及原点和检索点间的时间。

监控磁盘空间

磁盘空间不足是导致邮件服务器出现问题及失败的最常见原因之一。如果没有空间写入 MTA 队列或邮件存储库，邮件服务器将运行失败。此外，除非日志文件被监控和清理，否则它们将不受控制地增长直至充满整个磁盘空间。

当 `stored` 的清理功能失效时磁盘空间很快耗尽，被删除的邮件不会从邮件存储库中清除。其它耗尽磁盘空间的原因还有 MTA 邮件队列增长过大，邮件存储库超过可用磁盘空间，以及未受监控的日志文件不受控制地增长等。（请注意象 LDAP、MTA 以及 Message Access 这样的日志文件有许多，并且这些日志文件中的每一个都可存储在不同的磁盘中。）

磁盘空间问题表象

不同的耗尽空间的磁盘或分区，可能产生不同的表象。MTA 队列会溢出并拒绝 SMTP 连接，邮件会保留在 ims_master 队列而不被传递到邮件存储库，并且日志文件会溢出。

监控磁盘空间

可能需要依据系统配置监控各个磁盘和分区。例如， MTA 队列可能驻留在一个磁盘 / 分区，邮件存储库可能驻留在另一个，而日志文件可能驻留在另外的第三个。这些空间中的每一个都需要监控，并且这些空间的监控方法可能有所不同。

监控邮件存储库

建议邮件存储库的磁盘使用率不超过 75%。通过使用 `configutil` 实用程序配置下面的报警属性能够监控邮件存储库的磁盘使用：

- `alarm.diskavail.msgalarmstatinterval`
- `alarm.diskavail.msgalarmthreshold`
- `alarm.diskavail.msgalarmwarninginterval`

通过设置这些参数，能够指定系统监控磁盘空间的频度以及在系统应当在何种情况下发出警告。例如，若要系统每 600 秒监控一次磁盘空间，则指定用下面的命令：

```
configutil -o alarm.diskavail.msgalarmstatinterval -v 600
```

如果每当可用磁盘空间低于 20% 时都希望收到警告信息，则指定使用下面的命令：

```
configutil -o alarm.diskavail.msgalarmthreshold -v 20
```

请参照第 395 页表 15-1 以获得关于这些参数的更多信息。

监控 MTA 队列和日志记录空间

需要监控 MTA 队列磁盘和日志记录空间磁盘的使用。

监控 CPU 的使用情况

CPU 的高负荷使用是一个信号，表明 CPU 没有足够的应对如此高的负荷的能力，或者表明某个进程正在耗费过多的 CPU 周期。

CPU 使用问题的表象

漫长的系统响应时间。缓慢的用户登录。缓慢的传递率。

监控 CPU 使用

监控 CPU 使用是平台相关的任务。请参阅相关平台文件。

监控 MTA

本部分包括如下内容：

- 监控邮件队列的大小
- 监控传递失败率
- 监控入站 SMTP 连接
- 监控 Dispatcher 和作业控制器进程

监控邮件队列的大小

邮件队列的过度增长可能表明邮件没有被传递，在传递中被耽搁，或者到达过快以至系统不能传递。这可能由许多原因造成的，例如由于系统邮件泛滥造成的服务拒绝器型攻击，或是作业控制器不运行。

请参阅第 86 页“通道的邮件队列”，第 371 页“邮件未入队”和第 373 页“MTA 邮件未传递”以获得更多关于邮件队列的信息。

邮件队列问题的表象

- 磁盘空间使用增长。
- 用户没有在合理时间内收到邮件。
- 邮件队列异常的大。

监控邮件队列的大小

或许监控邮件队列的最好方法是使用 `imsimta qm`。请参阅第 401 页“imsimta qm 计数器”。

也能够监控队列目录（`/`*ServeRoot*`/msg-`*instance*`/imta/queue/`）中的文件数目。文件的数目是针对特定站点的，需要建立一基线历史记录以便发现多少才是“太多”。这可以通过在两周的周期内记录队列文件的大小以获得一大约均值来完成。

监控传递失败率

传递失败是指向外部站点传递邮件的一次失败尝试。传递失败率的大规模增长可能是一个信号，表明存在象无反应的 DNS 服务器或远程服务器对连接的响应超时等这样的网络问题。

传递失败频度表象

没有外在的表象。大量的 `Q` 记录将出现在 `mail.log_current`。

监控传递失败率

传递失败被记录在 MTA 日志，日志条目代码为 `Q`。
在文件 `msg-`*instance*`/log/imta/mail.log_current` 中可查看 Q 记录。

监控入站 SMTP 连接

来自一给定 IP 地址的入站 SMTP 连接数目的不寻常增长可能表明：

- 一外部用户尝试转发邮件。
- 一外部用户尝试服务拒绝型攻击。

未授权的 SMTP 连接的表象

- **外部用户转发邮件：**非外在表象。
- **服务拒绝型攻击：**通过邮件请求造成 SMTP 服务器超载的外部尝试。

监控入站 SMTP 连接

- **外部用户转发邮件：**查看 msg-*instance*/log/imta/mail.log_current 中日志条目代码为 J（被拒绝的转发）的记录。要开始远程 IP 地址的日志记录请将以下行加入到文件 option.dat：

  ```
  log_connection=1
  ```

  请注意此功能的启用时会付有轻微的性能代价。

- **服务拒绝型攻击：**要查明有多少用户和哪些用户正在连接 SMTP 服务器，可以运行命令 netstat 并且检查在 SMTP 端口 （默认：25）的连接。例如：

  ```
  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
  ```

  请注意首先需要为系统决定适当的 SMTP 连接数目及其状态 （ESTABLISHED，CLOSE_WAIT 等），以决定一特定读操作是否异常。

  如果发现许多连接保持 SYN_RECEIVED 状态，这可能是由于网络故障或是服务拒绝型攻击所导致的。另外， SMTP 服务器进程的生命周期是有限的。这受控于文件 dispatcher.cnf 中的 MTA 配置变量 MAX_LIFE_TIME。其默认值是 86,400 秒（一 天）。类似地，MAX_LIFE_CONNS 指定一服务器进程在其生命周期中能处理连接的最大数目。如果发现某个特定的 SMTP 服务器长时间闲置，就应当进行检查。

监控 Dispatcher 和作业控制器进程

MTA 如要工作， Dispatcher 和作业控制器进程必须运转。且每一种应当有一个进程。

Dispatcher 和作业控制器故障的表象

如果 Dispatcher 发生故障或者资源不足， SMTP 连接既被拒绝。

如果作业控制器发生故障，队列大小将会增长。

监控 Dispatcher 和作业控制器进程

请检查名为 dispatcher 和 job_controller 的进程是否存在。请参阅第 362 页“检查确认作业控制器和 dispatcher 的运行状态”。

监控邮件访问

本部分包括如下内容：

- 监控 imapd、 popd 和 httpd
- 监控 stored

监控 imapd、 popd 和 httpd

这些进程提供对 IMAP、POP 和 Web 邮件业务服务的访问。如果其中之一没有运行或没有响应，服务将不能正常发挥其功能。如果服务正在运行但超载，监控将使得检测到这一情况并将其配置更合适一些。

imapd、 popd 和 httpd 问题的表象

连接被拒绝或系统过慢以至于无法连接。例如，在 IMAP 未运行的情况下直接连接 IMAP，会看到类似这样信息：

```
telnet 0 143
Trying 0.0.0.0...
telnet: Unable to connect to remote host: Connection refused
```

如果尝试与客户程序连接，会得到如下这样的消息：

`netscape` 不能连接到指定位置的服务器。服务器故障或忙。

监控 imapd、 popd 和 httpd

- 能用 SNMP 监控。

  如果已设置了 SNMP，这是监控这些进程的非常好的方法。请参阅附录 A，“SNMP 支持”。服务器信息在 Network Services Monitoring MIB 上。

- 检查日志文件。

  查看目录 *msg-instance*/log/*service* 其中 *service* 可以是 http 或 IMAP 或 POP。在那个目录可以找到许多日志文件。其中一个文件名是 *服务*（imap、pop、http）的名称，其它文件名是服务名后跟一序列号和一日期。例如：

  ```
  imap  imap.29.1010221593 imap.31.1010394412  imap.33.1010567224
  ```

  仅包含服务名的文件是最新的日志文件。其它文件按顺序号 （此处为 29, 31, 33）排序，且最高序列号的文件是次新的文件。（参阅第 13 篇，“日志记录和日志分析”。）

  如果服务器关闭会看到象下面这样的信息：

  可用 `counterutil` 检查 `[05/Jan/2002:08:36:38 -0800] gotmail-a imapd[10275]: General Warning: iPlanet Messaging Server IMAP4 5.2 (built Dec 9 2001) shutting down`

- 请参阅第 396 页 “counterutil”和 **iPlanet Messaging Server Reference Manual**。
- 运行针对特定平台的命令，以证实 imapd、 popd 和 httpd 等进程正在运行。例如，在 Solaris 上可以使用命令 `ps` 寻找 `imapd`, `popd` 和 `mshttpd`。在 Windows NT 上，既可以使用任务管理器窗口也可以使用命令行。
- 可以通过设置服务器响应配置参数 （在第 395 页 “建议使用的 stored 参数”中有描述）为指定的服务器性能阈值设置报警。

监控 `stored`

`stored` 执行多种重要任务，例如邮件数据库的死锁和事务操作，执行时限政策以及清除存储在磁盘上的邮件。如果 `stored` 停止运行， messaging server 将最终产生问题。如果当 `start-msg` 运行时 `stored` 未启动，其它进程也不会启动。有关 `stored` 命令的详细说明，请参阅 **iPlanet Messaging Server Reference Manual**。

`stored` 问题的表象

没有外在表象。

监控 stored

- 请检查确认 `stored` 进程是正在运行。`stored` 在 `msg-`*`instance`*`/config` 中创建并更新一名为 `pidfile.store` 的 `pid` 文件。此 `pid` 文件在恢复时显示一 `init` 状态，当就绪时显示一 `ready` 状态。例如：

  ```
  231: cat pidfile.store
  28250
  ready
  ```

  第一行中的数字是 `stored` 的进程 ID。

  ```
  232: ps -eaf | grep stored
  mailsrv 28250     1   0   Jan 05 ?        8:44
  /usr/iplanet/server5/bin/msg/admin/bin/stored -d
  ```

- 请检查在 `msg-`*`instance`*`/store/mailboxlist` 中建立的日志文件。请注意并不是每个日志文件的建立都是由直接的 `stored` 问题造成的。在 `imapd` 死掉或有数据库问题时也可能建立日志文件。
- 请检查 `msg-`*`instance`*`/config` 中下列文件上的时间截：

  `stored.ckp` - 当尝试检查点操作时被触及 （touched）。应当每隔 1 分钟打一次时间戳。
  `stored.lcu` - 在每个 db 日志清理时被触及（touched）。应当每隔 5 分钟打一次时间戳。
  `stored.per` - 每当诞生一个逐用户 db 写出时被触及 （touched）。应每隔 60 分钟打一次时间戳。

- 请检查在默认日志记录文件中储存的邮件，即 `msg-`*`instance`*`/log/default/default`

监控 LDAP Directory Server

本部分包括如下内容：

- 监控 slapd

监控 slapd

LDAP 目录服务器（slapd）为邮件系统提供目录信息。如果 slapd 出现故障，系统将不能正常工作。如果 slapd 响应过于迟缓，将影响到登录速度以及任何其它请求 LDAP 查找的事务。

slapd 问题的表象

- 客户机 POP、 IMAP 或 Web 邮件业务认证失败或者比预期的慢。
- MTA 工作不正常

监控 slapd

- 请检查确认 ns-slapd 进程正在运行。
- 请检查在 slapd-*instance*/logs/ 中的 slapd 日志文件访问和错误。
- 检查搜索一用户时的 ns-slapd 响应时间。
- 查看 Admin Console 以监控 slapd。

监控邮件存储库

邮件被存储在一个数据库中。磁盘上的用户分布、其邮箱的大小以及磁盘空间要求都影响着存储性能。本部分包括如下内容：

- 监控邮件存储数据库锁定状态
- 监控在 mboxutil 目录中的数据库日志文件的数目

监控邮件存储数据库锁定状态

数据库锁定状态被不同的服务器进程保持着。这些数据库锁定能够影响邮件存储库的性能。在死锁的情况下，邮件不会在合理的速度下被插入到邮件存储库，并且 ims-ms 通道队列也会因此而增长得更大。有合理的理由为对队列备份，因此拥有队列长度的历史记录对于问题的诊断是十分有用的。

邮件存储数据库锁定问题的表象

积累且得不到解决的事务的数目。

监控邮件存储数据库锁定

使用命令 counterutil -o db_lock

监控在 mboxutil 目录中的数据库日志文件的数目

数据库日志文件参照困猫 （sleepycat）事物检查点日志文件（msg-*instance*/store/mboxlist） 。日志文件的建立是未发生数据库检查点操作的表象。日志文件的建立也有可能源于 stored 问题。

数据库日志文件问题的表象

应当有 2 个 或 3 个日志文件。如果有更多的日志文件，则是潜在的严重问题的信号。邮件存储库为邮件和空间配额使用几个数据库，它们出现问题会导致所有邮件服务器出现问题。

监控数据库日志文件

查看 msg-*instance*/store/mboxlist 目录并确认只有 2 个 或 3 个文件。

监控使用的实用程序和工具

以下工具可用于监控：

- stored
- counterutil
- 日志文件
- imsimta 计数器
- imsimta qm 计数器
- 使用 SNMP 进行 MTA 监控
- 用于邮箱配额检查的 mboxutil

stored

stored 实用程序在服务器上执行维护任务，但它也能用于监控。它能够周期性检查服务器状态、磁盘空间及服务响应时间，并且如果指定，它还能以邮件的形式发布报警给 Postmaster （请参阅 第 392 页）。

来自 stored 的报警以电子邮件的形式发送给 Postmaster 以警告某种指定情况。以下是一个当某个阈值被超越时 stored 发送的电子邮件报警的例子：

主题： **报警：“ldap_siroe.com_389”服务器响应时间为 10 秒**
日期： **Tue, 17 Jul 2001 16:37:08 - 0700 (PDT)**
发件人： **postmaster@siroe.com**
收件人： **postmaster@siroe.com**

服务器实例：/usr/iplanet/server5/msg-europa
报警 ID:serverresponse
实例：ldap_siroe_europa.com_389
说明服务器响应时间以秒计算
当前测量值 (17/Jul/2001:16:37:08 - 0700) ：10
最低记录值：0
最高记录值：10
监控间隔：600 秒
报警条件为当超过阈值 10
超过阈值的次数：1

可以指定 `stored` 监控磁盘和服务器性能的频度以及在何种情况下发送报警。这通过使用 `configutil` 命令设置报警参数来完成。表 15-1 列出了有用的 `stored` 参数及其默认设置。

表 15-1　建议使用的 `stored` 参数

参数	说明 （默认）
alarm.msgalarmnoticehost	报警邮件送往的 (localhost) 计算机。
alarm.msgalarmnoticeport	(25) 发送报警邮件时连接的 SMTP 端口。
alarm.msgalarmnoticercpt	(Postmaster@localhost) 报警通知的接收人。
alarm.msgalarmnoticesender	(Postmaster@localhost) 报警发件人的地址。
alarm.diskavail.msgalarmdescription	可用磁盘空间报警的说明。
alarm.diskavail.msgalarmstatinterval	(3600) 两次可用磁盘空间检查之间的间隔秒数。 将其设为 0 以禁止对磁盘使用的检查。
alarm.diskavail.msgalarmthreshold	(10) 低于其值将会发送报警的磁盘空间可用率。
alarm.diskavail.msgalarmthresholddirection	(-1) 指定当磁盘可用空间低于阈值 (-1) 或高于阈值 (1) 时是否发出报警。
alarm.diskavail.msgalarmwarninginterval	(24) 与下次重复的可用磁盘空间报警之间的间隔小时数。
alarm.serverresponse.msgalarmdescription	服务器响应报警的说明。
alarm.serverresponse.msgalarmstatinterval	(600) 两次服务器响应检查之间的间隔秒数。 将其设为 0 以禁止对服务器响应的检查。
alarm.serverresponse.msgalarmthreshold	(10) 如果服务器响应的描述超过此值，即刻发出报警。
alarm.serverresponse.msgalarmthresholddirection	(1) 指定当服务器响应时间高于阈值 (1) 或低于阈值 (-1) 时是否发出报警。
alarm.serverresponse.msgalarmwarninginterval	(24) 与下次重复的服务器响应报警之间的间隔小时数。

counterutil

此实用程序从不同的系统计数器获取统计信息。下面是一个可用计数器对象的当前列表：

```
counterutil -l
entry = alarm
entry = diskusage
entry = serverresponse
entry = db_lock
entry = db_log
entry = db_mpool
entry = db_txn
entry = popstat
entry = imapstat
entry = httpstat
entry = cgimsg
```

每一条目代表一计数器对象并提供针对此对象的多种有用的计数。在本部分中将仅讨论 `alarm`、`diskusage`、`serverresponse`、`db_lock`、`popstat`、`imapstat` 和 `httpstat` 这些计数器对象。counterutil 命令的使用细节请参阅 **iPlanet Messaging Server Reference Manual**。

`counterutil` 输出

`counterutil` 有多种标志。此实用程序可以具有如下的命令格式：

```
counterutil -o CounterObject -i 5 -n 10
```

其中，

`-o` *CounterObject* 表示 `alarm`、`diskusage`、`serverresponse`、`db_lock`、`popstat`、`imapstat` 和 `httpstat` 等计数器对象。

`-i 5` 指定一个 5 秒的间隔。

`-n 10` 表示重复次数（默认：无穷大）。

以下是一个 counterutil 用法的例子：

```
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
  ...
```

用 counterutil 进行报警统计

这些报警统计参照 stored 发出的报警。报警计数器提供如下的统计数据：

表 15-2　counterutil 报警统计

后缀	说明
alarm.countoverthreshold	超过阈值的次数。
alarm.countwarningsent	已发送警告的数量。
alarm.current	当前监视值。
alarm.high	所记录过的最高值。
alarm.low	所记录过的最低值。
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	上次进行重置的时间。
alarm.timestatechanged	上次更改报警状态的时间。
alarm.warningstate	警告状态 （是 (1) 或 否 (0)）。

使用 counterutil 进行 IMAP、 POP、和 HTTP 连接统计

要得到关于当前 IMAP、 POP 和 HTTP 连接数目，失败登录数目以及从开始起的连接总数等等信息，可以使用命令 `counterutil -o` *CounterObject* `-i 5 -n 10`。其中 *CounterObject* 表示计数器对象 `popstat`、`imapstat` 或 `httpstat`。`imapstat` 后缀的意思如表 15-3 中所示。对象 `popstat` 和 `httpstat` 以相同的格式和结构提供相同信息。

表 15-3　counterutil imapstat 统计

后缀	说明
currentStartTime	当前 IMAP 服务器进程的启动时间。
lastConnectionTime	上次接受新客户机的时间。
maxConnections	IMAP 服务器能处理的并发连接的最大数目。
numConnections	由当前 IMAP 服务器提供服务的连接的总数。
numCurrentConnections	当前活动的连接数。
numFailedConnections	由当前 IMAP 服务器提供服务的失败连接的次数。
numFailedLogins	由当前 IMAP 服务器提供服务的失败登录的次数。
numGoodLogins	由当前 IMAP 服务器提供服务的成功登录的次数。

使用 counterutil 进行磁盘使用的统计

命令：`counterutil -o diskusage` 产生如下信息：

表 15-4　counterutil diskstat 统计

后缀	说明
diskusage.availSpace	磁盘分区可用空间总量。
diskusage.lastStatTime	上次统计时间。
diskusage.mailPartitionPath	邮件分区路径。
diskusage.percentAvail	磁盘分区空间的可用百分比。
diskusage.totalSpace	磁盘分区空间总量。

服务器响应统计数据

命令：`counterutil -o serverresponse` 产生如下信息。此信息对于检查服务器是否正在运行以及其响应的迅速程度是有用的。

表 15-5 `counterutil serverresponse` 统计

后缀	说明
`http.laststattime`	上次检查 http 服务器响应的时间。
`http.responsetime`	http 响应时间。
`imap.laststattime`	上次检查 imap 服务器响应的时间。
`imap.responsetime`	imap 响应时间。
`pop.laststattime`	上次检查 pop 服务器响应的时间。
`pop.responsetime`	pop 响应时间。
`ldap_host1_389.laststattime`	上次检查 ldap_host1_389 服务器响应的时间。
`ldap_host1_389.responsetime`	ldap_host1_389 响应时间。
`ugldap_host2_389.laststattime`	上次检查 ugldap_host2_389 服务器响应的时间。
`ugldap_host2_389.responsetime`	对 ugldap_host2_389 的响应时间。

日志文件

对 SMTP、 IMAP、 POP 和 HTTP 记录的 Messaging server 日志事件。用户可自定义建立和管理 Messaging Server 日志文件的策略。

由于日志记录会影响服务器性能，在服务器承担此任务前应当仔细斟酌。有关详情，请参阅第 13 篇，“日志记录和日志分析”。

imsimta 计数器

MTA 依据 Mail Monitoring MIB、RFC 1566 对每个活动通道的邮件流通量进行累计。通道计数器意在帮助指出电子邮件系统的运行态势和状况。通道计数器并不是为准确计算邮件流通量而设计的。有关精确计数，可另行参阅第 13 篇，“日志记录和日志分析”中对 MTA 日志的讨论。

MTA 通道计数器使用最精简的机制实现，以使它在实际操作中产生尽可能小的影响。通道计数器不会过度地尝试：如果映射存储块的尝试失败，则不会记录任何信息；如果几乎无法立即得到存储块中的一个锁，则不会记录任何信息；当系统关闭时，驻留内存的存储块将永久丢失。

imsimta counters -show 命令提供 MTA 通道邮件统计数据 （见下）。这些计数器需要随时检查以发现最小值。对于某些通道，这个最小值竟可能是负数。一个负数最小值意味着在通道计数器被置零时 （例如，计数器的群集数据库被创建），有邮件排队进入该通道。当这些邮件出队时，通道的相关计数器进行减值从而导致一个负数最小值。对于此种计数器，正确的“绝对”值是当前值减去计数器初始化以来的最小值。

```
Channel           Messages    Recipients    Blocks
-------           --------    ----------    -------
tcp_local
   Received        29379        79714       982252                        (1)
   Stored             61          113        -2004                        (2)
   Delivered       29369        79723       983903 (29369 first time)     (3)
   Submitted       13698        13699        18261                        (4)
   Attempted           0            0            0                        (5)
   Rejected            1           10            0                        (6)
   Failed            104          104         4681                        (7)

   Queue time/count         16425/29440 = 0.56                             (8)
   Queue first time/count   16425/29440 = 0.56                             (9)

   Total In Assocs            297637
   Total Out Assocs            28306
```

1) Received（已接收）是入队至名为 tcp_local 的通道的邮件数目。也就是说，通过任何其它通道入队至通道 tcp_local 的邮件 （在文件 mail.log* 中的 E 记录）。

2) Stored 是存储在通道中排队等候传递的邮件数目。

3) Delivered （已传递）是已经被通道 tcp_local 处理 （出队）的邮件数目。（即文件 mail.log* 中的 D 记录。）一次出队操作或者对应一次成功的传递 （即出队到其它通道），或者对应由于邮件被退回到发件人而导致的出队。其通常对应于 Received （已接收）数减去 Stored （已存储）数。

MTA 也知道有多少邮件在首次尝试时即出队，这个数目表示在圆括弧中。

4) Submitted （已提交）是通过通道 tcp_local 入队至任何其它通道的邮件数目 （文件 mail.log 中的 E 记录）。

5) Attempted（已尝试）是在排队等候时曾经历过临时问题的邮件数目，即文件 mail.log* 中的 Q 或 Z 记录。

6) Rejected （已拒绝）是已被拒绝的入队尝试数，即在文件 mail.log* 中的 J 记录。

7) Failed （已失败）是失败的出队尝试数，即文件 mail.log* 中的 R 记录。

8) Queue time/count（入队时间 / 记数）是已传递邮件滞留队列的平均时间。这既包括首次尝试即被传递的邮件，参见 (9)，也包括请求过多次传递尝试的邮件（因而通常花费相当的时间在队列中等待）。

9) `Queue first time/count`（首次入队时间 / 记数）是首次尝试即被传递的邮件滞留队列的平均时间。

请注意提交的邮件数可以比传递的邮件数大。这种情况经常发生，因为通道出队（传递）的每封邮件将导致至少一封但可能多于一封新邮件入队（被提交）。例如，如果一封邮件有两个通达不同通道的接收人，那么将需要两次入队。或者如果已邮件退回，它的一个副本会退回到发件人处，另一副本会发送给 Postmaster。通常这将是两次提交（除非两者通达同一通道）。

更一般地说，`Submitted`（已提交）和 `Delivered`（已传递）之间的连接依通道的种类而异。例如，在转换通道中，一邮件会被某个任意的其他通道入队，然后转换通道会处理该邮件并将其入队到第三个通道，并在其自己的队列中将该邮件标志为已出队。每个单独的邮件占用一个路径：

```
elsewhere -> conversion    E record    Received
conversion -> elsewhere    E record    Submitted
conversion                    D record    Delivered
```

然而，对于像 `tcp_local` 这样不是“贯穿”的而是有两个单独部分（从和主）的通道，在 `Submitted`（已提交）和 `Delivered`（已传递）之间没有连接。`Submitted`（已提交）计数器与 `tcp_local` 通道的 SMTP 服务器部分有关，而 `Delivered`（已传递）计数器与 `tcp_local` 通道的 SMTP 客户程序部分有关。它们是两种完全不同的程序，通过它们的邮件穿越也可能完全不同。

提交到 SMTP 服务器的邮件：

```
tcp_local -> elsewhere   E record     Submitted
```

通过 SMTP 客户程序发送到其它 SMTP 主机的邮件：

```
elsewhere -> tcp_local   E record     Received
tcp_local                  D record     Delivered
```

通道出队（传递）将导致至少一封但可能多于一封新邮件入队（提交）。例如，如果一封邮件有两个通达不同通道的接收人，那么将需要两次入队。或者如果邮件退回，它的一个副本会退到发件人处，另一副本会发送给 Postmaster。通常通过同一通道到达。

在 UNIX 和 NT 上实现

由于性能原因，一个运行 MTA 的结点在内存中保留一个通道计数器缓存，这个缓存使用共享存储块（UNIX）或共享文件映像对象（NT）。在这个结点上的进程入队和出队邮件时，会修改这个驻留内存的计数器。如果当通道运行时驻留存储块不存在，地将会自动被创建。（`imta start` 命令也创建驻留存储块，如果它不存在的话。）

命令 `imta counters -clear` 或 `imta qm` 命令 `counters clear` 可用于将计数器重置为 0。

imsimta qm 计数器

`imsimta qm counters` 实用程序显示 MTA 通道队列邮件计数器。必须在根目录或 `mailsrv` 处运行这个实用程序。输出字段与第 399 页“imsimta 计数器”中描述的内容一样。有关使用细节，还可参阅 **iPlanet Messaging Server Reference Manual**。

例 1：

```
imsimta qm counters show
```

```
Channel                  Messages    Recipients     Blocks
----------------------  ----------  ----------    ----------
autoreply
   Received               13077        13859         264616
   Stored                    92           91           -362
   Delivered              12985        13768         264978
   Submitted               2594         2594           3641
...
```

例 2：

```
imsimta qm counters today
```

```
今天已处理 4370 封邮件
许可证对每日的邮件数没有限制。
```

使用 SNMP 进行 MTA 监控

iPlanet Messaging Server 通过简单网络管理协议 (SNMP) 支持系统监控。使用 SNMP 客户机（有时称为 *网络管理器*），如 Sun Net Manager 或 HP OpenView（不随本产品提供），可监控 iPlanet Messaging Server 的特定部分。有关细节请参阅附录 A，“SNMP 支持”。

用于邮箱配额检查的 mboxutil

您可通过 `mboxutil` 实用程序监控空间配额的使用和限制情况。 `mboxutil` 实用程序可生成一份报告，列示任何已定义的空间配额和限制情况，并提供空间配额使用量方面的信息。报告中的空间配额及其使用量以千字节为单位。

例如，下面的命令列示所有用户的空间配额信息：

```
% mboxutil -a
------------------------------------------------------------------------
Domain red.siroe.com (diskquota = not set msgquota = not set) quota usage
------------------------------------------------------------------------
diskquota        size(K)    %use    msgquota      msgs    %use    user
# of domains = 1
# of users = 705

no quota         50418              no quota      4392            ajonkish
no quota         5                  no quota      2               andrewt
no quota         355518             no quota      2500            aniksri
...
```

下面的例子显示了用户 sorook 的配额使用情况：

```
% mboxutil -u sorook
--------------------------------------------------------------------------
quota usage for user sorook
--------------------------------------------------------------------------
diskquota       size(K)     %use    msgquota       msgs      %use    user

no quota        1487                 no quota       305               sorook
```

附录 A

SNMP 支持

iPlanet Messaging Server 通过简单网络管理协议（SNMP）支持系统监控。使用 SNMP 客户机 （有时称作*网络管理器*），比如 Sun Net Manager 或 HP OpenView （不随此产品提供），可以监控 iPlanet Messaging Server 的特定部分。有关监控 iPlanet Messaging Server 方面的详细说明，请参见第 15 篇，“监控 iPlanet Messaging Server”。

本章介绍如何启用 Messaging Server 的 SNMP 支持功能。同时还概要介绍 SNMP 所提供的信息种类。注意，本章不描述如何从 SNMP 客户机处查看这些信息。有关如何用 SNMP 查看基于 SNMP 的详细信息，请参阅 SNMP 客户机文档。本文档还介绍来自 Messaging Server SNMP 实现的某些可用数据，但对于 MIB 的完整细节还请参阅：RFC 2788 和 RFC 2789。

本章包括以下几部分：

- SNMP 实现
- 为 iPlanet Messaging Server 配置 Solaris 8 的 SNMP 支持
- 为 Windows 平台配置 SNMP 支持
- 来自 SNMP 客户机的监控
- 在 Unix 平台上与其它 iPlanet 产品共存
- SNMP 信息来自 Messaging Server

SNMP 实现

iPlanet Messaging Server 实现两个标准化的 MIB，网络服务监控程序 MIB（RFC 2788）和邮件监控程序 MIB （RFC 2789）。网络服务监控程序 MIB 是提供来监控如 POP、 IMAP、HTTP 和 SMTP 等服务器这样的网络服务的。邮件监控程序 MIB 是提供来监控 MTA 的。邮件监控 MIB 用于监控每个 MTA 通道的状态，包括活动的和历史的状态。活动信息关注当前已入队邮件和打开网络连接 （如已入队邮件计数，打开网络连接的源 IP 地址等），而历史信息则提供汇总数据 （如已处理邮件总数和入站连接总数等）。

备注	有关 Messaging Server 的 SNMP 监控信息的完整列表，请参阅 RFC 2788 和 RFC 2789。

只有 Solaris 8 平台 支持 SNMP。今后的版本会得到其它平台的支持。Solaris 上的 SNMP 支持利用了固有的 Solaris SNMP 技术 Solstice Enterprise Agents （SEA）。客户不须在 Solaris 8 系统上安装 SEA：必要的运行库已经存在。

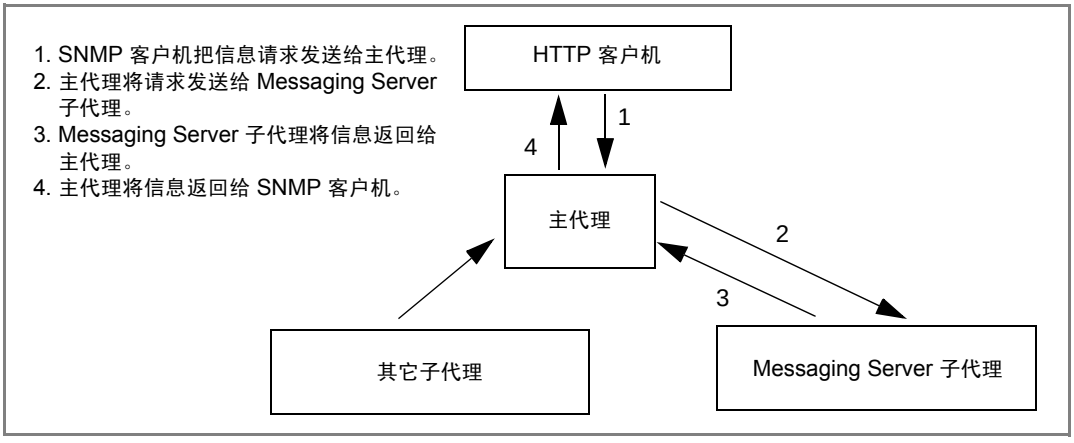
对 Messaging Server SNMP 支持的限制如下：

- 每台主机计算机上只有一个 Messaging Server 实例可以通过 SNMP 进行监控。
- SNMP 支持只用于监控。不支持任何 SNMP 管理。
- 没有实现 SNMP 陷阱。（RFC 2788 提供了相似的功能，但不使用陷阱）。

Messaging Server 中的 SNMP 操作

在 Solaris 平台上，Messaging Server SNMP 进程是一个 SNMP 子代理，一开始就将其自身注册到平台固有的 SNMP 主代理处。来自客户机的 SNMP 请求被传达给主代理。主代理会把任何针对 Messaging Server 的请求转发给 Messaging Server 子代理进程。Messaging Server 子代理进程则处理这些请求，并通过把主代理把响应返回给客户机。具体过程，请参阅：图 A-1。

图 A-1 SNMP 信息流



为 iPlanet Messaging Server 配置 Solaris 8 的 SNMP 支持

虽然 SNMP 监控程序的开销非常小，但提供的 Messaging Server 一开始仍然禁用 SNMP 支持。要启用 SNMP 支持，执行下列命令：

```
# su user-id-for-ims
# configutil -o local.snmp.enable -v 1
# start-msg snmp
```

一旦启用了 SNMP，则 `start-msg` 命令，不须指定任何参数，即可使 SNMP 子代理进程和与其它 Messaging Server 进程一起自动启动。

注意，Solaris 自带的 SNMP 主代理必须运行，Messaging Server SNMP 子代理才能操作。Solaris 自带的 SNMP 主代理是 `snmpdx` 守护程序，此程序通常作为 Sloaris 的启动进程的一部分运行。

SNMP 子代理会自动选择一个需监听的 UDP 端口。如需要，可以向子代理指定固定的 UDP 端口，命令是：

```
# configutil -o local.snmp.port -v port-number
```

以后可以通过给端口号值指定为零来撤消这一设置。零值，即默认设置，告诉 Messaging Server 允许子代理自动选择任意可用的 UDP 端口。

有两个 SNMP 子代理设置文件放置在 `/etc/snmp/conf` 目录中：`ims.acl`，含有 SNMP 访问控制信息，和 `ims.reg`，含有 SNMP MIB OID 注册信息。

通常没有任何理由编辑这两个文件中的任何一个。受 Messaging Server 支持的 MIB 是只读的，而且不需要在 `ims.reg` 文件指定端口号。如果指定了端口号，MIB 就会满足，除非也用 `configutil` 实用程序设置了端口号。在那种情况下，用 `configutil` 设置的端口号是子代理将要使用的端口号。如果编辑了文件，则须停止并重新启动 SNMP 子代理，这样更改能够生效。

```
# stop-msg snmp
# start-msg snmp
```

为 Windows 平台配置 SNMP 支持

虽然 SNMP 监控程序的开销非常小，但提供的 Messaging Server 一开始仍然禁用 SNMP 支持。要启用 SNMP 支持，在 DOS 提示下运行下列命令：

```
X:\> server_root\msg-instance\configutil /o local.snmp.enable /v 1
X:\> %SYSTEMROOT%\SYSTEM32\regsvr32.exe server_root\bin\msg\imta\bin\madmand.dll
```

然后，用 Windows Services 实用程序重新启动 SNMP 服务。Services 实用程序有时又称为 *Microsoft Management Console*。

请注意，Windows SNMP 服务在 Messaging Server SNMP 支持操作以前必须已经在运行。默认情况下， Windows SNMP 服务没有随 Windows NT 一起安装。必须手工安装 Windows SNMP 服务。

在 Windows NT 上安装 SNMP 服务的步骤如下：

1. 在**控制面板**右键单击**网络**图标。
2. 在**网络**窗口选择**服务**选项
3. 在**服务**对话框单击**添加 ...** 按钮。
4. 在弹出的**选择网络服务**窗口选择**网络服务**列表框中的 **SNMP 服务**。然后单击**确定**按钮。
5. Windows 开始安装 SNMP 服务。为完成安装可能需要提供 Windows NT CDROM。

关于安装 SNMP 服务更详细的信息，请参考 Microsoft 的 Windows 文档。

要撤消 Messaging Server SNMP 支持，使用命令：

```
X:\> server_root\msg-instance\configutil /o local.snmp.enable /v 0
X:\> %SYSTEMROOT%\SYSTEM32\regsvr32.exe /u server_root\bin\msg\imta\bin\madmand.dll
```

然后通过 Windows Services 实用程序重新启动 SNMP 服务。

在 Windows 平台上， `start-msg snmp` 命令和 `stop-msg snmp` 命令无效。 Messaging Server SNMP 支持在 Windows SNMP Services 下运行，而且只能通过启动或停止 Windows SNMP Services 来启动或停止。

来自 SNMP 客户机的监控

RFC 2788 和 RFC 2789 的基础 OID 是

mib-2.27 = 1.3.6.1.2.1.27

mib-2.28 = 1.3.6.1.2.1.28

使 SNMP 客户机指向那两个 OID ，并将之作为 “公共” SNMP 社区访问。

如要向 SNMP 客户机装载 MIB 副本，MIB 的 ASCII 副本位于 <*server_root*>`/plugins/snmp` 目录，文件名是：`rfc2788.mib` 和 `rfc2789.mib`。关于在 SNMP 客户机软件上装载 MIB 的指导，请参考 SNMP 客户机软件文档。MIB 使用的 `SnmpAdminString` 数据类型可能让一些老的 SNMP 客户机无法识别。在这种情况下，使用等价文件：`rfc2248.mib` 和 `rfc2249.mib`，这两个文件也在同一目录下。

在 Unix 平台上与其它 iPlanet 产品共存

其它 Netscape 或提供 SNMP 支持的 iPlanet 产品可能通过置换平台自带的 SNMP 主代理来做到这一点。如果在与 Messaging Server 同一主机上运行这样的 iPlanet 产品并想要通过 SNMP 对其进行监控，那么请配置 iPlanet Proxy SNMP Agent，详情请见 **Managing Servers with Netscape Console**（http://docs.iplanet.com/docs/manuals/console/42/html/7_snmp.htm#1024620）的第 7 章。这将允许 Messaging Server SNMP 子代理 - SNMP 自带的子代理 - 与非自带的 iPlanet SNMP 子代理在其他 iPlanet 产品中共存。

SNMP 信息来自 Messaging Server

本节总结通过 SNMP 提供的 Messaging Server 信息。关于单个 MIB 表的详细信息，请参阅：RFC 2788 和 RFC 2789。注意，按照 RFC/MIB 的术语，邮件传输服务（MTA、HTTP 等等）称作*应用程序*（`appl`），Messaging Server 网络连接称作*关联*（`assoc`），MTA 通道称作 *MTA 组*（`mtaGroups`）。

注意，在有多个 Messaging Server 实例的平台上，可能有多组 applTable 中的 MTA 和服务器以及多个其他表中的 MTA。

备注 在 MIB 中报告的汇总值（例如，传输的邮件总数，IMAP 连接总数等）在重新启动之后被重新设置为零。

每个站点有不同的阈值和重要的监控值。正常的 SNMP 客户机允许进行趋势分析并在突然出现背离历史趋势的情况时发送报警。

applTable

applTable 提供服务器信息。启动后，为单维表，内有一行 MTA 信息，而且下列的每个服务器若启用都有一行信息：Web 邮件服务 HTTP、IMAP、POP、SMTP 和 SMTP Submit。这张表提供版本信息，正常运行时间，当前操作状态（上升，下降，堵塞），当前连接数，积累连接总数以及和其他有关数据。

下面是来自 applTable（mib-2.27.1.1）数据的一个例子。

```
applTable:

    applName.1[1] = mailsrv-1[2] MTA on mailsrv-1.west.sesta.com
    applVersion.1 = 5.1
    applUptime.1 = 7322[3]
    applOperStatus.1 = up[4]
    applLastChange.1 = 7422[3]
    applInboundAssociations.1 = 5
    applOutboundAssociations.1 = 2
    applAccumulatedInboundAssociations.1 = 873
    applAccumulatedOutboundAssociations.1 = 234
    applLastInboundActivity.1 = 1054822[3]
    applLastOutboundActivity.1 = 1054222[3]
    applRejectedInboundAssociations.1 = 0[5]
    applFailedOutboundAssociations.1 = 17
    applDescription.1 = iPlanet Messaging Server 5.1
    applName.2[1] = mailsrv-1 HTTP WebMail server on mailsrv-1.west.sesta.com
    ...
    applName.3 = mailsrv-1 IMAP server on mailsrv-1.west.sesta.com
    ...
    applName.4 = mailsrv-1 POP server on mailsrv-1.west.sesta.com
    ...
    applName.5 = mailsrv-1 SMTP server on mailsrv-1.west.sesta.com
    ...
    applName.6 = mailsrv-1 SMTP Submit server on mailsrv-1.west.sesta.com
    ...
```

说明：

1. .1, .2, 等等。这里的后缀是行号， applIndex。 applIndex 的值 1 代表 MTA，值 2 代表 HTTP 服务器等等。在这个例子中，表的第一行提供 MTA 上的数据，第二行提供 POP 服务器上的数据，依此类推。
2. 实例 Messaging Server 的名称受到监控。在这个例子中，实例的名称是 mailsrv-1。
3. 这些是 SNMP 时间戳值并且是 sysUpTime 在事件发生时的值。 sysUpTime，进而是 SNMP 主代理启动后以百之一秒为单位的时间。
4. HTTP、IMAP、POP、SMTP 和 SMTP Submit 服务器的操作状态是由针对它们的实际连接决定的，完成这样的连接须通过其已配置的 TCP 端口并采用适当协议（比如 HEAD 请求 和 HTTP 响应，HELO 命令和 SMTP 响应等等）执行一简单的操作。从这次连接尝试，每个服务器的状态即被决定，包括：上升 （1），下降 （2）或堵塞 （4）。

   注意，这些检测表现为向服务器的正常入站连接，并影响每个 MIB 服务器的 applAccumulatedInboundAssociations 变量。

   MTA 的操作状态也即作业控制器的操作选状态。如果 MTA 表现为上升，那么作业控制器也上升。如果 MTA 表现为下降，那么作业控制器也下降。这种 MTA 操作状态独立于 MTA 的 服务 Dispatcher 的状态。 MTA 的操作状态的值只有上升或下降。虽然作业控制器确有 “堵塞”的概念，但是它没有作为 MTA 状态的一种。
5. 对 HTTP、IMAP 和 POP 服务器来说，applRejectedInboundAssociations MIB 变量表明失败登录尝试的数量，而不是被拒绝的入站连接尝试的数量。

applTable 用法

监控每个列出的应用程序的服务器状态 （applOperStatus）对于监控每个服务器是至关重要的。

如果 applLastInboundActivity 所表明的最后一次入站活动已经过了很久，那么可能有些部分出现故障阻碍着连接。如果 applOperStatus=2 （下降），那么受监控的服务器也下降。如果 applOperStatus=1 （上升），那么问题可能出现在别的地方。

assocTable

该表向 MTA 提供网络连接信息。这是一个二维表，提供关于每个活动网络连接的信息。这样的连接信息不是向其它服务器提供的。

下面是来自 applTable （mib-2.27.2.1）的数据的一个实例。

```
assocTable:

    assocRemoteApplication.1.1[1] = 129.146.198.167[2]
    assocApplicationProtocol.1.1[1] = applTCPProtoID.25[3]
    assocApplicationType.1.1 = peerinitiator(3)[4]
    assocDuration.1.1 = 400[5]
...
```

说明：

1. 在后缀 .x.y 中， x 是应用程序索引 applIndex，表明报告是针对 applTable 中的哪个应用程序的。在此例中，就是 MTA。 y 用来给报告中的应用程序的每个连接编号。
2. 远程 SMTP 客户机的源 IP 地址。
3. 这是一个 OID，表明网络连接所使用的协议。aplTCPProtoID 表示 TCP 协议。后缀 .n 表明使用的是 TCP 端口， .25 表明在 TCP 端口 25 上使用的协议是 SMTP。
4. 无法判断远程 SMTP 客户机是用户代理（UA）还是另一个 MTA。这样，子代理总是报告 peer-initiator ； 而从不会报告 ua-initiator。
5. 这是一个 SNMP TimeInterval 并以百分之一秒为单位。在这个例子中，连接打开了 4 秒。

assocTable 用法

该表用来诊断活动问题。例如，如果突然出现了 200,000 个入站连接，查看这个表可以知道它们是从哪里来的。

mtaTable

这是一个一维表，其中的每一行对应 applTable 表里的一个 MTA。每行为 mtaGroupTable 中的选择变量提供在相应 MTA 中所有通道 （称为组）的总数。

下面是来自 applTable （mib-2.28.1.1）中数据的一个实例。

```
mtaTable:

    mtaReceivedMessages.1[1] = 172778
    mtaStoredMessages.1 = 19
    mtaTransmittedMessages.1 = 172815
    mtaReceivedVolume.1 = 3817744
    mtaStoredVolume.1 = 34
    mtaTransmittedVolume.1 = 3791155
    mtaReceivedRecipients.1 = 190055
    mtaStoredRecipients.1 = 21
    mtaTransmittedRecipients.1 = 3791134
    mtaSuccessfulConvertedMessages.1 = 0[2]
    mtaFailedConvertedMessages.1 = 0
    mtaLoopsDetected.1 = 0[3]
```

说明：

1. 后缀 .x 提供此应用程序在 applTable 中的行号。在此例中， .1 表示这些是 applTable 表中第一个应用程序的数据。这就是 MTA 上的数据。
2. 转换通道只能取非零值。
3. 对当前存储在 MTA 邮件入队中的 .HELD 邮件文件进行计数。

mtaTable 用法

如果 mtaLoopsDetected 不是零，则存在循环邮件问题。定位并诊断 MTA 入队里的 .HELD 文件以解决问题。

如果系统对一个转换通道进行病毒扫描并拒绝带病毒的邮件，那么 mtaSuccessfulConvertedMessages 提供不包括其他转换失败在内的带病毒邮件的计数。

mtaGroupTable

这个二维表为 applTable 中的每个 MTA 提供通道信息。这些信息包括已存储（即已入队）和已传递邮件的计数这样的数据。监控已存储邮件计数 mtaGroupStoredMessages 对每个通道都是很重要的：当该值过高时，邮件服务正在队列中备份。

下面是来自 mtaGroupTable （mib-2.28.2.1）中数据的一个实例。

```
mtaGroupTable:

mtaGroupName.1.1[1] = autoreply[2]
        ...
mtaGroupName.1.2[1] = ims-ms
        ...
mtaGroupName.1.3[1] = tcp_local
    mtaGroupDescription.1.3 = mailsrv-1 MTA tcp_local channel
    mtaGroupReceivedMessages.1.3 = 12154
    mtaGroupRejectedMessages.1.3 = 0
    mtaGroupStoredMessages.1.3 = 2
    mtaGroupTransmittedMessages.1.3 = 12148
    mtaGroupReceivedVolume.1.3 = 622135
    mtaGroupStoredVolume.1.3 = 7
    mtaGroupTransmittedVolume.1.3 = 619853
    mtaGroupReceivedRecipients.1.3 = 33087
    mtaGroupStoredRecipients.1.3 = 2
    mtaGroupTransmittedRecipients.1.3 = 32817
    mtaGroupOldestMessageStored.1.3 = 1103
    mtaGroupInboundAssociations.1.3 = 5
    mtaGroupOutboundAssociations.1.3 = 2
    mtaGroupAccumulatedInboundAssociations.1.3 = 150262
    mtaGroupAccumulatedOutboundAssociations.1.3 = 10970
    mtaGroupLastInboundActivity.1.3 = 1054822
    mtaGroupLastOutboundActivity.1.3 = 1054222
    mtaGroupRejectedInboundAssociations.1.3 = 0
    mtaGroupFailedOutboundAssociations.1.3 = 0
    mtaGroupInboundRejectionReason.1.3 =
    mtaGroupOutboundConnectFailureReason.1.3 =
    mtaGroupScheduledRetry.1.3 = 0
    mtaGroupMailProtocol.1.3 = applTCPProtoID.25
    mtaGroupSuccessfulConvertedMessages.1.3 = 0[3]
    mtaGroupFailedConvertedMessages.1.3 = 0
    mtaGroupCreationTime.1.3 = 0
    mtaGroupHierarchy.1.3 = 0
    mtaGroupOldestMessageId.1.3 = <01IFBV8AT8HYB4T6UA@red.iplanet.com>
    mtaGroupLoopsDetected.1.3 = 0[4]
    mtaGroupLastOutboundAssociationAttempt.1.3 = 1054222
```

说明：

1. 在后缀 .x.y 中， x 是应用程序索引 applIndex，表明报告是针对 applTable 中的哪个应用程序。在此例中，就是 MTA。 y 用来给 MTA 中的每个通道编号。编号索引 mtaGroupIndex 也用于 mtaGroupAssociationTable 和 mtaGroupErrorTable 表。
2. 报告的通道名称。在此例中，就是 autoreply 通道。
3. 转换通道只能取非零值。
4. 对当前存储在 MTA 邮件入队中的 .HELD 邮件文件进行计数。

mtaGroupTable 用法

对 *Rejected* 和 *Failed* 的趋势分析可能对确定潜在的通道问题有用。

如果 mtaGroupStoredVolume 对 mtaGroupStoredMessages 的比率突然增高，可能意味着入队退回了一个巨大的垃圾邮件。

如果 mtaGroupStoredMessages 突然增高，可能表明正在发送大宗垃圾邮件或由于某种原因传递失败。

如果 mtaGroupOldestMessageStored 的值比无法传递邮件通知次数 （notices 通道关键字）还多，可能表明对一邮件无法进行即使象退回这样的处理。注意，退回是在夜里进行的，因此将需要使用 mtaGroupOldestMessageStored > （最大时限＋ 24 小时）检测。

如果 mtaGroupLoopsDetected 大于零，即检测到邮件循环。

mtaGroupAssociationTable

这是一个三维表，其条目是 assocTable 中的索引值。对于 applTable 表中的每个 MTA，都有一个两维子表。这个两维子表中的每一行对应相应 MTA 的一个通道。每个通道里的每个当前活动网络连接都有一个条目。这个条目的值就是 assocTable 的一个索引值（通过条目的值索引和并且要被 MTA 的 applIndex 索引查看）。这个 assocTable 中的表示条目是通道所保持的网络连接。

简单说来， mtaGroupAssociationTable 表与 assocTable 表中显示的网络连接以及 mtaGroupTable 表中的对应通道相关。

下面是来自 mtaGroupAssociationTable （mib-2.28.3.1）表中数据的一个实例。

```
mtaGroupAssociationTable:

    mtaGroupAssociationIndex.1.3.1[1] = 1[2]
    mtaGroupAssociationIndex.1.3.2 = 2
    mtaGroupAssociationIndex.1.3.3 = 3
    mtaGroupAssociationIndex.1.3.4 = 4
    mtaGroupAssociationIndex.1.3.5 = 5
    mtaGroupAssociationIndex.1.3.6 = 6
    mtaGroupAssociationIndex.1.3.7 = 7
```

说明：

1. 在后缀 .x.y.z 中，x 是应用程序索引 applIndex，表示报告的是 applTable 中的哪个应用程序。在此例中，就是 MTA。而 y 表明报告的是 mtaGroupTable 的哪个通道。在此例中， 3 表明是 tcp_local 通道。而 z 则用来给向通道打开的或来自通道的关联编号。
2. 此值是 assocTable 的一个索引值。特别是， x 和这个值分别成为 applIndex 和 assocIndex 在 assocTable 里的索引。或者，换句话说，（忽略 applIndex）assocTable 中的第一行描述受 tcp_local 通道控制的网络连接。

mtaGroupErrorTable

这是另外一个三维表，它给出每个 MTA 尝试传递邮件时遇到的临时性和永久性的错误的计数。具有索引值为 4000000 的条目是临时性错误，索引值为 5000000 的条目是永久性错误。临时性错误导致邮件重新入队以便以后尝试传递，永久性错误则导致邮件被拒绝或者作为无法传递邮件而被退回。

下面是来自 mtaGroupErrorTable （mib-2.28.5.1）中数据的一个实例。

```
mtaGroupErrorTable:

    mtaGroupInboundErrorCount.1.1.4000000[1] = 0
    mtaGroupInboundErrorCount.1.1.5000000 = 0
    mtaGroupInternalErrorCount.1.1.4000000 = 0
    mtaGroupInternalErrorCount.1.1.5000000 = 0
    mtaGroupOutboundErrorCount.1.1.4000000 = 0
    mtaGroupOutboundErrorCount.1.1.5000000 = 0

    mtaGroupInboundErrorCount.1.2.4000000[1] = 0
    ...

    mtaGroupInboundErrorCount.1.3.4000000[1] = 0
    ...
```

说明：

1. 在后缀 .x.y.z 中，x 是应用程序索引 applIndex，表示报告的是 applTable 中的哪个应用程序。在此例中，就是 MTA 而 y 表明报告的是 mtaGroupTable 的哪个通道。在此例中，1 是 autoreply 通道，2 是 ims-ms 通道，3 是 tcp_local 通道。最后，z 是 4000000 或 5000000，分别表示在该通道尝试传递邮件时遇到的临时性和永久性错误的计数。

mtaGroupErrorTable 用法

错误计数的突然增高很可能表明出现不正常传递问题。例如，tcp_channel 通道的计数突然增高可能表明出现 DNS 或网络问题。ims_ms 通道的计数突然增高可能表明向邮件存储库传递邮件时遇到问题 （例如，分区已满、存储问题，等等。）

MTA 直接 LDAP 操作

在 iPlanet Messaging Server 5.2 版之前， MTA 使用的有关用户和组的目录信息是通过许多文件和数据库存取的。这些文件和数据库中的数据更新由 `dirsync` 进程控制，该进程可监控目录的变化并相应地更新文件和数据库数据。在 5.2 版中，这仍然是默认运行状态，然而有一新选项可用来使 MTA 直接与目录交互。这个选项就是*直接 LDAP 模式*。

当被配置为按直接 LDAP 模式操作时，MTA 便可不使用 `dirsync` 进程及其数据库。取而代之的是，MTA 将进行相等的 LDAP 调用，首先确定在 MTA 上是否有托管的域，然后再存取所需的发送信息。当把 `dirsync` 操作模式更改为直接 LDAP 模式时，对地址转换几乎没有实际影响，但直接 LDAP 模式更便于配置、机制更透明。但是，受托域的工作方式还是有一些变化，对系统运行方式也有一些影响。有关详细信息，请参阅第 434 页 “转变到直接 LDAP 模式的意义”。

本章由以下的部分组成：

- 启用直接 LDAP 模式
- 直接 LDAP 模式的工作原理
- 转变到直接 LDAP 模式的意义

启用直接 LDAP 模式

启用直接 LDAP 模式时，须对标准 MTA 配置做如下改动：

1. 在文件 `.../imta/config/imta.cnf` 中的 “重写”部分中添加下一行

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

   其中， `localhost` 是 MTA 的主要主机名。

   例如，如果 MTA 叫做 `island.siroe.com`，需修改文件 `.../imta/config/imta.cnf` 中的 “规则”部分，将其改为：

   ```
   ! Rules to select   local users
   $*                  $E$F$U%$H$V$H@island.siroe.com
   island.siroe.com    $U%$D@island.siroe.com
   siroe.com           $U%$D@island.siroe.com
   ```

2. 更改 .../imta/config/imta.cnf 文件中 ims-ms 的通道定义以移除其中的 filter ssrd:$A 子句。

   如果 ims-ms 通道定义是

   ```
   ! ims-ms
   ims-ms defragment subdirs 20 notices 1 7 14 21 28  \
    backoff "pt5m" "pt10m" "pt30m" "pt1h" "pt2h" "pt4h" \
    maxjobs 1 pool IMS_POOL fileinto $U+$S@$D filter ssrd:$A
   ims-ms-daemon
   ```

   则应改为

   ```
   ! ims-ms
   ims-ms defragment subdirs 20 notices 1 7 14 21 28 \
    backoff "pt5m" "pt10m" "pt30m" "pt1h" "pt2h" "pt4h" \
    maxjobs 1 pool IMS_POOL fileinto $U+$S@$D
   ims-ms-daemon
   ```

3. 在 .../imta/config/option.dat 文件中添加下列各行：

   ```
   ALIAS_MAGIC=8764
   ALIAS_URL0=ldap:///$V?*?sub?$R
   USE_REVERSE_DATABASE=4
   REVERSE_URL=ldap:///$V?mail?sub?$Q
   USE_DOMAIN_DATABASE=0
   ```

   如果需要虚拟域支持，还必须设置下列附加的选项：

   ```
   DOMAIN_MATCH_URL=ldap:///$B?msgVanityDomain?sub? \
   (msgVanityDomain=$D)
   ALIAS_URL1=ldap:///$B?*?sub?(&(msgVanityDomain=$D)$R)
   ALIAS_URL2=ldap:///$1V?*?sub?(mailAlternateAddress=@$D)
   ```

4. 从 .../imta/config/job_controller.cnf 文件中移除下列各行：

   ```
   [PERIODIC_JOB=dirsync_incr]
   command=IMTA_TABLE:../../imsimta dirsync
   time=/00:10
   !
   [PERIODIC_JOB=dirsync_full]
   command=IMTA_TABLE:../../imsimta dirsync -F
   time=02:00/24:00
   !
   ```

5. 从文件 .../imta/config/mappings 末尾的 SEND_ACCESS 映射中移除下列各行

   ```
   *|*|inactive|*  $X4.2.1|$NMailbox$ temporarily$ disabled
   *|*|deleted|*   $X5.1.6|$NRecipient$ no$ longer$ on$ server
   ```

6. 删除，或者至少移动这些 MTA 数据库：

```
.../imta/db/aliasesdb.db
.../imta/db/domaindb.db
.../imta/db/reversedb.db
```

7. 编译已修改的 MTA 配置。这必须在其生效之前进行。

直接 LDAP 模式的工作原理

MTA 在对目标邮件地址的处理方面基本上没有变动。这一过程简述如下：首先，MTA 使用重写规则：1）确定是否有经过验证的域； 2）重写相应的地址； 3）将邮件路由到相应的通道。如果邮件被路由到 `l` 通道，则用别名查找进程转换地址 （请参阅第 420 页 “直接 LDAP 别名解析”），然后再次用重写规则重写所得地址，以将这些地址路由到与别名相关联的通道上。通常这个通道就是 `ims-ms` 通道、 `auto_reply` 通道或其它标准的 MTA 通道中的某一个。

直接 LDAP 模式操作改变了地址处理的重写规则阶段和别名阶段。这些改动会在下面的章节中说明。

- 使用直接 LDAP 模式解析地址 （$V）
- 管理地址重写期间的 LDAP 错误
- 直接 LDAP 别名解析
- 别名缓存
- 反转地址转换

使用直接 LDAP 模式解析地址 （$V）

MTA 解析地址时，首先依照重写规则检查地址中的域部分 （@ 右边的部分）。重写规则位于 `.../imta/config/imta.cnf` 文件的上半部分。如果发现匹配，规则会指定邮件将被路由到哪个通道。例如，邮件可被路由到 `tcp_local` 的出站因特网通信流，或如果是目录中配置的用户，则可将邮件路由到本地通道 `l`。

当 MTA 被配置为 `dirsync` 模式时，规则评价程序将使用域数据库中的信息，该数据库是 `dirsync` 进程维护的数据库中的一个。当 MTA 被配置为直接 LDAP 模式时，在则使用一个特殊的 “try me first”重写规则。这一规则格式如下：

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

位于规则左侧的 `$*` 模式，其含义是首先尝试这个规则，而且是在所有的地址上。规则右侧的含义是：

- `$E` - 只在信封地址上使用。
- `$F` - 只在向前指引 （`To:`）地址上使用。
- `$U%$H` - “重写”一地址为 `user@host` 格式。（规则实际上是指定使用未修改的原始地址。）

- VH - 如果地址中主机部分，即地址中 @ 符号的右边部分，与定义在目录中的一个域相匹配，则只匹配此规则。
- @localhost - 发送到 l 通道。

LDAP 域查找功能的工作原理

重写规则进程的新部分是 $V 匹配参数。 $V 用来确定一地址是否是本地的，若是，则在目录树中查找其位置。 $V 需要一个表示地址主机部分的参数，如此例中的 $H。 $V 标记可将几个 LDAP 查找同时投入运行。查找过程包括在 DC 树中查找地址中的域部分，以发现用户树和组树的相应的子树。例如，如果有关地址是：

```
robinson.crusoe@desert.island.siroe.com
```

MTA 首先检查域 desert.island.siroe.com，如果失败，再依次检查 island.siroe.com、siroe.com 以及 com。这一 LDAP 查找通常在目录中的 DC 树中进行（有关 iPlanet Messaging Server 名字空间和 DIT 结构的详细说明，请见 **iPlanet Messaging Server Provisioning Guide**）。此树所在的位置是由 service.dcroot 配置属性指定的，默认值为 o=internet。查找对象为那些有判别名的条目：

```
dc=desert,dc=island,dc=siroe,dc=com,o=internet
dc=island,dc=siroe,dc=com,o=internet
dc=siroe,dc=com,o=internet
dc=com,o=internet
```

如果找到的条目是 inetDomain 的对象类和 inetDomainBaseDn 的属性，或是 inetDomainAlias 的对象类和 aliasedObjectName 属性，一次域查找才视为成功。

如果想防止对上一级域的检查，如例子中的 island.siroe.com、 siroe.com 和 com，就需清除 DOMAIN_UPLEVEL 选项的最低有效位。 DOMAIN_UPLEVEL 是在文件 .../imta/config/option.dat 中指定的。它的默认值是 1，以便防止上一级检查添加下行:

```
DOMAIN_UPLEVEL=0
```

to .../imta/config/option.dat.

这里有另一个新标记， $Z，其含义与 $V 完全相反。 $V 在目录中找到主机时使一条规则与之匹配， $Z 则在目录中找不到主机时使一条规则与之匹配。

虚拟域查找

如果有为任何用户定义的任何虚拟域 （不是受托域），也需要为之启用 LDAP 检查。虚拟域检查在默认设置中是禁用的。要启用虚拟域检查，需要把下列各行添加到文件 .../imta/config/option.dat 中：

```
DOMAIN_MATCH_URL=ldap:///$B?msgVanityDomain?sub? \
  (msgVanityDomain=$D)
```

仅当受托域检查失败时，才会进行虚拟域检查。

域查找缓存

检查所有域中的目录是一项开销很大的操作，因为它必须在所有的域中执行，包括任何有邮件向之发送的 internet 域。为了减少开销，查找的结果被 MTA 缓存。按默认方式，多达 100000 个结果 （成功与否）可缓存长达 600 秒。缓存方式可以通过设置文件 .../imta/config/option.dat 中的下列选项而加以控制。

```
DOMAIN_MATCH_CACHE_SIZE=100000
DOMAIN_MATCH_CACHE_TIMEOUT=600
```

管理地址重写期间的 LDAP 错误

在目录中的查找域时，有四种可能出现的结果。

- 找到域且状态良好
- 找到域但状态不好
- 找不到域
- 查找失败 （LDAP 错误）

第一种情况说明没有问题。第二种情况和第三种情况将被当作同一问题进行处理，并导致 $V 规则失败。最后的一种情况是比较困难的。在这种情况下， MTA 有两套可采取的合理操作：

1. 拒绝带有 *400 Temporary lookup failure* SMTP 响应。
2. 将邮件重定向到 reprocess 通道等待稍后处理。

如果邮件来自某些远端 MTA，第一种操作是显然的和正确的。如果邮件来自一用户代理提交的邮件，第二种操作更适合。MTA 需要区分这两种情况并采取相应的行动。启用这一处理机制的是 MTA 选项 DOMAIN_FAILURE。 DOMAIN_FAILURE 指定在一个字符串，用来在域查找失败的情况下覆盖一个重写规则中的不用部分。因此，如果 DOMAIN_FAILURE 的默认值为

```
DOMAIN_FAILURE=reprocess-daemon$Mtcp_local$1M$1~-error$4000000?Temp
orary lookup failure
```

并且被处理的重写规则是标准的

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

以及由 VH 语句所实施的域查找失败，则处理继续进行，如同重写规则为：

```
$*      $E$F$U%$H$V$H@reprocess-daemon$Mtcp_local$1M$1~-error$400000
0?Temporary lookup failure
```

结果规则的处理如下：

- $E - 只有在信封地址上使用。
- $F - 只在向前指引 （To:）地址上使用。
- $U%$H -“重写”一地址为 user@host 格式。（规则实际上指定使用未修改的原始地址）。
- VH - 如果地址中主机部分，即地址中 @ 符号的右边部分，与定义在目录中的一个域相匹配，则只匹配此规则。这会遇到一个 LDAP 错误，从而生成修改的规则。

- `@reprocess-daemon` - 路由到 reprocess 通道。
- `$Mtcp_local` - 如果来源通道不是 `tcp_local`，则“失败”。这个失败是处理开始以来的结果。规则的处理继续进行。
- （`$1M`）- 如果通道不是一个象 `reprocess` 或 `conversion` 这样的内部再处理通道，则“失败”。
- `$~` - 如果规则当前是失败的，以一次成功匹配停止处理。
- – 错误 - 将目标通道变更为无效通道 `reprocess-daemon-error`
- `$4000000?Temporary lookup failure` - 将 SMTP 扩展错误码设置为 4.0.0 并将相应的出错信息文本设置为 “`Temporary lookup failure`”。

因此，如果来源通道是 `tcp_local`（在所有可能的源于某些远程 MTA 的连接中）则重写规则成功，但没有 `reprocess-daemon-error` 的通道存在，因而地址被拒绝，并以规则中指定的 `400` 出错代码而被拒绝。

如果源通道是 `tcp_intranet` （可能是一个用户代理），规则成功地将邮件路由到 `reprocess` 通道。

这个 `DOMAIN_FAILURE` 选项和由之创建的有效的重写规则使用某些新的重写标记。

`$1M` 与现存的 `$Mchannel` 标志类似，当源通道是一个 reprocess 通道时会引起一个规则失败。大致上等同于 `$Mreprocess$Mprocess$Mdefragment$conversion`。

`$~` 使通道执行任何由 `$M` 或 `$1M`（或 `$M` 或 `$1N`）标志所指定的匹配检查，如果结果是失败，立即以一个成功终止处理。

`$abbbccc?text` 指定在出错事件发生时使用的出错代码和出错信息文本。出错代码实际上是三个十进制数 `a`、 `bbb`、 `ccc` 并生成扩展的 SMTP 结果代码：`a.bbb.ccc`。

直接 LDAP 别名解析

别名解析的作用是提取邮件的进入地址（别名），并产生一个用来传递邮件到一个通道的电子邮件的地址。这个地址被称为*传递地址*，通常有形式 *uid@ 通道名称*。

重写规则只考虑地址的 `@` 标记右边的部分。但是，别名解析潜在地考虑整个地址。使用于地址解析的机制由文件 `.../imta/config/option.dat` 中的 `ALIAS_MAGIC` 选项所控制。默认行为是在 `aliases` 文件和由 `dirsync` 进程维护的 `aliases` 数据库中查找一个匹配。（参阅第 113 页 “别名”。）

为了启用直接 LDAP 操作，增加以下各行到文件 `.../imta/config/option.dat` 中。

```
ALIAS_MAGIC=8764
```

这导致使用 `aliases` 文件尝试进行别名解析 （通常仅用于网站的 Postmaster），然后通过 LDAP 目录。 LDAP 别名解析在产生一个发送通道前要经过一系列。这些步骤如下：

1. 在 LDAP 目录中寻找地址的用户 / 组条目。
2. 确定条目类型 （用户或组）。
3. 提取条目状态 （例如：`active`, `inactive`, `deleted`, `hold`）。

4. 提取 uid 属性。
5. 寻找用户位置。
6. 核实邮件的长度没有超过指定的限制。
7. 产生基于 mailDeliveryOption 属性 （例如：邮箱、自动回复、程序和转发）的传递地址。

这部分的剩余内容对每一步进行了详细地说明。

在 LDAP 目录中寻找用户 / 组条目

查找别名地址的用户 / 组条目的 LDAP 查询是由文件 .../imta/config/option.dat 中的以下选项所指定的 URL 定义的：

```
ALIAS_URL0
ALIAS_URL1
ALIAS_URL2
```

除非支持虚拟域，仅使用 ALIAS_URL0。这个选项的推荐设置是

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

处理 $V 标志类似于处理在第 418 页“LDAP 域查找功能的工作原理”中描述的 $V 标志。如果地址的域名部分查找成功的话， URL 中的 $V 即被找到的条目中的 inetDomainBaseDn 属性或 aliasedObjectName 属性所指向的 DN 所置换。如果查找失败，别名将无法扩展（存在着 $V 标志的一个可用变体 $1V，如果查找失败，返回用户树和组树最顶层的 DN - local.ugldapbasedn 的值。）

$R 被一个适合于在用规划的过滤器置换，该规划是通过 configutil 的参数 local.imta.schematag 定义的。对于匹配的邮件地址，可能的规划值和要搜索的属性如下：

```
ims50     mail,mailalternateAddress,mailEquivalentAddress
nms41     mail,mailalternateAddress
sims40    mail,rfc822mailalias
```

local.imta.schematag 可以指定多于一个这样的值，但须用逗号隔开。如果指定了多个规划，相关属性的并被搜索以寻找一个匹配。如果目录规划不能完全匹配这些规划中的任何一个，可以通过指定 configutil 参数 local.imta.mailaliases 来覆盖被搜索的属性列表。例如：

```
local.imta.mailaliases=mail,mailAlternateAddresses,email
```

启动一次搜索，以寻找在 mail、mailAlternateAddresses 和 email 等属性上的匹配项。

默认情况下，由 $R 标志生成的过滤器只搜索给定的地址。但是，可能需要使别名表示更高层的域。因此，尽管在 desert.island.siroe.com 域中已经提供了 robinson.crusoe，还可能需要在域树的所有域中匹配其用户名。因此，如果在重写规则的评估中匹配的域是 siroe.com，那么在目录中搜索的地址是

```
robinson.crusoe@desert.island.siroe.com
robinson.crusoe@island.siroe.com
robinson.crusoe@siroe.com
```

为了达到这样的效果，必须设置 DOMAIN_UPLEVEL 选项的次最低有效位，例如添加如下行到文件 .../imta/config/option.dat 中：

```
DOMAIN_UPLEVEL=3
```

在非标准目录中的域查找

如果你不能使用由用户和组树中分离出来的标准目录结构 DC 树，可用另一种机制来寻找树的基以便在其中搜索别名。与上述在 ALIAS_URL0 中使用的 $V 不同的是，您可以调用一个映射。完成这种操作的语法是，用下面的短语来替换 URL 中的 $V：

$|/*mapping-name*/*mapping-argument*|

| 启动和终止 CALLOUT。紧接在 $| 后的字符是映射名和参数之间的分隔符；所选择的分隔符不得同用于映射名或参数中的字符值发生冲突。 *mapping name* 是*域查找*映射表的名称。*mapping-argument* 是域的名字，例如：$D 成为一个域的名字。

虚拟域别名的域查找

为了支持虚拟域别名，下列附加 URL 必须在文件 .../imta/config/option.dat 中定义

```
ALIAS_URL1=ldap:///$B?*?sub?(&(msgVanityDomain=$D)$R)
ALIAS_URL2=ldap:///$1V?*?sub?(mailAlternateAddress=@$D)
```

别名解析过程中的 LDAP 失败

在目录中的别名查找的结果可以是 0，1，或几个结果。如果与多于一个条目相匹配，查找被认为失败，就象没有结果返回，该地址将作为非法地址而被拒绝。对于任何原因，如果所设置的目录服务器没有一个能连接，或如果 LDAP 查找导致出错，地址将以临时失败的提示（SMTP 中 4xx 错误）而被拒绝。发送的 MTA 会稍后重试邮件，那时目录问题可能已经解决。

确定条目类型

一旦一条目在目录中被发现，它就能够被处理并且邮件能够被传递到适当的通道。处理条目的第一步是判断它是否代表了一个用户、组或者不可识别的任何类型。如果我们发现条目是一个用户或一个组，处理会正常地继续进行。如果条目既不是用户又不是组，条目以及地址即被忽略。

条目类型是通过观察条目所属的对象类来决定的。用户和组所必需的对象类是目录在用规划所暗示的，就象被 local.imta.schematag 设置所定义了一样。必须为不同的规划中一个用户或组的条目而加以定义的对象类是：

```
ims50:      users:    inetLocalMailRecipient + inetmailuser
            groups:   inetLocalMailRecipient + inetmailgroup

nms41:      users:    mailRecipient + nsMessagingServerUser
            groups:   mailGroup

sims40:     users:    inetMailRouting + inetmailuser
            groups:   netMailRouting + inetmailgroup
```

如果目录规划不能与这些规划中的任何一个完全相匹配，则可以定义自己的识别因子，以便于识别不同的用户和组的目录条目。 MTA 选项 LDAP_USER_OBJECT_CLASSES 和 LDAP_GROUP_OBJECT_CLASSES 可用来指定对象类，这些对象类必须显式地作为一个条目给出并分为用户或组两类。例如，增加以下各行到 .../imta/config/option.dat 文件中。

```
LDAP_USER_OBJECT_CLASSES=inetLocalMailRecipient+inetmailUser,
mailRecipient+nsMessagingServerUser

LDAP_GROUP_OBJECT_CLASSES=inetLocalMailRecipient+inetmailgroup,
mailGroup
```

与设置 local.imta.schematag=ims50,nms41 下述方面是等价的：如果一个条目有对象类 inetLocalMailRecipient 和 inetmailUser，或者由对象类 mailRecipient 和 nsMessagingServerUser，该条目即被确定为一个用户。

提取用来创建传递地址的属性

一旦地址条目的类型确定了，MTA 需要从域和用户或组条目中提取一系列属性来创建发送地址并且传递邮件。来自域和用户或组条目中的下列属性中的部分或全部（请参阅表 B-1，表 B-2 和表 B-3）会被提取出来。下列表格给出了所用的必需的默认属性名，以及用来选择不同属性名的 MTA 选项。通常这些选项不会设置为同标准规划相符的默认值。但是，你的目录可能针对这些属性中的一个或多个属性使用了不同的属性名，这些属性名可通过在 .../imta/config/option.dat 中设置适当的选项来改变。

表 B-1　默认域属性和 Override 选项

LDAP 属性名称	MTA Override 选项
domainUidSeparator	LDAP_DOMAIN_ATTR_UID_SEPARATOR
mailDomainCatchallAddress	LDAP_DOMAIN_ATTR_CATCHALL_ADDRESS
mailDomainConversionTag	LDAP_DOMAIN_ATTR_CONVERSION_TAG
mailDomainMsgMaxBlocks	LDAP_DOMAIN_ATTR_BLOCKLIMIT
mailDomainReportAddress	LDAP_DOMAIN_ATTR_REPORT_ADDRESS
mailDomainSieveRuleSource	LDAP_DOMAIN_ATTR_FILTER
mailDomainStatus	LDAP_DOMAIN_ATTR_STATUS
mailRoutingHosts	LDAP_DOMAIN_ATTR_ROUTING_HOSTS
mailRoutingSmarthost	LDAP_DOMAIN_ATTR_SMARTHOST

表 B-2　默认用户属性和 Override 选项

LDAP 属性名	MTA override 选项
mailConversionTag	LDAP_CONVERSION_TAG
mailDeliveryFileURL	LDAP_PROGRAM_INFO
mailDeliveryOption	LDAP_DELIVERY_OPTION
mailhost	LDAP_MAILHOST
mailMsgMaxBlocks	LDAP_BLOCKLIMIT
mailMsgQuota	LDAP_MESSAGE_QUOTA
mailProgramDeliveryInfo	LDAP_PROGRAM_INFO
mailQuota	LDAP_DISK_QUOTA
mailRoutingAddress	LDAP_ROUTING_ADDRESS
mailSieveRuleSource	LDAP_FILTER
UID	LDAP_UID
	LDAP_SPARE_1*
	LDAP_SPARE_2*

* 这两个备用的 LDAP 选项很重要，因为它们可用于替代传递选项模式。具体说明，请见后面的“配置传递选项”。

表 B-3　默认组属性和 Override 选项

LDAP 属性名称	MTA override 选项
mailRejectText	LDAP_REJECT_TEXT
memberURL	LDAP_GROUP_URL2
mgrpAddHeader	LDAP_ADD_HEADER
mgrpAllowedBroadcaster	LDAP_AUTH_URL
mgrpAllowedDomain	LDAP_AUTH_DOMAIN
mgrpAuthPassword	LDAP_AUTH_PASSWORD
mgrpBroadcasterPolicy	LDAP_AUTH_POLICY
mgrpDeliverTo	LDAP_GROUP_URL1
mgrpDisallowBroadcaster	LDAP_CANT_URL
mgrpDisallowDomain	LDAP_CANT_DOMAIN

表 B-3　默认组属性和 Override 选项（接上页）

LDAP 属性名称	MTA override 选项
mgrpErrorsTo	LDAP_ERRORS_TO
mgrpMsgMaxSize	LDAP_ATTR_MAXIMUM_MESSAGE_SIZE
mgrpMsgPrefixText	LDAP_PREFIX_TEXT
msgpMsgSuffixText	LDAP_SUFFIX_TEXT
mgrpModerator	LDAP_MODERATOR_URL
mgrpRemoveHeader	LDAP_REMOVE_HEADER
mgrpRFC822MailMember*	LDAP_GROUP_RFC822
rfc822MailMember*	LDAP_GROUP_RFC822
uniqueMember	LDAP_GROUP_DN

* 注意，按默认方式，即可使用 mgrpRFC822MailMember 又可使用 rfc822MailMember，但不能同时使用。

提取用户 / 组状态

控制生成的传递地址的关键属性之一就是用户 / 组和域的状态。如果 mailDomainStatus 所定义的域状态是 inactive 或 deleted，则作为用户状态使用，而用户状态就不再加以检查。如果域状态是 active，则使用用户或组条目的状态。用什么属性来定义条目状态，取决于所使用的规划。如下所示：

```
ims50:        users:     inetuserstatus or mailuserstatus
              groups:    inetmailgroupstatus
nms41:        NO STATUS ATTRIBUTES
sims40:       users:     inetsubsscriberstatus
              groups:    inetmailgroupstatus
```

如果有必要，用来定义用户和组状态的属性名可以被覆盖。选项 LDAP_USER_STATUS 可以用来指定用于用户状态的属性， LDAP_GROUP_STATUS 选项可以用来指定用于组状态的属性。一旦用户或组的状态确定了，它将是 active、 inactive、 deleted 或 hold 中的一种。

active - 如果发现用户或组的状态是 active （活动的），处理将如第 426 页 “用户位置”中描述的那样继续进行。

inactive - 如果发现用户或组的状态是 inactive （非活动的），地址将以一个临时失败的提示 （4xx SMTP 出错代码）而被拒绝。

deleted - 如果发现用户或组的状态是 deleted（被删除的），地址将以一个临时失败的提示（5xx SMTP 出错代码）而被拒绝。

hold - 如果发现用户或组的状态是 hold （保留），生成一个别名来使地址被重写到 hold 通道中。生成的别名被 HOLD_TEMPLATE MTA 选项所指定的模式所控制。模板的默认值是：

```
$M?$2I@hold-daemon
```

模式中标志的含义在第 427 页 “使用 DELIVERY_OPTIONS 生成传递地址”中说明。如果给出的地址是

```
robinson.crusoe@desert.island.siroe.com
```

并且匹配条目给出一个在 island.siroe.com 的受托域中的 rcrusoe 的 UID，生成别名应为

```
rcusoe?island.siroe.com@hold-daemon
```

该地址与文件 .../imta/config/imta.cnf 中的同重写规则相匹配。

```
hold-daemon    $U%$H@hold-daemon
```

它匹配但不修改地址，因此邮件被传递到 hold 通道。

提取 UID

目录中所有有效用户条目必须有一个 uid 属性，组条目*可以*有一个 uid。 uid 是用来生成传递地址的。如果一个用户条目没有 uid 属性，该条目被忽略。如果一个用户有多个 uid 属性，只使用第一个。

有时，目录中的 uid 属性可能包含了比需要的还要多的信息。例如，受托域的条目可能具有这样的形式：真实的 uid，一个分隔字符 （由 domainUidSeparator 属性定义），然后是一个域 （例如：uid=walter@siroe.com）。如果分隔字符出现在 uid 中，则用于构建别名的 uid 仅是分隔字符之前的那部分。

如果有必要使用除 uid 外的一个属性作为传递地址的 uid，则 LDAP_UID 选项可以用来指定该属性名。

用户位置

一旦一个用户或者组被确定为一个活动用户，MTA 必须检查确认该用户是这个 MTA 的本地用户。要认定为本地用户，一条目必须有一个 mailhost 属性，它或者与 local.hostname configutil 属性匹配，或者与 local.imta.hostnamealiases configutil 属性所指定的名称之一匹配。如果用户是本地的， MTA 进行下一步 - 确认邮件没有超越大小限制。

如果 mailhost 不能与这个 MTA 的任何名称相匹配，一个新的地址，其格式为

```
@mailhost:user@domain
```

被生成。这是一个源路由 RFC822 地址，它将通过重写规则而被处理。对于源路由地址，重写规则查将之看成是域部分。

如果一用户条目没有 mailhost 属性，那么生成的地址将使用 mailRoutingSmarthost，但必须关联这个域：

```
@smarthost:user@domain
```

如果用户没有 mailhost 属性并且域没有 mailRoutingSmartHost，地址被放弃并生成一个 5xx 出错报告。

如果一个组没有 mailhost 属性，组将再本地处理。这个明显的矛盾是重要的，因为对于一个在入站转发 MTA 上 - 而不是在一个特定的服务器上 - 进行扩展的组来说，有时是有意义的。

提取大小限制

有一个 MTA 必须在传递地址被构建 （为用户）或组被扩展之前进行的最终检查。这个最终检查保证邮件消息自身没有超越该用户的 mailMsgMaxBlocks 属性，或者，如果该属性没有设置，没有超越该域的 mailDomainMsgMaxBlocks 属性。如果邮件太大，地址会以一个 5xx size exceeded 错误被拒绝。

使用 DELIVERY_OPTIONS 生成传递地址

如果找到的条目是一个用户条目，它保留下来仅用于生成用户的传递地址，它将通过将规则重写到相应的通道而使邮件向回路由。传递地址生成处理也对组进行，但是对于组有一些额外事由将在以后的章节中说明。

通过一组模式生成传递地址。所用模式取决于为属性 mailDeliveryOption 所定义的值。对于每个合法的 mailDeliveryOption 都将生成传递地址。这个模式是由 MTA 选项 DELIVERY_OPTIONS 定义的，该选项可在文件 .../imta/config/option.dat 中定义。DELIVERY_OPTIONS 默认值是

```
DELIVERY_OPTIONS=*mailbox=$M%$2I+$2S@ims-ms-daemon,
       &members=*,
       *native=$M@native-daemon,
       *unix=$M@native-daemon,
       &file=+$F@native-daemon,
       hold=$M?$2I@hold-daemon,
       &$members_offline=*,
       program=$M%$P@pipe-daemon,
       forward=**,
       *autoreply=$M@autoreply-daemon
```

DELIVERY_OPTIONS 的值是用逗号分隔的一组规则。每个规则的左边是传递方法的名称（例如：mailbox、unix、forward ），右边是构建传递地址的模式。每个规则的前面都可以有一个或两个特殊标志字符，以影响如何和何时应用规则。这些标记字符是

*　　这个规则仅应用于用户

&　　这个规则仅应用于组

$　　这个标志使邮件在 reprocess 通道入队这样扩展即可在脱机进行。

因此，传递方法 mailbox、native、unix 以及 autoreply 只能为用户所使用。传递方法 members 和 members_offline 只能为组所使用，传递方法 program 和 forward 可被用户和组二者使用。

右边由简单替代文本和一些标志组成，这些标志插入各种 LDAP 属性的值。请参阅第 259 页“置换标志 （不区别大小写）”。

生成传递地址 - 例子

设想，作为一个例子，一邮件发送到地址

```
robinson.crusoe+goats@desert.island.siroe.com
```

假定目录条目中包含属性

```
UID: rcrusoe@desert.island.siroe.com
mail: robinson.crusoe@desert.island.siroe.com
mailDeliveryOption: mailbox
mailDeliveryOption: native
mailDeliveryOption: program
mailDeliveryOption: forward
mailDeliveryOption: autoreply
mailProgramDeliveryInfo: capriform.msg
mailForwardingAddress: friday@desert.island.siroe.com
mailForwardingAddress: hulahula@londonbank.siroe.com
```

那么原始地址将生成六个别名，一个别名对应一种传递方法，即 `mailbox`、 `native`、 `program` 和 `autoreply`，另两个别名对应传递方法 `forward`。

`mailbox` 的模式 `$M%$2I+$2S@ims-ms-daemon`，是相当复杂的一个。

表 B-4　传递选项 mailbox 的模式扩展

模式组合	操作	结果
`$M`	生成 `rcrusoe`	`rcrusoe`
`%`	生成 `%`	`rcrusoe%`
`$2I`	生成 `desert.island.siroe.com`	`rcrusoe%desert.island.siroe.com`
`+`	生成 `+`	`rcrusoe%desert.island.siroe.com+`
`$2S`	生成 `goats`	`rcrusoe%desert.island.siroe.com+goats`
`@ims-ms-daemon`	生成 `@ims-ms-daemon`	`rcrusoe%desert.island.siroe.com+goats@ims-ms-daemon`

此结果地址有一个域部分，它严格匹配 `ims-ms` 通道的通道标志，所以被路由到该通道而无须进一步重写。

这个 `native` 的模式 `$M@native-daemon` 简单一些。

传递选项 native 的模式扩展。

表 B-5　传递选项 native 的模式扩展

模式组合	操作	结果
$M	生成 rcrusoe	rcrusoe
@native-daemon	生成 @native-daemon	rcrusoe@native-daemon

此结果地址有一个域部分，它严格匹配 native 通道的通道标志，因此被传递到该通道而无须进一步重写。

autoreply 模式 $M@autoreply-daemon 非常简单。

表 B-6　传递选项 autoreply 的模式扩展

模式组合	操作	结果
$M	生成 rcrusoe	rcrusoe
@autoreply-daemon	生成 @autoreply-daemon	rcrusoe@autoreply-daemon

此结果地址有一个域部分，它严格匹配 autoreply 通道的通道标志，因此被传递到该通道而无须进一步重写。

program 模式 $M%$P@pipe-daemon 几乎等同于：

表 B-7　传递选项 program 的模式扩展

模式组合	操作	结果
$M	生成 rcrusoe	rcrusoe
%	生成 %	rcrusoe%
$P	生成 prog	rcrusoe%prog
@pipe-daemon	生成 @pipe-daemon	rcrusoe%prog@pipe-daemon

此结果地址有一个域部分，它严格匹配 pipe 通道的通道标志，因此被传递到该通道而无须进一步重写。

forward **. 的模式只是生成属性 mailForwardingAddress 所使用的值而已，从而产生下列地址：

```
friday@desert.island.siroe.com
hulahula@londonbank.siroe.com
```

因此，发送到 robinson.crusoe 的邮件可生成下列传递地址并且被发送到下列通道：

```
rcrusoe%desert.island.siroe.com+goats@ims-ms-daemon      ims-ms
rcrusoe@native-daemon                                    native
rcrusoe@autoreply-daemon                                 autoreply
rcrusoe%prog@pipe-daemon                                 pipe
friday@desert.island.siroe.com
hulahula@londonbank.siroe.com
```

SIEVE 规则

最终从用户条目中获得的 LDAP 属性是 mailSieveRuleSource。此属性包含用户的 SIEVE 过滤器规则。在邮件到达要入队到传递通道这一点以前这些规则不被应用。尽管在 MTA 扩展别名时获得 SIEVE 过滤器，不被使用直到要到结果传递地址被扩展并被发送到 ims-ms、native、autoreply 或者 pipe 通道之后， SIEVE 规则才被使用。注意出自 non-dirsync 操作模式的行为改变: 在该模式下，只有传递到 ims-ms 通道的邮件才通过 SIEVE 规则进行处理。

处理组条目

对于组这有四个可用的程序传递选项。它们是 program、 forward、 members 和 members_offline。

program 和 forward 是专为用户设立的。

members 和 members_offline 二者的模式是 *，它调用组扩展处理的全部功能，并将在下一部分中说明。

members_offline 规则的前面缀以 $，意味着组扩展发生在 reprocess 通道。如果入队的通道不是 reprocess 通道 - 最初入队的通道几乎肯定是 tcp_ 通道中的一个 - 则地址处理停止，原始地址被接受，邮件入队到 reprocess 通道。当 reprocess 通道运行时，采用与处理地址相同的逻辑，所不同的是，入队的通道是 reprocess 通道，因此对 members_offline 及其 $ 处理与对 members 的处理完全相同。

原则上，处理组是直接的：有一对属性可将组成员列出，或者作为电子邮件地址，或者作为判别名。无论哪种情况，那些地址都被作为部分组扩展的结果使用。

实际上，组处理所涉及的属性比上述情况要多得多，有超过一打的其它的属性能够影响组条目得处理。

处理组条目的详细信息

MTA 通过依次考虑每个不同的组处理选项来处理一组条目。选项的处理顺序是重要的。组属性可大致分为三类：

- 为诸如 `mailRejectText` 这样的处理提供参数的属性。这些参数不对做或不做产生影响，但是能为处理提供一些输入。
- 控制在何种情况之下邮件能够被发送到列表的属性。这包括如 `mgrpAllowDomain` 这样的属性，它指定那个域可向组提交邮件。这些属性被处理的顺序在下边表格中列出。
- 给出列表实际成员资格的属性。

下面表格列出了组的处理属性。

表 B-8　提供组处理参数的属性

属性	说明
`mailRejectText`	在任何与组相关联的认证机制引发邮件被拒绝的情况下，提供作为 SMTP 响应的返回文本。这个属性应该是一个以 US-ASCII 表示的单值属性，仅服从 SMTP 协议规则。如果属性是多值的，那么只使用第一个值。如果值的表示不止一行，只采用第一行。
`mgrpMsgMaxSize`	陈旧的属性。应当取而代之地使用 `mailmsgMaxBlocks`，因为该条目在开始处理时就已检查完毕。如果邮件超过这个值 （以字节计），邮件将以 *message too large* （邮件太大）错误而被拒绝。
`mgrpAuthPassword`	如果指定的 `mgrpBroadcasterPolicy` 需要一个密码，则需指定一个组密码并使用这个密码。
`mgrpErrorsTo`	信封原创者 （MAIL FROM）地址会被设置成这个属性的一个值，如果指定了该属性的话。如果不指定，邮件的原创者地址保持不变。
`mgrpAddHeader`	（目前尚不支持）
`mgrpRemoveHeader`	（目前尚不支持）
`mgrpMsgPrefixText`	（目前尚不支持）
`mgrpMsgSuffixText`	（目前尚不支持）

表 B-9　邮件组访问控制属性

属性	说明
mgrpBroadcasterPolicy	指定发送一邮件到组所需要的认证级别。可能的级别是： SMTP_AUTH_REQUIRED 或 AUTH_REQ 二者都意味着必须在用 SMTP AUTH 命令鉴别了发件人之后，才能邮递到组。 PASSWORD_REQUIRED、 PASSWD_REQUIRED 或 PASSWD_REQ，无论哪个都意味着针对 mgrpAuthPassword 属性指定的列表的密码必须出现在一个邮件的 Approved: 标题字段中。 NO_REQUIREMENTS 与未提供属性的效果相同，因此没有特殊要求。
mgrpAllowedDomain	多值。列出用户能提交邮件到组的域。若没有，任何域的用户都能够邮寄邮件到组。
mgrpDisallowedDomain	多值。列出用户不能够邮寄邮件到组的域。
mgrpAllowedBroadcaster	URL 在扩展时生成一个允许发送到通道列表的地址表。如果 URL 扩充的结果地址是一个组，那么这个组将扩展以生成一个详细列表，但是只限于 MTA 扩展 URL。针对每个作为这种扩展结果的地址来检查邮件的信封收件人地址，只有匹配成功的那个邮件才是被允许的邮件。
mgrpDisallowedBroadcaster	URL 在扩展时生成一个不允许发送到通道列表的地址表。如果 URL 扩充的结果地址是一个组，那么这个组将扩展以生成一个详细列表，但是只限于 MTA 扩展 URL。针对每个作为这种扩展结果的地址来检查邮件的信封收件人地址，只有匹配成功的那个邮件才是被允许的邮件。
mgrpModerator	URL 在扩展时生成一个允许发送到通道列表的地址表。如果 URL 扩充的结果地址是一个组，那么这个组将扩展以生成一个详细列表，但是只限于 MTA 扩展 URL。针对每个作为这种扩展结果的地址来检查邮件的信封收件人地址。 如果信封收件人地址与这些地址中的一个匹配，则邮件来自中介人，而且允许邮寄到组。 如果信封收件人地址不与这些地址中的任何一个相匹配，那么邮件将被发送到刚扩展的中介人地址的列表，并不以其他任何方法发送到组。也就是说，在下面组成员表中的所有属性将被忽略，并且任何 program 或 forward 传递选项也将被忽略。

表 B-10　邮件组扩展属性

属性	说明
mgrpDeliverTo	URL 在扩展时生成一个地址表。如果 URL 扩充的结果地址是一个组，那么这个组被扩展以生成一个详细列表，以此类推。重复的地址将被消除，但又可能创建相互参照的组，从而产生无限递归。MTA 为解决这个问题，只允许列表扩展嵌套到 10 层。
memberURL	另一个 URL 列表以 mgrpDeliverTo 相同的方式被扩展。
uniqueMember	组成员的判别名。每 DN 能够参照用户条目、组条目或者目录中一个子目录，在后一种情况下目录中的所有条目都将被扩展。
mgrpRFC822MailMember, rfc822MailMember	这些属性的值是组的成员邮件住址。在对于任何给定的条目，只有这些属性中的一个中被允许。对 rfc822MailMember 的支持只是为了提供对 Netscape Messaging Server 的向后兼容性。

别名缓存

所有的这种 LDAP 活动可严重影响 MTA 的性能。为了减轻这种影响， MTA 进程将缓存 LDAP 查找的结果。这样的缓存操作是受到下列各选项控制的，显示内容包含默认值：

```
ALIAS_ENTRY_CACHE_SIZE=1000
ALIAS_ENTRY_CACHE_TIMEOUT=600
ALIAS_ENTRY_CACHE_NAGATIVE=0
```

这意谓缓存条目的最大数是 1000 条，而且条目保存的最长度时间是十分钟 （600 秒）。这里的缓存条目比域缓存条目要大，但是如果系统上有足够的内存，增加缓存大小可能是值得的。ALIAS_ENTRY_CACHE_NEGATIVE 控制匹配失败的别名是否缓存。默认为不缓存。不缓存失败别名会加速新用户活动，而且使这样的情况不太可能：重复的失败尝试将使得以一种影响系统的性能的频率传递同一用户。

反转地址转换

反转地址，如 From: 标题，通常在流经 MTA 时被规范化。（规范化意味着在标题地址中，个人名称被移到前面，而注释则被移到后面。此外，对于 From: 地址，查地址被查找，如果发现是一个 mailalternateaddress 地址，就转而使用邮件地址。）通常所应用的原则是，用户目录条目中列出第一个邮件地址就是应使用的地址。处理包括在 DC 树中查找地址的域部份，以发现要在其中查找地址的用户树和组树的子树，然後查找这样一个条目：它包含任何匹配给出的地址条目的电子邮件地址，并返回该条目的第一邮件地址。这是一个和别名处理非常相似的处理。

直接 LDAP 地址转换依赖于在文件 .../imta/config/option.dat 中设置的两个选项。

```
USE_REVERSE_DATABASE=4
REVERSE_URL=ldap:///$V?mail?sub?$Q
```

USE_REVERSE_DATABASE=4 通知 MTA 不要使用旧的反转数据库，而是改为使用直接 LDAP 机制。这个 REVERSE_URL 与 ALIAS_URL0 URL 非常相似，这在第 421 页“在 LDAP 目录中寻找用户 / 组条目”中已有讨论。$V 标志被扩展的方式在该节中有说明。$Q 标志类似于用于标准的 ALIAS_URL0 中的 $R 标志，不同的是生成一个过滤器搜索含有地址的属性，该地址可能与 MTA 正试图匹配的反转地址匹配。被 $R 生成的过滤器依靠设置的 local.imta.schematag configutil 选项：

```
ims50          mail,mailalternateAddress
nms41          mail,mailalternateAddress
sims40         mail,rfc822mailalias
```

通过在 MTA 选项 LDAP_MAIL_REVERSES 中加以指定，可以覆盖搜索要使用的属性。

实际生成的搜索非常类似于用于别名查找 $R 标志所生成的搜索：不但搜索最初给出的地址，而且还搜索这样的地址：它含有在 DC 树置换中实际找到的域。这在第 421 页“在 LDAP 目录中寻找用户 / 组条目”中有说明。

如果反转地址查找失败，反转地址保持不变。

如同其它 LDAP 查找，反转地址查找的结果被缓存。缓存的大小和超时由选项控制，如下所示（包括默认值）：

```
REVERSE_ADDRESS_CACHE_SIZE=10000
REVERSE_ADDRESS_CACHE_TIMEOUT=600
```

转变到直接 LDAP 模式的意义

对于 MTA 地址转换，从 dirsync 操作模式改为 LDAP 模式几乎没有明显的影响，但处理更方便配置并且其机制更透明然而，这一转换改变了受托域的工作方式。在 dirsync 模式中，受托域的所有子域隐含地归自己拥有，这相当于在直接 LDAP 模式中设定 DOMAIN_UPLEVEL=3。然而，只有实际配置的域属于 principle domain，这相当于在直接 LDAP 模式中设定 DOMAIN_UPLEVEL=0。操作模式的这种分歧在直接 LDAP 模式不存在：你必须拿定主意，选择一种你所需要的域所有权机制。这种不同大概没有差别，但是应该清除。

显然对系统运行的整体状况有一些影响。所影响之处是：

- 改变了的 LDAP 负荷。
- 减少了对数据库的依赖。
- 改变了总体邮件吞吐量。

改变了 LDAP 负荷

dirsync 处理产生少量的但带来大量潜在的基于 LDAP 目录的检索。在直接 LDAP 模式中，MTA 在目录上生成许多小的检索。实际效果是，吞吐量的明显减少不是因为所使用的缓存。然而，施加于目录上的负荷变得更加常规，因此系统具有了更好的可扩展性。同时对于 dirsync 来说，很难将一个 MTA 扩展到超过大约 6 百万用户，而在直接 LDAP 模式中应当能够提供一千万个用户。

减少对数据库的依赖

在 dirsync 模式中， MTA 的操作依赖于许多的数据库，特别是别名数据库和域数据库。如果一个系统突然失败，这些数据库具有复杂的磁盘结构，在突遇系统故障时容易遭到损坏。对于高效系统这被证明是一个问题领域。在直接 LDAP 模式中，MTA 对数据库几乎没有依赖。

改变了整体邮件吞吐量

增加目录使用和减少数据库使用对吞吐量有一定的影响。从目录中提取信息并将之处理为要求的格式比起简单地在数据库中查找结果又更多的开销。然而，如果条目在缓存中发现，整体代价就小于在数据库中查找。这意谓如果大多数邮件的处理是针对少数用户的，而这些用户的条目又在缓存中，则吞吐量上升。如果邮件分布在一个大的用户社区，吞吐量将下降。

针对直接 LDAP 模式下邮件吞吐量的性能调整

系统性能对于别名缓存的大小很敏感，缓存的大小通过 ALIAS_ENTRY_CACHE_SIZE 设置。这个默认值是 1000，对任何重要的系统可能都太小：这些缓存条目可以比较大，大约 2K 字节，而默认值是选来避免一个小型系统超负荷的。对于一个大系统，合理取值可能高达 10,000 甚至 50,000。为使这种改变有用，增加 dispatcher.cnf 中的 MAX_LIFE_CONNS 的值是很重要的。MAX_LIFE_CONNS 应该至少两倍，或许四倍于 ALIAS_ENTRY_CACHE_SIZE，以发挥缓存的优势。从 dirsync 操作模式转变到直接 LDAP 模式，地址转换几乎没有变化，但配置和机制更透明了。

在 iPlanet Messaging Server 中管理 Event Notification Service

本附录说明如何在 iPlanet Messaging Server 中启用 iPlanet Event Notification Service Publisher 程序 （ENS Publisher）并管理 iPlanet Event Notification Service （ENS）。

本章 / 附录包括下列各节：

- 将 ENS Publisher 载入 iPlanet Messaging Server
- 运行样板 Event Notification Service 程序
- 管理 Event Notification Service

有关 ENS 和 ENS API 的详细说明，请见位于 *iPlanet Calendar Server* 和 *Messaging Server Documentation* 网页的 **iPlanet Messaging and Collaboration Event Service Notification Manual**。

将 ENS Publisher 载入 iPlanet Messaging Server

Event Notification Service (ENS) 是 iPlanet 的基础 “发布 - 订阅服务”。 ENS 起着调度程序的作用，iPlanet 的应用程序把它当作收集某种相关*事件*的中心点。所谓 “事件”是指资源的一个或多个属性的值所发生的变化。任何应用程序，如果需了解这些事件发生的时间，可在 ENS 注册，由其识别事件的顺序并将通知与订阅匹配起来。

ENS 和 iBiff（iPlanet Messaging Server 的 ENS 发布程序）是与 iPlanet Messaging Server 捆绑提供的软件。系统的默认设置是启用 ENS，但并不载入 iBIFF。（请参阅 “将 ENS Publisher 载入 iPlanet Messaging Server”）。

若需订阅 iPlanet Messaging Server 的通知服务，您需先在 iPlanet Messaging Server 主机上载入 `libibiff` 文件，然后停机并重新启动 Messaging Server。

将 ENS Publisher 载入 iPlanet Messaging Server

请从命令行执行下列步骤。在这些操作步骤， iPlanet Messaging Server 安装目录的位置是 *server_root*， iPlanet Messaging Server 用户是 *mailsrv*。这些变量的典型值分别为 `/usr/iplanet/server5` 和 `mailsrv`。

1. 先以 `mailsrv` 运行 `configutil` 实用程序，以载入 `libibiff` 文件。

   `cd` *server_root*`/msg-`*instance*

```
./configutil -o "local.store.notifyplugin" -v "server_root/bin/msg/lib/libibiff"
```

2. 然后以 `root` 停机并重新启动 Messaging Server。

   `cd` *server_root*`/msg-`*instance*

   `./stop-msg`

   `./start-msg`

3. 此后，您便可通过 ENS 接收通知了。有关详细说明，请见 “运行样板 Event Notification Service 程序”。

运行样板 Event Notification Service 程序

iPlanet Messaging Server 提供了一写样板程序，供您学习使用如何接收通知。这些样板程序位于 *server_root*`/bin/msg/enssdk/examples` 目录。

运行 ENS 样板程序

1. 换到 *server_root*`/bin/msg/enssdk/examples` 目录。
2. 用 C 编译器，通过 `Makefile.sample` 文件编译 `apub` 和 `asub` 范例。将程序库搜索路径设置为包括 *server_root*`/bin/msg/lib` 目录。
3. 待程序编译后，便可在分开的窗口中按下列运行之：

   `apub localhost 7997`

   `asub localhost 7997`

   您在 `apub` 窗口中键入的任何内容都应在 `asub` 窗口中显示。另外，如果使用的默认设置，则所有 iBiff 通知都应在 `asub` 窗口中显示。

4. 若需接收 iBiff 发布的通知，可编写一个类似 `asub.c` 的程序。

   有关样板程序和编写自用的 ENS 程序方面的详细说明，请参见 *iPlanet Event Notification Service for Messaging and Collaboration Manual*。

备注 当把程序库搜索路径设置为包括 *server_root*`/bin/msg/lib` 目录时，您将不再能停止和启动目录服务器。迂回方法是从程序库搜索路径中移除该条目。

管理 Event Notification Service

ENS 的管理工作包括：启动和停止服务以及更改配置参数以控制 ENS 的 iBiff 出版程序的行为。

启动和停止 ENS

您可通过 `start-msg ens` 和 `stop-message ens` 命令启动和停止 ENS 服务器。但必须以 `root` 用户身份运行这些命令。

启动和停止 ENS

- 启动 ENS：

  server_root/msg-*instance*/**start-msg ens**

- 停止 ENS：

  server_root/msg-*instance*/**stop-msg ens**

iPlanet Event Notification Service 配置参数

可控制 iBiff 行为的配置参数有下列几个。请用 `configutil` 实用程序设置这些参数。

表 C-1　iBiff 配置参数

参数	说明
`local.store.notifyplugin.maxHeaderSize`	用于指定可与通知一起传输的报头的最大大小（以字节为计算单位）。默认值为 8192 个字节。
`local.store.notifyplugin.maxBodySize`	用于指定可与通知一起传输的正文部分的最大大小（以字节为计算单位）。默认值为 100 个字节。
`local.store.notifyplugin.`*`eventType`*`.enable`	用于指定特定的事件类型是否可生成通知。详情请见 *iPlanet Messaging Server for Messaging and Collaboration Manual* 中说明的各种 *eventTypes* （事件类型），如 `ReadMsg`、`NewMsg` 等。有效值为 1（启用）和 0（禁用）。默认值是 1；即若将 `local.store.notifyplugin.ReadMsg.enable` 设置为 0 将禁用 `ReadMsg` 通知功能。
`local.store.notifyplugin.ensHost`	用于指定 ENS 服务器的主机名。默认设置是 `127.0.0.1`。

表 C-1　iBiff 配置参数 （接上页）

参数	说明
`local.store.notifyplugin.ensPort`	用于指定 ENS 服务器的 TCP 端口。默认值为 `7997`。
`local.store.notifyplugin.ensEventKey`	用于指定使用 ENS 通知所需的事件密钥。默认设置是 `enp://127.0.0.1/store`。该事件密钥的主机名部分不是用来确定 ENS 主机的。这只是 ENS 使用的一个独特的标识符。 该密钥是用户在订阅时应使用的密钥，以便能够接收与此密钥相匹配的有关通知。

管理邮件用户和邮件发送列表

本附录说明如何使用 Console 界面创建并管理用户邮件帐户和邮件发送列表。建议您**不要**使用在此描述的 Console 界面创建和管理用户以及邮件发送列表，而应使用 iPlanet Delegated Administrator for Messaging 的 Delegated Administrator 命令行实用程序创建和修改用户以及邮件发送列表。有关用户 / 组命令行实用程序的说明，请参阅 **iPlanet Messaging Server Reference Manual**。

注意	如果使用在此附录中描述的 Console 界面创建用户和组，您将无法用 Delegated Administrator 查看和对其进行修改。iPlanet 建议您使用 iPlanet Delegated Administrator for Messaging 的 Delegated Administrator 命令行实用程序或 **iPlanet Messaging Server Provisioning Guide** 中提供的指令创建 / 修改用户和组。

本附录包含以下各节：

- 管理邮件用户
- 管理邮件发送列表

备注	如果安装的是 iPlanet Directory Server 5.1，您则必须通过 iPlanet Console 5.0（与 Directory Server 5.1 一起安装）对其进行管理。iPlanet Messaging Server 5.2 必须通过 Netscape Console 4.2 （与 Messaging Server 5.2 一起安装）进行管理。

管理邮件用户

访问邮件用户

本节说明在需要对用户进行管理时如何打开邮件管理界面。 Messaging Server 邮件帐户是以用户条目属性储存在公司企业的中央 LDAP 用户目录中的。因此在管理邮件帐户时，须在该目录中修改用户条目。

创建新用户

要创建新的邮件帐户，要先在目录中创建一个新用户。还必须为创建的用户安装一个邮件帐户，如果没有为用户安装邮件帐户，用户则无法使用 Console 中的邮件管理部分。（**Managing Servers with Netscape Console** 第 4 章的“User and Group Administration”一节中较详细地说明了创建用户并为其指定其他种类用户信息的全部过程。）

新建邮件用户：

1. 在 Console 主窗口中，单击“用户和组”选项卡。
2. 从下拉列表中选择 “新用户”，然后单击 “创建”。
3. 选择用户的组织单位，然后单击 “确定”按钮。“创建用户”窗口随即打开。
4. 请按照 **Managing Servers with Netscape Console** 第 4 章的 “User and Group Administration”一节中的说明输入用户的有关信息。
5. 保持 “创建用户”窗口的打开状态，然后单击 “帐户”选项卡。右侧面板上此时显示为新用户帐户安装的产品列表。
6. 单击 “安装邮件帐户”复选框。“邮件”选项卡随即显示在 “创建用户”窗口中。
7. 在 “创建用户”窗口中单击 “邮件”选项卡，然后单击右侧面板中所需的选项卡。
8. 输入修改内容后，单击 “创建用户”窗口底部的 “确定”按钮。

备注 请在单击确定按钮之前确保已在所有相关选项卡中完成了全部设置工作。

访问现有用户

若需修改现有的某个邮件帐户或为现有的用户添加邮件功能，首先需要访问用户目录中的相应用户，然后再添加或修改该用户的邮件帐户属性。

访问现有用户的邮件信息：

1. 在 Console 主窗口中，单击“用户和组”选项卡。
2. 在 “用户和组”主窗口内，单击 “搜索”或 “高级搜索”按钮。
3. 在搜索窗口中输入搜索条件 （例如用户的姓氏），然后在用户目录中进行搜索。
4. 返回到 “用户和组”主窗口中，从搜索结果中选择一个用户，然后单击 “编辑”。
5. 如果在 “编辑条目”窗口中没有显示 “邮件”选项卡，请按下列步骤操作：
   a. 单击 “帐户”选项卡。右侧面板上随即显示已安装的帐户列表。
   b. 选中 “邮件帐户”复选框。“邮件”选项卡随即显示在 “编辑条目”窗口中。
6. 在 “编辑条目”窗口中单击 “邮件”选项卡，然后单击右侧面板中所需的选项卡。
7. 输入修改内容，然后单击 “编辑条目”窗口底部的 “确定”按钮。

指定用户电子邮件地址

在邮件能够被成功地发送给用户之前，必须为该用户指定邮件地址信息。此地址信息包括 Messaging Server 主机名，用户的主地址以及任何备用地址。主机名和主地址信息是必须有的，备用地址信息是可选的。

指定用户的邮件地址信息：

1. 在 Console 中，按照第 441 页“访问邮件用户”中的说明访问“创建用户”或“编辑条目”窗口。
2. 单击“邮件”选项卡。
3. 如果“设置”选项卡为非现用状态，则单击该选项卡。
4. （必须填写项）输入 Messaging Server 主机名。

   即托管 Messaging Server 的机器，该用户的邮件完全由其处理。该主机名必须是 Messaging Server 所在机器的全限定域名 （FQDN）。
5. （必须填写项）输入用户的主电子邮件地址。

   主地址是向该用户发送邮件的公开地址。一个用户只可以有一个主地址，该地址必须是符合 RFC 821 规定的、有效的、格式正确的 SMTP 地址。

   如果要使用主机名隐藏功能 （即：使用户地址信息中的主机名不显示在发出邮件的邮件头中），请不要在主电子邮件地址字段中指定主机名。而应在备用地址中包含主机名（请见下一步说明）。
6. （选项）在“备用地址”列表中添加地址。

   备用地址实际上是用户主地址的别名。该功能可以达到以下目的：

   - 确保正确地向经常发生拼写错误的地址传递邮件 （例如“Smith”作为“Smythe”的别名）。
   - 启用在发出邮件邮件头中隐藏主机名功能。启用该功能时，须提供一个包含主机名的备用地址，但不要提供用户主电子邮件地址中的主机名。例如，输入 `jsmith@siroe.com` 作为主电子邮件地址，然后输入 `jsmith@sesta.com` 作为备用地址。当该用户发送邮件时，发送的邮件头以 `jsmith@siroe.com` 显示，但所有发往该地址的邮件（包括回复邮件）则实际上经路由选择被发往 `jsmith@sesta.com`（假定 `sesta.com` 是一个有效的主机名）。

   您可以为特定用户指定任意数目的备用地址，但每一备用地址必须是独特的。向这些别名中任意一个发送的邮件将直接转到主地址中。

   添加备用地址：

   a. 单击“备用地址”字段下方的“添加”按钮。
   b. 在“备用地址”窗口中输入备用地址信息。（可以添加所希望的任意数量的备用地址，但每次打开该窗口时只能输入一个地址。）
   c. 单击“确定”按钮后便可添加备用地址，并可用此按钮关闭备用地址窗口。（若需输入另一个备用地址，再次单击“添加”按钮即可重新打开“备用地址”窗口。）

7. 在完成了对该用户邮件信息的所有修改后，可单击 “编辑条目”窗口底部的 “确定”按钮。否则，单击其他选项卡继续进行修改。

配置传递选项

Messaging Server 支持三个主要的、能够启用和配置的邮件传递选项，对每一个用户而言，这三个选项可以任意组合。既可以提供常规的 POP/IMAP 传递，也可以提供程序传递和 UNIX 传递 （UNIX Messaging Server 主机的客户端）。

iPlanet Delegated Administrator for Messaging 也支持终端用户的 HTML 界面，通过该界面用户可以自己启用和配置这三个选项。 Console 界面和 Delegated Administrator 界面两者都使用相同的目录属性，当每一种界面打开时都显示当前的设置，无论这些设置是由系统管理员还是由用户自己设置的。

配置用户的传递选项：

1. 在 Console 中，按照第 441 页 “访问邮件用户”中的说明访问 “创建用户”或 “编辑条目”窗口。
2. 单击 “邮件”选项卡。
3. 单击 “传递”选项卡。
4. 选择欲为该用户启用的一个或多个传递方法：
   - 若需指定 POP/IMAP 传递，请遵照第 444 页 “指定 POP/IMAP 传递”中的说明。
   - 若需指定程序传递，请遵照第 445 页 “指定程序传递”中的说明。
   - 若需指定 UNIX 传递，请遵照第 445 页 “指定 UNIX 传递”中的说明。
5. 在完成了对该用户邮件信息的所有修改后，可单击 “编辑条目”窗口底部的 “确定”按钮。否则，单击其他选项卡继续进行修改。

指定 POP/IMAP 传递

指定该选项后，邮件将传递到用户常规的 POP3 或 IMAP4 邮箱。若需为用户启用 POP/IMAP 传递，请按下列步骤操作：

1. 单击 “传递”选项卡。
2. 选中 POP/IMAP 复选框，然后单击 “属性”按钮打开 “POP/IMAP 传递”窗口。
3. （选项）输入邮件存储库分区别名 （不是路径名或绝对物理路径），即等待处理的用户邮件所需传递和保存的分区。如果不填写该字段，系统将使用当前主分区。有关详细信息，请参阅第 263 页 “邮件存储库的管理”。
4. （选项）输入分配给该用户的存储限制，或磁盘空间配额。磁盘空间配额可以是指定的默认值（参阅第 270 页 “配置邮件存储库空间配额”）、无限 （没有最大存储量限制），或是一个指定的极限 （以 KB 或 MB 为单位）。
5. （选项）输入分配给该用户的邮件数量限制。该限制可以是指定的默认值（参阅第 270 页 “配置邮件存储库空间配额”）、无限 （没有最大存储个数限制），或是一个指定的极限（数量）。

指定程序传递

指定该选项后，系统将把邮件转发到一个外部应用程序进行处理，然后再传递给用户。

备注 本节只说明如何使程序传递选项对某单个用户生效。在使该选项对某个用户生效之前，必须先整体启用程序传递模块，以执行其他几项管理任务。有关详细信息，请参阅第 212 页 “使用管道通道传递邮件到程序”。

若需为用户启用程序传递功能，请按下列步骤操作：

1. 单击 “传递”选项卡。
2. 选中 “程序传递”复选框，然后单击 “属性”按钮打开 “程序传递”窗口。
3. 输入处理该用户邮件所使用的外部应用程序命令。
4. 单击 “确定”。

指定 UNIX 传递

指定该选项后，即为用户选择了 UNIX 传递功能。 UNIX 传递能够将邮件发送到用户指定的 UNIX 邮箱中。 UNIX 传递只对那些 Messaging Server 运行于 UNIX 主机上的用户有效。

若需为用户启用 UNIX 传递功能，请按下列步骤操作：

1. 单击 “传递”选项卡。
2. 选中 “UNIX”传递复选框。

备注 若需为 Messaging Server 用户提供 UNIX 传递，还必须执行正常的 UNIX 邮件管理任务。

指定转发地址

Messaging Server 的邮件转发功能可将用户邮件转发到用户主地址之外的另一个地址，也可以将邮件同时发送到另一个地址和主地址。

iPlanet Delegated Administrator for Messaging 提供终端用户 HTML 界面，通过该界面用户可以自己指定转发地址。 Console 界面和 Delegated Administrator 界面两者都使用相同的目录属性，当每一种界面打开时都显示当前的设置，无论这些设置是由系统管理员还是由用户自己设置的。

指定用户的转发地址信息：

1. 在 Console 中，按照第 441 页 “访问邮件用户”中的说明访问 “创建用户”或 “编辑条目”窗口。
2. 单击 “邮件”选项卡。

3. 单击“转发”选项卡。

   如果该用户有转发地址，“转发地址”字段则显示当前的转发地址。

4. 若需添加一个转发地址，可单击“添加”。

5. 在“转发地址”窗口中输入转发地址。

6. 在“邮件转发”选项卡中单击“确定”将地址添加到“转发地址”字段，并关闭“转发地址”窗口。

7. 在完成了对该用户邮件信息的所有修改后，可单击“编辑条目”窗口底部的“确定”按钮。否则，单击其他选项卡继续进行修改。

备注 对于同一 Messaging Server 上的两个用户而言，如果两个用户帐户都没有启用其他传递类型，则不要为这两个用户设置指向对方地址的转发地址。否则将产生邮件传递问题。

配置自动回复设置

您可通过 iPlanet Messaging Server 的邮件自动回复功能为用户指定对所有到访邮件的自动应答方式。您可指定三种不同的自动回复模式：回送模式、休假模式以及自动回复模式。

iPlanet Delegated Administrator for Messaging 还提供终端用户使用的 HTML 界面，通过该界面用户可以自己启用和配置自动回复设置。 Console 界面和 Delegated Administrator 界面两者都使用相同的目录属性，当每一种界面打开时都显示当前的设置，无论这些设置是由系统管理员还是由用户自己设置的。

若需为用户启用自动回复服务，请按下列步骤操作：

1. 在 Console 中，按照第 441 页“访问邮件用户”中的说明访问“创建用户”或“编辑条目”窗口。

2. 单击“邮件”选项卡。

3. 单击“自动回复”选项卡。

4. 选择一种自动回复模式：

   关闭：关闭该用户的自动回复功能。

   回送：自动应答收到的每一封邮件。如果选择这个模式，则需在“邮件”字段中输入应答信息。

   休假：用户从给定发件人处收到第一封邮件时将产生一个自动应答；此后再从该发件人处收到邮件时将不产生应答，直到达到自动回复超时限制为止。当达到超时限制时，系统将发送一封新邮件，下一次再达到超时限制时，再一次发送，如此反复。如果选择这种模式，则须使用休假开始 / 结束日期选项，并在回复文本字段中输入回复邮件。

5. 如果选用了休假模式，就要提供日期和时间以确定自动回复邮件的开始和结束时间。

   - 选中“休假开始 / 结束日期”复选框。
   - 单击“开始和结束日期”的编辑按钮，然后使用屏幕上的日历指定日期和时间。

6. 指定以小时或天为单位的自动回复超时限制。
7. 如果选择了回送或休假模式，则需先输入自动回复主题行，然后输入一封返回给发件人的回复邮件。

   用户可以为内部发件人和外部发件人分别输入不同的回复邮件。如果只输入针对内部发件人的回复邮件，那么只有位于同一个网域的发件人才能收到自动回复。

   几种可选语言中的任一种都能够用来创建邮件，从位于邮件文本区域上方的下拉列表中选择所需的语言。
8. 在完成了对该用户邮件信息的所有修改后，可单击“编辑条目”窗口底部的“确定”按钮。否则，单击其他选项卡继续进行修改。

配置特许服务

若需启用该用户在访问邮件时可使用的邮件服务。请按下列步骤操作：

1. 在 Console 中，按照第 441 页“访问邮件用户”中的说明访问“创建用户”或“编辑条目”窗口。
2. 单击“邮件”选项卡。
3. 单击“特许服务”选项卡。

   特许服务窗口此时将显示特定域可使用的服务项。
4. 单击相关按钮即可添加、编辑或删除服务。此时屏幕上出现“修改特许服务规则”窗口。
5. 从服务下拉列表中，选择希望为其创建规则的服务项（IMAP, POP, SMTP, HTTP, 全部）。
6. 指定允许或拒绝的项目并指定此规则适用的域。
7. 单击“确定”按钮提交所做的修改。

管理邮件发送列表

访问邮件发送列表

本节说明如何打开邮件发送列表的管理界面。因为 Messaging Server 的邮件发送列表以组条目属性的形式存储在 LDAP 用户目录中，所以管理邮件发送列表时须访问和修改组目录。

创建新组

若需新建一个邮件发送列表，须在目录中创建一个新组。还需为该组安装邮件帐户；如果没有安装邮件帐户， Console 的邮件管理部分则不能用于该组。（**Managing Servers with Netscape Console** 第 4 章的“User and Group Administration”一节中较详细地说明了创建目录组并为其指定其他种类组信息的全部过程。）

若需新建邮件发送列表，请按下列步骤操作：

1. 在 Console 主窗口中，单击“用户和组”选项卡。
2. 从下拉列表中选择“新组”，然后单击“创建”。
3. 为该组选择一个组织单位，然后单击“确定”。
4. 在“创建组”窗口中，请按照 **Managing Servers with Netscape Console** 第 4 章的“User and Group Administration”一节中的说明输入创建组条目所需的信息。

   注意，仅就邮件发送列表来说，添加成员时*没有必要*使用“用户和组成员”选项卡，而用“邮件帐户仅电子邮件成员”选项卡就可添加成员：

   - 组的正式成员不仅拥有全部的邮件发送列表权限，而且同时还具有作为组成员应有的任何其他权限。您可通过“成员”选项卡添加正式成员（静态或动态均可）。
   - 邮件发送列表成员拥有的组权限，局限于由该组邮件发送列表组件（可能是，也可能不是该组存在的唯一目的）所提供的权限。邮件发送列表成员被称之为*仅电子邮件成员*，可通过“邮件”选项卡添加。

5. 保持“创建组”窗口的打开状态，然后单击“帐户”选项卡。

   右侧面板上此时显示为该组帐户安装的产品列表。

6. 选中“邮件帐户”复选框。

   “邮件”选项卡随即显示在“创建组”窗口中。

7. 在“创建组”窗口中单击“邮件”选项卡，然后单击右侧面板中适当的选项卡。
8. 输入所做的修改，然后单击位于在“创建组”窗口底部的“确定”按钮。

   此项操作将提交输入的条目，并关闭“创建组”窗口。

备注	单击任意邮件管理窗口底部的“确定”按钮时，系统将提交已经输入到所有邮件管理选项卡中的所有当前邮件配置信息。请在单击“确定”按钮之前检查是否已在所有相关窗口中完成了全部设置工作。

访问现有的组

若需修改现有的邮件发送列表，或向现有组中添加邮件发送列表功能，先须访问邮件目录中相应的组，然后再添加或修改该组的邮件帐户属性。

若需访问现有组的邮件发送列表信息，请按下列步骤操作：

1. 在 Console 主窗口中，单击“用户和组”选项卡。
2. 在“用户和组”主窗口内，单击“搜索”或“高级搜索”按钮。
3. 在搜索窗口中输入搜索条件（例如组名），然后对用户目录进行搜索。
4. 返回到“用户和组”主窗口，从搜索结果中选择一个组，然后单击“编辑”按钮。

5. 如果在 “编辑条目”窗口中没有显示 “邮件”选项卡，请按下列步骤操作：
   - 单击 “帐户”选项卡。右侧面板上随即显示已安装的帐户列表。
   - 选中 “邮件帐户”复选框。“邮件”选项卡随即显示在 “编辑条目”窗口中。
6. 单击编辑条目窗口中的 “邮件”选项卡，然后单击右侧面板中所需的选项卡。

   （这些选项卡和通过 “创建组”窗口访问的选项卡是一样的。）
7. 输入所需的修改，然后单击 “编辑条目”窗口底部的 “确定”按钮以提交所做的修改。

指定邮件发送列表设置

在邮件能成功地发送到邮件发送列表中之前，必须指定其邮件地址信息。邮件地址信息包括组的主地址和任何可接受为主地址别名的备用地址。还可以指定列表所有者、供选用的说明性信息、成员、属性、限制条件和邮件发送列表的操作项 （应答电子邮件）。

若需指定邮件发送列表信息，请按下列步骤操作：

1. 在 Console 中，按照第 447 页 “访问邮件发送列表”中的说明访问 “创建组”或 “编辑条目”窗口。
2. 单击 “邮件”选项卡。
3. 如果 “设置”选项卡为非现用状态，则单击该选项卡。
4. （必须填写项）输入邮件发送列表的主电子邮件地址。

   主电子邮件地址是向该邮件列表发送邮件的公开地址。每个列表只能有一个主地址。该地址必须是符合 RFC 821 规定的、格式正确的 SMTP 地址。
5. （选项）为邮件发送列表指定一个备用地址。

   备用地址是组主地址的别名。该功能可以达到以下目的：
   - 确保向经常发生拼写错误的地址进行正确传递。
   - 启用在发出邮件邮件头中隐藏主机名功能。启用该功能时，须提供一个包含主机名的备用地址，但不要提供该组主电子邮件地址中的主机名。

   您可以为一个组指定任意数目的备用地址，但每一备用地址必须是独特的。向这些别名中任意一个发送的邮件将直接转到主地址中。

   若需添加一个备用电子邮件地址，请按下列步骤操作：

   a. 单击 “备用电子邮件地址 “字段下方的”添加 “按钮。

   b. 在 “备用电子邮件地址 “窗口中输入一个备用地址。（可以添加所希望的任意数量的备用地址，但每次打开该窗口时只能输入一个地址。）

   c. 单击“确定 “按钮便可添加该备用地址并关闭 “备用电子邮件地址”窗口。（要输入另一个备用地址，可再次单击“添加”按钮以重新打开 “备用电子邮件地址”窗口。）

6. （选项）在“错误”字段中输入某人的电子邮件地址，以便将列表发送邮件时出错的信息发往此人。

7. （选项）在“Messaging Server 主机名”字段中输入托管发送邮件列表的机器的主机名。

   如果该邮件发送列表的“主电子邮件地址”字段中包含主机名，则可空白不填。如果以主电子邮件地址中不显示主机名之方式启用主机名隐藏功能，则须在此字段中指定主机名。

   与用户邮件帐户不同是，如果不为邮件发送列表指定主机名，任何能访问该列表 LDAP 条目的主机都能够处理该列表（在大多数情况下这正是您所希望的）。如果希望限定该列表只能由特定的一台或多台主机处理，则需要指定一个或多个主机名。例如，可以强行将一个大组的处理任务由一个利用率低的服务器承担，以此降低负荷较大的服务器的压力。

   请注意，此窗口一次只能输入一个主机名。若需输入多个主机名，请使用命令行工具 `ldapmodify`。

8. （选项）输入邮件发送列表所有者。

   列表所有者拥有添加或去除用户的管理权限，还可以修改配置设置或删除列表。

   若需指定一个新的列表所有者，请单击“所有者”选项卡，然后做下列之一：

   - 单击“添加”，然后在“输入列表所有者 DN”窗口中输入新的邮件发送列表所有者的判别名 (DN)（例如 `uid=jsmith, ou=people, o=siroe.com`）并单击“确定”。
   - 要想查找某个所有者可以单击“搜索”打开“搜索用户和组”窗口。

   请注意，从“搜索用户和组”窗口中选择一个所有者将自动为用户添加正确的 DN 语法。有关“搜索用户和组”窗口的详细说明，请参见 **Managing Servers with Netscape Console** 第 4 章的“User and Group Administration”一节。

9. （选项）添加说明性信息。

   如果为了信息说明（不是为 Messaging Server 所用）而需要添加文本或 URL，可单击“说明”选项卡，然后使用下列一种或全部选项：

   - 输入有关此邮件发送列表的目的或性质的说明性信息。
   - 输入指向 HTML 页面的 URL，提供其它有关此邮件发送列表的信息。这仅仅是为了说明情况， Messaging Server 并不使用该 URL。

10. 如果已经完成对该邮件发送列表的所有修改，则可单击“编辑条目”窗口底部的“确定”按钮。否则，单击其他选项卡继续进行修改。

指定列表成员

需要添加邮件发送列表的仅电子邮件成员时，可以使用下列一种或全部方法：

- 直接在邮件发送列表中添加每一个成员。
- 定义用户目录使用的动态标准，以作为确定组成员资格的过滤器。

此处说明的邮件发送列表成员在 Console 的用户和组界面中被称为*仅电子邮件成员*，因为这些成员拥有的组权限受限于该组的邮件发送列表组件所提供的权限。通过该界面的不同部分（见 **Managing Servers with Netscape Console** 中的说明）添加的“正式”组成员，可能拥有邮件发送列表成员所不拥有的其它权限或责任。有关组信息的详细说明，请见 **Managing Servers with Netscape Console** 第 4 章中的“User and Group Administration”一节。

定义动态成员资格标准

动态标准由 LDAP 搜索 URL 构成，LDAP 搜索 URL 是搜索用户目录以便确定成员资格的过滤器。该机制的动态性在于，当一个组的邮件进站时，能够接收该邮件的个体成员是通过目录搜索来确定的，而不是由静态的名称列表提供的。因此无须直接跟踪每一个成员就能够创建和维护非常大或复杂的组。

LDAP 的搜索过滤器必须符合 LDAP URL 的语法格式。有关构建 LDAP 过滤器的详细说明，请见 **Managing Servers with Netscape Console** 第 4 章中的“User and Group Administration”一节。另请参阅 iPlanet Directory Server 说明书和 RFC 1959。

LDAP URL 的语法如下：

```
ldap://hostname:port/base_dn?attributes?scope?filter
```

此处 URL 的选项有下列含义：

表 D-1　　LDAP URL 的选项

选项	说明
主机名	Directory Server 的主机名（自动使用 Messaging Server 使用的默认 Directory Server 主机名）。
端口	LDAP 服务器的端口号。如果没有指定端口号，默认值为 Messaging Server 使用的标准 LDAP 端口。
base_dn	目录中某条目的判别名，用做搜索基。该组件是必须输入项。
属性	系统返回的属性。这些属性由 Messaging Server 提供。
范围	搜索范围： 范围 `base` 只基于 （*base_dn*）这个搜索基本身检索信息。 范围 `one` 在搜索基的下一级检索信息 (不包含搜索基一级）。 范围 `sub` 在搜索基以及其下所有条目中检索信息。
过滤器	应用于特定搜索范围内条目的搜索过滤器。如果没有指定过滤器，则使用 （`objectclass=*`）。

下面是 LDAP 搜索 URL 的一个例子，用来过滤邮件主机为 Sunnyvale 的用户：

```
ldap:///o=Siroe Corp,c=US??sub?(&(mailHost=sunnyvale.siroe.com)
  (objectClass=inetLocalMailRecipient))
```

上述 URL 的过滤对象为：用户是 Siroe 组织的成员（`o=Siroe`），位于美国（`c=US`），邮件主机为 Sunnyvale（`mailHost=sunnyvale`）。`objectClass` 属性可用来定义要搜索的条目的类型，在这个例子中为 `inetLocalMailRecipient`（`objectClass=inetLocalMailRecipient`）。

请注意，当使用 Console 创建搜索过滤器时，所有的组名都将被忽略，也就是说搜索结果中只包含用户名，而不包含组成员。此设置之目的是为了避免搜索结果中用户和组成员之间的重复现象。此设置能够替代使用命令行配置工具（`configutil`），但不推荐这样做。

如下一节所述，Console 提供有模板窗口（Construct LDAP Search URL 窗口），您可借助该窗口构建搜索 URL。

添加发送邮件列表成员

在邮件发送列表中添加（仅电子邮件）成员时，请按下列步骤操作：

1. 在 Console 中，按照第 447 页“访问邮件发送列表”中的说明访问“创建组”或“编辑条目”窗口。
2. 单击“邮件”选项卡。
3. 单击“仅电子邮件成员”选项卡。
   - （选项）若需指定 LDAP 搜索 URL 以确定成员资格，可单击“仅电子邮件成员资格的动态标准”字段下方的“添加”按钮，然后在“添加动态标准”窗口中做下列操作：
   - 在该字段中输入 LDAP 搜索 URL 或单击“构建”按钮打开“构建 LDAP 搜索 URL”窗口，此窗口是帮助您构建搜索 URL 的模板窗口。
   - 单击“确定”将条目添加到“仅电子邮件成员资格的动态标准”字段，并关闭“添加动态标准”窗口。

   有关创建 LDAP 搜索 URL 的说明，请参阅第 451 页“定义动态成员资格标准”。
4. （选项）若需在邮件发送列表中添加单个成员，可单击“仅电子邮件成员资格成员”字段下方的“添加”按钮，然后在“添加仅电子邮件成员”窗口中做下列操作：
   - 在该字段中输入新成员的主地址。主地址必须是符合 RFC 821 规定的格式正确的 SMTP 地址。不应输入备用地址，特别是当为该组指定权限之时。每次打开该窗口时只能添加一个新成员，该字段只能容纳一个地址。
   - 单击“确定”将用户添加到列表成员中。并关闭“添加仅电子邮件成员”窗口。若需输入另一个地址，再次单击“添加”按钮即可重新打开“添加仅电子邮件成员”窗口。
5. 如果已经完成对该邮件发送列表的所有修改，则可单击“编辑条目”窗口底部的“确定”按钮。否则，单击其他选项卡继续进行修改。

定义邮件在发送上的限制

您可在送往邮件发送列表的邮件上施加各种限制。您可定义允许发送邮件之人的集合体，可要求对发件人实行认证，可限制投寄邮件的来源，并可对投寄邮件的大小进行限制。不符合限制规定的邮件将被拒收。

备注 虽然这些限制对组来说在控制到访邮件的某些方面很有用，但这些限制并不以提供高度安全的访问控制为目的。

若需定义组级的邮件投寄限制，请按下列步骤操作：

1. 在 Console 中，按照第 447 页“访问邮件发送列表”中的说明访问“创建组”或“编辑条目”窗口。
2. 单击“邮件”选项卡。
3. 单击“限制”选项卡。
4. （选项）从下列选项中选择允许的发件人：
   - **任何人：**对发件人没有限制。（此为默认值）注意，选择此选项后就不能选择下一步中说明的 SMTP 认证。
   - **邮件发送列表中的任何人：**只有邮件发送列表成员 （包含不是仅电子邮件成员的组成员）能够发送邮件。
   - **以下列表中的任何人：**只有明确列示在以下字段中的用户才能够发送邮件。

   如果选择了 “以下列表中的任何人”选项，添加发件人时，可单击 “允许的发件人”字段下方的 “添加”按钮，或单击 “搜索”打开 “搜索用户和组”窗口。若单击 “添加”按钮，则打开 “添加允许的发件人”窗口。在该字段中输入允许的发件人的电子邮件地址或判别名 （DN） 。单击 “确定”以将发件人添加到 “允许的发件人”字段，并关闭 “添加允许的发件人”窗口。对所有想添加的其他的允许发件人重复此步骤。

   有关 “搜索用户和组”窗口的使用说明，请见 **Managing Servers with Netscape Console**。
5. （选项）定义允许的发件人域，即限制能够发送邮件的发件人域：
   - 单击 “允许的发件人域”字段下方的 “添加”按钮。
   - 在 “添加允许的发件人域”窗口中输入一个域名，然后单击 “确定”将该域添加到列表中。

   请注意，域自动包含所有的子域。例如， `siroe.com` 包含 `sales.siroe.com`。
6. （选项）定义邮件的最大允许篇幅。

   输入大小 （以字节为单位）。
7. 如果已经完成对该邮件发送列表的所有修改，则可单击 “编辑条目”窗口底部的 “确定”按钮。否则，单击其他选项卡继续进行修改。

定义中介人

可为邮件发送列表添加一个或多个中介人。

当某一中介人 （分检员）收到转发的邮件时，他 （她）将决定如何处理该邮件。（在有多个中介人的情况下，对邮件的处理是由第一个中介人所采用的操作决定的）。所谓处理可能包括核准邮件并将其发回到列表 （也许须用口令）或删除该邮件。

在定义邮件发送列表的中介人时，请按下列步骤操作：

1. 在 Console 中，按照第 447 页“访问邮件发送列表”中的说明访问“创建组”或“编辑条目”窗口。
2. 单击“邮件”选项卡。
3. 单击“中介人”选项卡。
4. 单击“中介人列表”字段下方的“添加”按钮。
5. 在“添加中介人”窗口的字段中输入中介人的主电子邮件地址或判别名（DN）。既可直接输入地址，也可单击“搜索”，用“搜索用户和组”窗口查找地址。请注意，每次打开“添加中介人”窗口时只能添加一个中介人。

   有关“搜索用户和组”窗口的使用说明，请见 **Managing Servers with Netscape Console**。
6. 单击“确定”以将中介人添加到“中介人列表”字段，并关闭“添加中介人”窗口。（若需输入另一个地址，须再次单击“添加”按钮以重新打开“添加中介人”窗口。
7. 如果已经完成对该邮件发送列表的所有修改，则可单击“编辑条目”窗口底部的“确定”按钮。否则，单击其他选项卡继续进行修改。

词汇表

A 记录 一种 DNS 记录类型，其中包含主机名及与之相关联的 IP 地址。互联网上的 Messaging Servers 是用这种 A 记录对电子邮件的路由进行管理的。*还可参见* **域名系统（DNS）、MX 记录**。

Administration Server 管理员 即使在无 Directory Server 连接的情况下，也能通过其管理权限启动或停止服务器的用户。对本地服务器组中所有服务器而言， Administration Server 管理员只承担有限的服务器方面的任务 （通常只有重新启动服务器和停止服务器两项任务)。
当 Administration Server 安装好后，该管理员条目会自动在本地创建（该管理员不是用户目录中的用户）。

Allow 过滤器 Messaging Server 的一项访问控制规则，可标识出允许访问下列一个或多个服务项的客户机：POP、 IMAP 或 HTTP。另请参见 **Deny 过滤器**。

APOP 经认证的邮局协议类似于邮局协议 （POP），但不是用明文口令进行的认证，而是用经编码的口令加上 challenge string 进行的认证。

AUTH 一 SMTP 命令，可使 SMTP 客户机向服务器指定认证方法、实施认证协议交换，必要时可为随后的协议交互协商安全层。

base DN 目录中的判别名条目，搜索可从该条目开始，因此也被称为搜索基。
例如， `ou=people`、 `o=siroe.com`。

Berkeley DB 一种事项处理数据库，可用于高并行性读写工作负荷及需要事项处理和恢复性能的应用程序。 iPlanet Messaging Server 出于多种目的而使用 Berkeley 数据库。

bind DN 执行某项操作时用于认证到 Directory Server 的判别名。

CA 证书管理机构发行数字证书（电子验证）的机构，其公共密钥可在较广的范围内为预定的接受单位所使用。

CLI 请参见**命令行界面**。

cn 普通名称的 LDAP 别名。

CNAME 记录 一种把域名的别名映射到域名的 DNS 记录类型。

config 配置一词的英文缩写。

Console （控制台） 一种图形用户界面 （GUI） ，用户可通过该界面对多种 iPlanet 组件进行配置、监控、维护和故障排除。

cookie　纯文本字符串。当访问特定的服务器站点时，它能自动输入到浏览器的存储器中。Cookies 由网页作者进行编程。用户可以接受或拒绝 cookie。接受 cookie 可使网页较快地载入， cookie 对计算机的安全没有威胁。

CRAM-MD5　RFC 2195 文献提供的一种轻型标准跟踪认证机制。当只有用户的登录口令需要保护而防止网上窃贼盗用时，这种机制提供了一种快速的（尽管安全性较弱）认证方法，用以代替 TLS (SSL)。

cronjob　仅限 UNIX 使用。cron 守护程序在配置时间内自动执行的一项任务。另请参阅 **crontab 文件**。

crontab 文件　仅限 UNIX 使用。一个命令列表，每行一条命令，能在给定的时间里自动执行。

DC 树　域组件树。镜像反映 DNS 网络语法的目录信息树。例如，域组件（DC）树的判别名可为 `cn=billbob， dc=bridge， dc=net， o=internet`。

Delegated Administrator Console（代理管理器控制台）　一个基于 web 浏览器的软件控制台。域管理员可用来向托管域添加或更改用户，终端用户也可用来更改口令、设置邮件转发规则、设置休假规则、及列示邮件列表项目。

Delegated Administrator for Messaging and Collaboration。即邮件传输和协作代理管理程序，这是一套界面（GUI 和实用程序），域管理员可用来向托管域添加或更改用户和组。

deliver　见**邮件传递**。

Deny 过滤器　Massaging Server 的一种访问控制规则，它能标识出那些被拒绝访问下列服务的用户：POP、IMAP 或 HTTP。另请参见 **Allow 过滤器**。

DIGEST-MD5　一种比 CRAM-MD5 更安全的轻型标准跟踪认证机制。已列入 RFC 2831 文献，这种认证机制可在不需要 TLS (SSL) 那种系统设置开销的情况下为保护整体网络提供了一种选择方案。

Directory Server　基于 LDAP 的 iPlanet 目录服务。还可参见**目录服务**、**轻型目录访问协议（LDAP）**、**配置目录服务器**，**用户 / 组目录服务器**。

Dispatcher　为指定的 TCP 端口处理连接请求的 MTA 组件。Dispatcher 是多线程连接调度代理程序，可使多个多线程服务器共同负责一项特定的服务。使用 Dispatcher 时，可以有几个多线程 SMTP 服务器进程并行运行。

DIT　请参阅**目录信息树**。

DN　请参见**判别名**。

dn　LDAP 判别名的别名。还可参见**判别名**。

DNS　请参见**域名系统**。

DNS 别名　主机名，DNS 服务器将之识别为指向不同的主机。计算机只有一个实名，但可以有一个或多个别名。例如， `www.siroe.domain` 可能是一个指向实名为 `realthing.siroe.domain` 主机的别名，服务器当前即存在于该主机中。

DNS 数据库　域名（主机名）及其相应的 IP 地址的数据库。

DNS 域 主机名后缀相同的一组计算机，该后缀即域名。在语法上讲， Internet 域名由被英文句号（点）分隔的名称（标签）序列构成。例如， `corp.mktng.siroe.com`。另见**域**。

DNS 电子欺骗 攻击网络的一种形式，它使服务器被扰乱并提供虚假信息。

DSN 请参阅 **传递状态通知**。

dsservd 守护程序，可访问存有目录信息的数据库文件并可通过 LDAP 协议与目录客户程序通信。

dssetup Directory Server 准备工具，可用来使现有的 Directory Server 做好准备，供 iPlanet Messaging Server 使用。

EHLO 命令 一条 SMTP 命令，用于对某服务器进行查询，以确认该服务器是否支持扩展的 SMTP 命令。 RFC 1869 对其有所定义。

ESMTP 请参阅**扩展的简单邮件传输协议**。

ESP 企业服务供应商 （Enterprise Service Provider）。

ETRN SMTP 命令。当邮件队列中的邮件正在服务器中等待客户机处理时，该 SMTP 命令可使客户机请求服务器启动对其邮件队列的处理。定义见 RFC 1985。

EXPN 用于扩展邮件发送列表的 SMTP 命令。定义见 RFC 821。

FQDN 请参阅**全限定域名**。

GUI 图形用户界面。

HA 请参见**高可用性**。

hashdir 命令行实用程序，用以确定哪个目录应包含特定用户的文件存储库。

HTTP 请参见**超文本传输协议**。

IDENT 请参阅**标识协议**。

IMAP4 参见 **Internet 邮件访问协议第 4 版**。

imsadmin 命令 用于管理域管理员、用户和组的一系列命令行实用程序。

imsimta 命令 为邮件传输代理 （MTA）实施各种维护、测试和管理任务的一系列命令行实用程序。

INBOX（收件箱） 为用户的默认邮箱保留的名称，用于传递邮件。 INBOX 是唯一对大小写不敏感的文件夹名。例如：INBOX、 Inbox 和 inbox 都是用户默认邮箱的有效名称。

instance_root 参见**实例目录**。

Internet （互联网） 这个名称特指使用 TCP/IP 协议的全球网。

Internet 邮件访问协议第 4 版 （IMAP4） 一标准通信协议，允许用户与主邮件系统断开连接后仍能处理邮件。IMAP 规范考虑到了这些断开连接用户的管理控制和一旦重新连接到邮件系统时用户邮件存储库的同步性。

Internet 协议 （IP） 基本网络层协议，是互联网和企业内部网的基础。

IP 请参见 **Internet 协议**。

IP 地址 由圆点分隔的一列数字，如 `198.93.93.10`，用于指定企业内部网或互联网上计算机的实际位置，是分配给使用 TCP/IP 协议主机的 32 位地址。

iPlanet Setup	用于所有 iPlanet 服务器和 iPlanet Console 的安装程序。
ISP	Internet 服务提供商向客户提供互联网服务的公司，提供的服务项包括电子邮件、电子日历、接入万维网和站点托管等。
LDAP	请参阅**轻型目录访问协议**。
LDAP 数据交换格式（LDIF）	以文本形式显示目录服务器条目的一种格式。
LDAP 过滤器	一种基于当前特定属性或属性值来指定一系列条目的方法。
LDAP 转荐对象	一个 LDAP 条目，由符号链接（转荐对象）组成，可连接到另一个 LDAP 条目。LDAP 转荐对象由 LDAP 主机和判别名构成。LDAP 转荐对象通常用于引用现有的 LDAP 数据，以避免复制这些数据。也用于保持程序的兼容性，即那些依赖于特定条目（可能已被移动者）的程序的兼容性。
LDAP 搜索串	含有可替换参数的字符串，用于定义目录搜索项的属性。例如， LDAP 搜索串“uid=%s”表示该搜索项乃基于用户的 ID 属性。
LDAP 服务器	软件服务器，用于维护 LDAP 目录并提供目录查询服务。 iPlanet 目录服务就是通过 LDAP 服务器实现的各项服务。
LDAP 备用服务器转换	LDAP 服务器的一种备份功能。如果某一 LDAP 服务器发生故障，系统可转换到另外一部 LDAP 服务器。
LDBM	LDAP 数据库管理程序。
LDIF	请参阅 **LDAP 数据交换格式**。
Legato Networker	由 Legato® 发行的第三方备份实用软件。
MD5	RSA Data Security 使用的邮件摘要算法。MD5 可用于生成一个短而独特的、有很高概率的数据摘要。从数学角度讲，要生成一段数据，并据此产生相同的电子邮件摘要，是十分困难的。
Messaging Multiplexor（邮件多路复用器）	一种专用的 iPlanet Messaging Server，是多个邮件服务器的单一连接点，可便于将大量用户分布到多个邮箱主机。
Messenger Express	Messenger Express 是一种邮件客户程序。使用时，用户可通过浏览器式（HTTP）的界面访问邮箱。邮件、文件夹和其他邮箱信息均在一个浏览器窗口中以 HTML 显示。还可参见 **webmail**。
Messenger Express Multiplexor	起 Multiplexor 作用的代理传报服务器；用户可通过该服务器连接到 iPlanet Messaging Server（Messenger Express）的 HTTP 服务。 Messenger Express Multiplexor 可便于多服务器机器上的邮件用户分配操作。
MHS	请参阅**邮件处理系统**。
MIME	请参阅**多用途 Internet 邮件扩充**。
MMP	请参阅 **Messaging Multiplexor**。
MTA	请参见**邮件传输代理**。

MTA 配置文件 包含 Messaging Server 所有通道定义以及重写规则的文件（imta.cnf），可用来确定如何重写待转发邮件的地址。还可参见**通道**、**重写规则**。

MTA 目录高速缓存 MTA 处理邮件时所需的关于用户目录服务信息的快照。还可参见**目录同步**。

MTA 转发 将邮件从一个 MTA 经路由选择发送到另一个 MTA 的操作。

MUA 请参见**用户代理**。

Multiplexor 请参见 **Messaging Multiplexor（邮件多路转发器）**。

MX 记录 邮件交换记录。可将主机名映射到另一部主机的 DNS 记录类型。

NDN 请参见**未送达通知**。

NMS Netscape Messaging Server。

OSI 树 一种映射“开放系统互连”（OSI）网络语法的目录信息树。 OSI 树中的判别名例子可为：cn=billt、 o=bridge、 c=us。

POP3 请参阅**邮局协议第 3 版**。

postmaster 帐户 电子邮件组或一系列电子邮件地址的别名，它们从 Messaging Server 接收系统生成的邮件。 postmaster 帐户必须指向有效的一个或多个邮箱。

RC2 RSA Data Security 使用的一种大小可变的密钥块密码。

RC4 RSA Data Security 使用的一种流密码。比 RC2 更快。

RDN 相对判别名的英文缩写。某条目的原状在附加到字串以形成全判别名之前的实际名称。

RFC 请求评论。一组文档系列，始于 1969 年，描述 Internet 协议组及相关实验。不是所有的（实际上只有很少一点）RFC 都描述 Internet 标准，但所有的 Internet 标准都作为 RFC 发表。请参见 http://www.imc.org/rfcs.html。

SASL 请参阅**简单认证与安全层**。

SCM 请参阅 **Service Control Manager**。

sendmail UNIX 机器上使用的普通 MTA。在大多数应用程序中， iPlanet Messaging Server 都能顺便用做 sendmail 的替代。

server_root 服务器目录中安装有与指定主机上指定的 Administration Server 相关联的所有 iPlanet 服务器。其典型的目录名是 *server-root*。另请参见**安装目录**、**实例目录**。

Service Control Manager Windows NT 的服务管理程序。

servlet 网络服务器运行的服务器端 Java 程序，应客户机的请求生成相应的内容。Servlet 程序与小应用程序（applet）的相似之处在于二者都在服务器端运行，但无需使用用户界面。

Sieve 一种邮件过滤语言的建议标准。

SIMS Sun Internet Mail Server。

SIZE 一种 SMTP 扩展，可使客户机向服务器声明某特定邮件的大小。服务器将向客户机说明是否愿意接收基于所称邮件大小之邮件；服务器还可向客户机声明可以接受的邮件篇幅的最大值。定义见 RFC 1870。

SMTP　请参阅**简单邮件传输协议**。

SMTP AUTH　请参阅 **AUTH**。

sn　姓氏的别名目录属性。

SSL　请参阅**安全套接层**。

SSR　请参阅**服务器端规则**。

TCP　请参阅**传输控制协议**。

TCP/IP　请参阅**传输控制协议 /Internet 协议**。

TLS　请参阅**传输层安全性**。

UA　请参阅**用户代理**。

UBE　请参阅**大宗商业电子邮件**。

UID　(1) 用户标识。便于系统识别用户的独特字符串，也指用户 ID。(2) 用户 ID（登录名）别名的目录属性。

UUCP　UUCP 复制程序。

/var/mail　一个名称，通常用于指 Berkeley 式样的收件箱。在这种收件箱中，新邮件按顺序存储在一个纯文本文件中。

Veritas 集群服务器　Veritas Software 公司的高可用性群集软件，iPlanet Messaging Server 可将其集成使用。

VRFY　检验用户名的 SMTP 命令。定义见 RFC 821。

webmail　浏览器式邮件服务的通用词。基于浏览器的客户机（称为“瘦型”客户机，因为多数处理量由服务器端完成）所访问的邮件总是存储在服务器上。还可参见 **Messenger Express**。

Web 服务器　可提供访问万维网功能的软件程序或服务器。Web 服务器用于接收用户的请求，检索用户请求的文件或应用程序，并发送出错信息。

X.400　一种邮件处理系统标准。

访问控制　当外界请求访问服务器或服务器上的文件夹和文件时，系统对这些访问请求所实行的一种控制方法。

访问控制信息　访问控制列表中的单一信息项，英文缩写为 ACI。

访问控制列表　（ACL）与目录相关联的一组数据，用于定义用户和 （或）组访问该目录的权限。

访问控制规则　用以为给定的目录条目集或属性指定用户权限的规则。

访问域　在一个特定域内，限制其对某些 Messaging Server 操作的访问。例如，通过访问域可以限制从何处收取发往某帐户的邮件。

帐户　定义一个特定用户或用户组的信息。信息包括用户名或组名、有效的电子邮件地址（一个或多个）以及电子邮件的传递方法和传递位址。

地址　电子邮件中确定邮件如何传递，传递到何处的信息。在邮件头和信封中都能找到地址。其中，信封地址将确定邮件的路由及传递方式，而邮件头地址则仅起显示作用。

地址处理 MTA 执行的各项操作，其中包括探测地址中的错误，必要时重写地址，及将地址与收件人匹配。

地址协议 使电子邮件能够顺利传递而制定的寻址规则。RFC 882 是互联网上使用最广泛的协议，也是 iPlanet Messaging Server 所支持的协议。其它协议包括 X.400 和 UUCP（UUCP 复制协议）。

地址标号 重写规则模式的地址元素。

管理域 一种管理控制区域。另请参阅**域**。

管理控制台 请参阅 **Console** 。

管理权限 定义用户管理角色的一系列权限。

管理员 具有一系列指定管理权限的用户。还可参见**配置管理员**、**目录管理者**、**Administration Server 管理员**、**服务器管理员**、**邮件存储库管理员**、**最高层管理员**、**域管理员**、**机构管理员**、**家庭群组管理员**、**邮件列表所有者**。

别名 电子邮件地址的备用名。

别名文件 一个可用来设置别名的文件，用于在目录中设置那些没有设置的别名，如 postmaster 别名。

备用地址 一个帐户的第二地址，通常为主地址的变异。在某些情况下，多个地址会给单一帐户带来方便。

认证 （1）向 iPlanet Messaging Server 证明客户机用户身份的过程。（2）向客户机或其它服务器证明 iPlanet Messaging Server 身份的过程。

认证证书 从服务器发送到客户机或从客户机发送到服务器的数字文件，用以确认和认证对方。该证书可确保其持有者 （客户机或服务器）的真实性。证书不可转让。

自动回复选项文件 一个用于设置自动回复选项 （如休假通知）的文件。

自动回复实用程序 一种实用程序，当自动回复功能启用后，可对发送到帐户的邮件自动应答。iPlanet Messaging Server 中的每个帐户都能通过配置而对来件进行自动回复。

主干 分布式系统的主要连接机制。所有与主干上的中间系统相连的系统都彼此相连，但这并不妨碍由于成本、性能或安全原因而建立绕过主干的系统。

后端服务器 一种电子邮件服务器，其唯一的作用是储存和检索电子邮件。亦称邮件存储服务器。

备份 把文件夹内容从邮件存储库备份到备份设备的过程。还可参见**恢复**。

标志 当客户机首次连接到某项服务 （如 IMAP）上时，系统显示的文字串。

正文 电子邮件的一部分。虽然邮件头和信封必须遵从标准格式，但邮件正文的内容则完全由发件人决定。正文可包括文本，图形，甚至多媒体。结构化的正文遵守 MIME 标准。

容量 提供给客户机的字符串，用来定义特定 IMAP 服务项中的可用功能。

证书管理机构 请参阅 **CA**。

基于证书的认证 通过客户提交的数字证书对用户进行的识别。还可参见**口令认证**。

证书数据库 包含某服务器数字证书的文件，也叫证书文件。

证书名 可用来识别证书及其所有者的名称。

通道 处理邮件的基本 MTA 组件。通道表示与另一个计算机系统或一组系统的连接。每条通道由一个或多个通道程序和外发邮件队列组成，这些存储在队列中的邮件将被指定发送到一个或多个与通道相连接的系统。另请参见**通道块**、**通道主表**、**通道程序**。

通道块 一个单一通道定义。还可参见**通道主表**。

通道主表 通道定义的集合体。

通道程序 通道的一部分，可执行下列功能：（1）向远程系统传输邮件并在发送后将邮件从队列中删除。（2）接受远程系统发来的邮件并将邮件排在适当的通道队列中。还可参见**主通道程序**、**从属通道程序。**

密码 加密所使用的算法。

密文 已加密的文本。相对于**明码文本**。

客户 （机、程序） 向服务器请求服务或信息的一种软件实体。

明码文本 未加密的文本

客户机服务器模型 联网计算机向其他客户机提供特定服务的一种计算模型。例如 DNS 中的名称服务器 / 名称解读器的范型，以及如 NFS 与无磁盘主机之间的那种文件服务器 / 文件客户关系。

注释字符 一个字符，当放在行的开头时可把该行转化成不可执行的注释行。

配置管理员 在整体 iPlanet 拓扑中，对服务器和配置目录数据具有管理权限的人。配置管理员可不受限制地访问 iPlanet 拓扑中的所有资源。他 （她）是唯一能给其他管理员指定服务器访问权限的管理员。在管理员组及其成员就位之前，配置管理员负责掌管初期的管理配置工作。

配置目录服务器 一个为服务器或服务器组维护配置信息的目录服务器。

配置文件 一个包含 iPlanet Messaging 系统特定组件配置参数的文件。

拥塞阈值 一种可由系统管理员设置的磁盘空间限制，当系统资源不足时，通过限制新的操作以防止数据库超载。

守护程序 一个在后台运行、独立于终端、并可在需要时随时实施其功能的 UNIX 程序。守护程序（daemon）的常见例子有邮件处理程序、许可证服务器和打印守护程序等。在装有 Windows NT 的计算机上，这类程序被称为一项服务。还可参见**服务**。

数据存储 包含目录信息 （通常为整个目录信息树）的存储库。

拆分邮件重新整合 多用途 Internet 邮件扩充 （MIME）的功能，通过该协议可把分割成许多小邮件 （碎片）的大邮件进行重新组装。出现在每个碎片中的“邮件部分内容类型”报头段含有有助于重新将碎片组装成一个完整邮件的信息。还可参见**邮件拆分**。

Delegated Administrator for Messaging（邮件代理管理器）。一系列界面（GUI 和 CLI），域管理员可通过这些界面在一托管域中添加和更改用户或用户组。

代理管理服务器（delegated administrator server） 一种守护程序，可通过托管域对目录访问实行控制。

删除邮件 标记待删除邮件的一种操作。在用户进行专门的擦除或清除操作之前，已删除邮件不会从邮件存储库中去除。还可参见**清除邮件**、**擦除邮件**。

传递 请参见**邮件传递**。

传递状态通知 传达邮件传递状态信息的消息。例如，一则表示邮件因网络故障而被延迟传递的消息。

抑制服务型攻击 一种因超量邮件而造成的人为的或意外的邮件服务器失效状态。此状态下服务器吞吐量会受到明显的影响或使服务器本身因超负荷而不能工作。

间接引用别名 在绑定操作或搜索操作中所指定的、由目录服务器把一个判别名的别名翻译成条目的实际判别名之操作。

目录上下文 在目录树信息中对条目进行搜索的起始点，这些条目可用来认证访问存储库的用户和口令。还可参见 **base DN**。

目录条目 由判别名标识的一系列目录属性和它们的值。每个条目都包含一个对象类属性，用于指定条目记述的对象种类，并用于定义该对象种类所包含的一系列属性。

目录信息树 树状的层次结构，即目录条目的编织结构，亦称 DIT。 DIT 能在 DNS（DC 树）或开放系统互连网络 （OSI 树）中编织。

目录查找 为获取给定用户或资源的信息而进行的基于用户名、资源名或其它特征的目录搜索过程。

目录管理者（Directory Manager） 有权管理目录服务器数据库的用户。访问控制不适用于这种用户 （可把目录管理者看作目录的超级用户）。

目录体制 目录体制乃是一系列规则，用于定义哪些数据可以存储到目录。

目录服务 以逻辑方式集中起来的机构人员和资源信息档案库。还可参见**轻型目录访问协议**。

目录同步 用目录服务储存中的当前目录信息更新 MTA 目录高速缓存的过程，即同步过程。另请参见 **MTA 目录高速缓存**。

脱机状态 邮件客户连接到服务器并将所选邮件复制到高速缓存后，与服务器断开连接之状态。

判别名 以逗号分隔的属性和值的序列，用于指定条目在目录信息树中的独特位置，常简写为 DN。

分配表 见**邮件发送列表**。

分配表所有者 见**邮件发送列表所有者**。

文档根目录 服务器上的目录，其中包含文件、图象和数据，当用户访问 iPlanet Web Server 时可向其显示。

域管理员 有管理权限的用户，可通过 Delegated Administrator for Messaging and Collaboration 程序的 GUI 或 CLI 在托管域中建立、更改和删除邮件用户、邮件发送列表和家庭帐户。系统的默认设置是：这个用户可扮演拓扑中所有邮件服务器的邮件存储管理员。

域 单一计算机系统控制下的资源。另请参见**管理域、 DNS 域、托管域、虚拟域**。

域别名 指向另一个域的域条目。通过使用别名，托管域可以有几个域名。

域托管 在一个共享邮件服务器上托管一个或多个域的能力。例如，域 siroe.com 和 sesta.org 两个域能一起在 siroe.net 邮件服务器上托管。用户向托管域发送并从那里接收电子邮件，但邮件服务器名并不出现在电子邮件地址中。

域名 （1）电子邮件地址中使用的主机名。（2）定义管理组织的独特名称。一个域可以包含其它域。域名从右到左解释。例如，siroe.com 既是 Siroe 公司的域名又是最高层域 com 的一个子域。域 siroe.com 可以进一步分成子域，比如 corp.siroe.com 等。还可参见**主机名、全限定域名**。

域名系统（DNS） 分布式名称分析软件，可使计算机通过域名在网络或 Internet 上确定别的计算机的位置。该系统可将主机名与标准 IP 地址相关联。（如 www.siroe.com）。在正常情况下，计算机从 DNS 服务器获得这一信息。在将主机名翻译成 Internet 地址时，DNS 服务器可提供分布式的、重复的数据查询服务。还可参见 **A 记录**、**MX 记录**、**CNAME 记录**。

域组织 组织树中托管域下面的子域。对于希望依据部门的隶属关系组织用户和用户组条目的公司来说，域组织非常有用。

域名部分 电子邮件地址中 @ 符号右边的部分。例如， siroe.com 是电子邮件地址 dan@siroe.com 的域名部分。

域空间配额 由系统管理员配置的、分配给电子邮件域的空间大小。

域重写规则 请参见**重写规则**。

域模板 重写规则的一部分，定义怎样重写地址的主机 / 域部分。可包括一个完全静态的主机 / 域地址，或单一字段的置换字串，或者二者兼有。

动态组 由 LDAP 搜索 URL 定义的邮件组。用户一般须先在目录条目中设置一个 LDAP 属性，然后便可加入动态组。

加密 伪装信息之过程，使之不能被任何人解密，有代码密钥的预定收件人除外。

企业网 由在广泛地理区域上分布的相互连接的网络集体构成的网络。企业网服务于分布范围很广的公司业务活动，通常为公司的关键性任务应用程序所用。

信封 传输关于电子邮件发送人和收件人信息的容器。该则信息不是邮件标头的一部分。各种电子邮件程序都使用信封在各地点之间移动或传输邮件。用户只能看到标头和邮件正文。

信封字段 一个命名的信息项，如邮件信封中的 RCPT TO。

命令行界面 可从命令行执行的命令。亦称实用程序。

错误处理程序 可处理错误的程序。在 Messaging Server 中，该程序可发布错误讯息，并在 postmaster 填写好错误操作表格后对之进行处理。

错误处理操作表格 发送给 postmaster 帐户的表格，伴随有收到但 Messaging Server 不能处理的邮件。Postmaster 须填写这个表格并指示服务器怎么处理这封邮件。

错误讯息 报告错误或其它情况的讯息。iPlanet Messaging Server 在许多情况下都会生成这样的讯息，特别是在收到不能处理的邮件的时候。其他讯息（被称为通知错误）则仅供有关人员参考。

扩展器 电子邮件传递系统的一部分，可将一封电子邮件传递到一系列地址。邮件扩展器用于实现邮件发送列表。用户只需将邮件发送到单一地址（如 `hacks@somehost.edu`），然后由邮件扩展程序负责传递到列表中的有关邮箱。亦称为邮件爆发器（mail exploders）。还可参见 **EXPN**。

扩展 该术语用于邮件发送列表的 MTA 处理。一项转换操作，可将发送到邮件发送列表地址的邮件转换成足够多的副本，以分配给邮件发送列表中的每个成员。

擦除邮件 一项删除操作，可标记出待删除的邮件，然后从 INBOX（收件箱）中永久地去除这些邮件。还可参见**删除邮件**、**清除邮件**。

扩展的简单邮件传输协议（ESMTP） Internet 的一种邮件传输协议。为了增加功能， ESMTP 可将选项命令添加到 SMTP 命令集中，其中包括可使 ESMTP 服务器能够发现远程站点执行了哪些命令等这样的功能。

企业外部网（extranet） 公司内部网中客户和厂商可以访问的那一部分。另请参见**企业内部网（intranet）**。

工具程序 Messaging Server 日志文件条目中的一个标志，用以表示生成该日志条目的软件子系统（比如 Network 或 Account）。

备用系统转换 某项计算机服务从一个系统到另一个系统的自动转移，以提供冗余备份。

家庭群组管理员 在家庭群组中具有添加和去除家庭成员管理权限的用户。该用户可将家庭群组管理访问权授与组中别的成员。

防火墙 一种网络配置，通常既有硬件又有软件；防火墙可在某组织机构内的联网计算机和外部计算机之间形成一个屏障。防火墙通常用来保护信息，如网络上的电子邮件、讨论组、建筑物或组织站点中的数据文件等。

文件夹 邮件集的名称。文件夹内可以包含另外的文件夹，也叫邮箱。另请参见**个人文件夹**、**共享文件夹**， **INBOX**。

转发 请参阅 **邮件转发**。

邮件拆分 多用途 Internet 邮件扩充（MIME）功能，可以把大邮件拆分成若干个小邮件。参阅**拆分邮件重新整合**。

全限定域名（FQDN） 标识特定 Internet 主机的独特名称。还可参见**域名**。

网关 网关和应用网关这两个术语指的是可将一个本地格式翻译成另一格式的系统。例如，X.400 to/from RFC 822 电子邮件网关。网关实际上是一台连接两个或更多的电子邮件系统（特别是两个不同网络上的不相似邮件系统）、并在其间转移邮件的机器。有时映射和翻译可能很复杂，通常需要一种存储 - 转发方案，通过这种方案电子邮件就可从一个系统在完全被接收后，经过适当的翻译再传输给下一个系统。

问候表格 帐户建立后发给用户的电子邮件。这种表格可用来确认新帐户并检查其内容。

组 判别名下排列的一组 LDAP 邮件条目。通常用作邮件发送列表，但也可用来向组内成员赋予一定的管理权限。另请参见**动态组**、**静态组**。

组文件夹 包括共享文件夹和组文件夹的文件夹。另请参阅**共享文件夹**。

邮件头 电子邮件中先于邮件正文的部分。邮件头由字段名、紧跟其后的冒号及其值所构成。邮件头中所含的信息对电子邮件程序和试图阅读电子邮件的用户非常有用。例如，邮件头中包括传递信息、内容概要、追踪和 MIME 信息；邮件头可标示邮件发给谁、谁发的、什么时候发的以及主题是什么等信息。邮件头必须按照 RFC 822 格式写，以使邮件程序能够读取。

邮件头字段 一个命名的信息项，比如邮件头中的发件人：（`From:`）或收件人：（`To:`）。常被称作“标题行”。

高可用性 在系统或进程出现故障时，能够检测到服务中断情况并提供恢复机制之能力。另外，在主系统出现故障的情况下，可使备份系统接管服务。

转发 两台计算机之间的一种传输。

主机 驻留有一部或多部服务器的计算机。

托管域 外包给 ISP 提供的电子邮件域，即由 ISP 向一组织机构提供电子邮件域托管服务，从而可为该组织操作和维护电子邮件服务。一个托管域通常与其它托管域共享一个 Messaging Server 主机。在早期的基于 LDAP 的电子邮件系统中，一个域曾由一个或多个电子邮件服务器主机支持。使用 Messaging Server 后，很多域就可以同在一台服务器上由互联网服务供应商托管。每个托管域都有一个 LDAP 条目，用于指向该域的用户和组集装箱。托管域也叫做虚拟托管域或虚拟域。另请参见**域**、**虚拟域**。

主机名 一个网域内的某个特定的计算机的名称。主机名称就是 IP 主机名，可为一种“短格式”主机名 （例如， mail）或全限定主机名。全限定主机名由两部分组成：主机名和域名。例如，`mail.siroe.com` 是域 `siroe.com` 中的计算机 `mail`。网域中的主机名必须非常独特。只要计算机驻留在不同的子域中，您所在组织机构就可以有多个名叫 `mail` 的计算机；例如，`mail.corp.siroe.com` 和 `mail.field.siroe.com`。主机名总是映射到特定的 IP 地址。另请参见**域名**、**全限定域名**、 **IP 地址**。

主机名隐藏 一种措施，可使基于域的电子邮件地址不包含特定的内部主机名。

集线器 一部主机，起着系统单一联络点的作用。例如，当两个网被防火墙隔开的时候，防火墙使用的计算机就经常起着邮件集线器的作用。

超文本传输协议 用于在 Web 上传输超文本文档的标准协议。 iPlanet Messaging Server 可提供 HTTP 服务，支持基于 Web 的电子邮件。请参阅 **Messenger Express**。

标识协议 一种协议，可提供确定远程进程标识的手段，该远程进程代表一个特定 TCP 连接的远程终端。见 RFC 1413 中的定义。

安装目录 安装有服务器二进制 （可执行）文件的目录。对 Messaging Server 来说，安装目录是服务器根目录的子目录：*server-root*`/bin/msg/`。另请参见**实例目录**、**服务器根目录**。

实例 服务器或其它软件一种配置，可在给定的主机上分别执行。即使只安装了一套二进制文件集，也可建立彼此独立运行和存取的 iPlanet 服务器的多个实例。

实例目录 该目录中的文件可用来定义服务器的特定实例。对 Messaging Server 而言，该目录是服务器根目录 *server_root*`/msg-`*instance*`/` 的子目录，这里的 *Instance* 是安装中指定的服务器名。另请参见**安装目录**、**服务器根目录**。

互联网协议地址 请参阅 **IP 地址**。

企业内部网 （intranet） 公司或组织机构内的 TCP/IP 网络。借助于企业内部网，公司能把万维网上同类型的服务器和客户软件应用于分布在公司局域网上的内部应用程序。企业内部网上与互联网通信的敏感信息通常由防火墙保护。另请参见**防火墙、企业外部网 （extranet）**。

无效用户 邮件处理过程中出现的一种错误情形。当出现这种情况时，邮件存储库将向 MTA 发送一条信息，并删除邮件存储库内的邮件副本。 MTA 随后将邮件退回给发件人，并删除 MTA 内的邮件副本。

任务控制器 负责应其他各种 MTA 组件的请求而调度和执行任务 MTA 组件。

密钥数据库 一个包含服务器证书密钥对的文件。也叫密钥文件。

知识信息 目录服务基础信息的一部分。目录服务器用知识信息向其他服务器传递信息请求。

级别 日志详细程度的一个标志，用以表示须记录在日志文件里的事件类型的相对数目。例如，对于 Emergency 级别，很少有事件被记入日志；反之对于 Informational 级别，则有很多事件被记入日志。

轻型目录访问协议 （LDAP） 目录服务协议，可在 TCP/IP 和多种平台上运行。是 X.500 目录访问协议（DAP）的简化版本，允许在单一的点上管理存储、检索和信息分配，其中包括用户目录文件、邮件发送列表和 iPlanet 服务器上的配置数据。 iPlanet Directory Server 使用 LDAP 协议。

监听端口 服务器端口，用于与客户机和其他服务器通信联系。

本地部分 电子邮件地址中识别收件人的部分。还可参见**域部分**。

日志目录 保存服务项所有日志文件的目录。

日志失效 当日志文件达到其最大允许时间时将其从日志目录中删除。

日志轮换 创建新的日志文件以取代当前日志文件。随后记录的所有事件都将写入这个新的当前文件中。以前的当前日志文件不再写入，但仍保留在日志目录中。

查找 同搜索，用特定参数对数据进行的排序。

邮箱 存储和查看邮件的处所。另请参阅**文件夹**。

邮件客户程序 帮助用户发送和接收电子邮件的程序。这是各种网络程序和邮件程序中用户接触最多的部分。邮件客户程序可用来撰写邮件和提交需传递的邮件，检查新来件，接收和整理来件。

邮件交换记录 请参阅 **MX 记录**。

邮件交换记录 请参阅 **MX 记录**。

邮件列表 亦称邮件发送列表，一种电子邮件地址列表，可通过列表上的地址向其发送电子邮件。

邮件列表所有者 具有在邮件发送列表中添加和删除成员的管理权限的用户。

邮件分程转发 邮件服务器从 MUA 或 MTA 收到邮件后将邮件**分程转发到**收**件人邮件**存储**库或另一部路由器之过程**。

邮件路由器 见**邮件分程转发**。

管理对象 可配置属性的集合体，例如目录服务的属性集合体。

主通道程序 一种通道程序，通常为向远程系统传输信息的发起者。另请参见**从属通道程序**。

主目录服务器 包含待复制数据的目录服务器 （Directory Server）。

成员 一个用户或用户组，可接收定址到**邮件发送列表**的电子邮件副本。还可参见**邮件发送列表**、**扩展**、**中介人**、**所有者**。

邮件 电子邮件的基本单位，邮件由一个标题和一段正文组成，在由发件人传输到收件人的过程中通常被包含在一个信封中。

邮件访问服务 支持客户机访问 Messaging Server 邮件存储库的协议服务器、软件驱动程序和程序库。

邮件传递 当 MTA 将邮件传递到本地收件人 （邮件文件夹或程序）时所发生的操作。

邮件转发 当 MTA 将传递到一个特定帐户的邮件发送到由帐户属性指定的一个或多个新目的地时所发生的操作。转发功能可由用户配置。还可参见**邮件传递**、**邮件路由选择**。

邮件处理系统 （MHS） 一组互连的 MTA、其代理服务器和邮件存储库。

邮件路由选择 当第一个 MTA 确定收件人不是本地用户但可能存在于其他某个地方时，将邮件从一个 MTA 传到另一个 MTA 的操作。路由选择通常只能由网络管理员配置。还可参见**邮件转发**。

邮件队列 一种邮件目录，从客户和其他邮件服务器接收到的电子邮件在该目录中被排成队列等待（立即或延迟）传递。

邮件空间配额 空间配额限度，定义了特定文件夹能够耗用的磁盘空间容量。

邮件存储库 存储有 Messaging server 实例的所有于本地传递的邮件数据库。邮件可存储在单个物理磁盘上或跨越存储在多个物理磁盘上。

邮件存储库管理员 拥有 Messaging Server 邮件存储库管理权限的用户。该用户可以查看和监控邮箱，并指定存储库的访问控制。该用户可通过代理认证权运行某些管理存储库的实用软件。

邮件存储库分区 驻留在单一物理文件系统分区上的邮件存储库或其子集。

邮件提交 客户机的用户代理 （UA）将邮件传输给邮件服务器并请求传递之过程。

邮件传送代理 （MTA） 邮件路由选择和传递作业使用的的专用程序。几个 MTA 可合作传输邮件并将邮件传递给预定的收件人。 MTA 需确定邮件是传递到本地邮件存储库，还是通过路由选择远程传递到另一个 MTA。

邮件服务器管理员 该管理员的权限包括安装和管理 iPlanet Messaging Server 实例。

中介人 在实现下列操作之前，首先收到所有发送到邮件发送列表之电子邮件的人，然后由其：（A）将电子邮件转发到邮件发送列表；（B）编辑电子邮件然后转发到邮件发送列表；或 （C）不转发到邮件发送列表。另请参见**邮件发送列表**、**扩展**和**成员**。

多用途 Internet 邮件扩充（MIME） 一种通信协议，通过在邮件中附加多媒体文件而在电子邮件中包含多媒体协议

名字转换 将 IP 地址映射到相应名称的过程。还可参见 **DNS**。

域名空间 LDAP 目录的树结构。还可参见**目录信息树**。

属性 以成对是属性值显示的 LDAP 数据。任何与描述性属性相关的具体信息。另请参见**允许使用的属性**、**所需属性**。

允许使用的属性 可在使用特定对象类的条目中选用的属性，但不要求一定要有。另见**属性、必需属性**。

必需属性 在使用特定对象类的条目中必须具备的属性。另见**允许使用的属性、属性**。

命名属性 目录信息树判别名中的最终属性。还可参见**相对判别名**。

命名上下文 通过其 DN 识别的目录信息树的某个特定后缀。在 iPlanet Directory Server 中，特定类型的目录信息存储在命名上下文中。例如，存储 Siroe 公司驻波士顿办事处的营销人员的所有条目的命名上下文可以叫做 `ou=mktg`、 `ou=Boston`、 `o=siroe`、 `c=US`。

网管程序 一种能够读、格式化和显示 SNMP 数据的程序。亦称 SNMP 客户程序。

再转发列表 一个相邻系统的表列，邮件路由用它来决定邮件传输到何处。再转发列表中的系统顺序决定邮件路由传输到相应系统的顺序。

节点 DIT 中的一个条目。

未送达通知 在信息传输过程中，如果 MTA 不能在地址模式和重写规则之间找到匹配项， MTA 就会将未送达报告连同原邮件一起发还给发件人。

公证邮件 遵守 RFC 1892 NOTARY 规范的未送达通知 （NDN）和传递状态通知 （DSN）。

通知邮件 由 Messaging Server 发送的一种邮件，可提供邮件传输处理状态，并对任何传递方面的问题和失败原因给以说明。这种邮件只供参考之用，并不要求 postmaster 采取任何行动。另参见**传递状态通知**。

类路径 运行 servlet 引擎和 servlet 模板所需的目录和 `.jar` 文件的路径。

对象类 一种模板，用以确定条目所描述之对象的类型及其所包含的属性集。例如， iPlanet Directory Server 确定的 `emailPerson` 对象类可具有如下属性: `commonname`、`mail`（电子邮件地址）、 `mailHost` 和 `mailQuota`。

脱机状态 邮件客户程序将邮件从服务器系统下载到客户系统以便进行查看和回复的一种状态。邮件可以从服务器上删除，也可以不删除。

联机状态 邮件可保存在服务器并由邮件客户远程响应的一种状态。

组织机构管理员 一个有下列管理权限的用户：通过 Delegated Administrator for Messaging and Collaboration 程序的 GUI 或 CLI 创建、更改和删除所在组织机构或子组织内的邮件用户和邮件列表。

分区 请参见**邮件存储库分区。**

口令认证 通过用户名和口令识别用户。另参见**基于证书的认证**。

模式 用于匹配目的的字符串表达式，比如在 Allow 和 Deny 过滤器中。

永久性失败 一种在邮件处理过程中发生的错误情形。当发生这种情形时，邮件存储库将删除库内的电子邮件副本。 MTA 将邮件退回发件人，并删除邮件副本。

个人文件夹 只供其所有者阅读的文件夹。还可参见**共享文件夹**。

纯文本 指传输数据的一种方法。其定义依上下文而定。例如，使用 SSL 时，纯文本口令将被加密，因此，不会作为明码发送。使用 SASL 时，纯文本口令将被散列，仅有口令的散列码作为文本发送。还可参见 **SSL** 和 **SASL**。

纯文本认证 请参阅**口令认证**。

端口号 用于指定主机上一个单独的 TCP/IP 应用程序的数字，并可提供传输数据的目的地。

邮局协议第 3 版（POP3） 提供标准传递方法的协议，该通信协议不要求有邮件传输代理即可访问用户邮件文件夹。在网络环境中这是一种优势，因为在联网环境中，邮件客户机和邮件传输代理常在不同的计算机上。

进程 由操作系统设置的、独立且功能齐全的执行环境。每一个应用程序实例都在分开的进程中运行。另参见**线程**。

协议 就两个或更多系统之间的信息交换，而对待交换的邮件所做的正规描述和须遵守的规则。

目录条目配置 在 iPlanet Directory Server 中添加、更改和删除条目的过程。这些条目包含用户、用户组以及网域信息。

代理 一系统作为另一系统的“代办”以响应协议请求的一种机制。代理系统用于网络管理中，可以避免在简单设备（如调制解调器）中执行全部协议栈。

公共密钥加密法 一种加密方法，所用密钥（代码）由公共和专用组件两部分组成。对邮件加密时，该方法使用公开的收件人公共密钥。解密时，收件人使用只有自己知道的不公开的专用密钥。

清除邮件 指永久性地去除邮件的过程，即那些已被删除、在用户和组文件夹中不再引用的邮件，并把空间还给邮件存储文件系统。还可参见**删除邮件**、**擦除邮件**。

队列 请参阅**邮件队列**。

转荐对象 目录服务器将信息请求返还给客户（提交请求者）的过程，返回的信息中包括客户应通过请求与之联系的目录服务代理（DSA）方面的信息。还可参见**知识信息**。

正则表达式 一种文字串，使用特殊的字符表示用于模式匹配的字符的范围或类型。

相对判别名 参见 **RDN**。

分程转发 将邮件从一个 Messaging Server 传到另一个 Messaging Server 的过程。

复制目录服务器 收到所有或部分数据之副本的目录。

恢复 将文件夹的内容从一个备份设备恢复到邮件存储库的过程。还可参见**备份**。

反 DNS 查找 查询 DNS 之过程，以将数字 IP 地址转换成相等的全限定域名。

重写规则 亦称域重写规则。 MTA 用来把邮件通过路由选择传输到正确的主机以便传送的一种工具。重写规则具有下列功能：（1）从来件地址摘出主机 / 域的规范说明；（2）以重写规则模式匹配主机 / 域的规范说明；（3）基于域模板重写主机 / 域的规范说明；（4）确定邮件的排列通道。

根条目 目录信息树（DIT）层次结构中的最高层条目。

路由器 路由器系统决定沿哪条网络路径分配信息量。路由器可通过路由选择协议获得网络的信息，并可根据几个叫做“路由矩阵”的标准使用一些算法来选择最佳路由。在 OSI 术语中，路由器是指网络层的中间系统。还可参见**网关**。

路由选择 请参阅**邮件路由选择**。

安全文件系统 一种文件记录系统，其记录方式如下：如果一系统毁损，安全文件系统可将数据反转到毁损前状态并恢复所有数据。安全文件系统典型示例是 Veritas 文件系统， VxFS。

方案 在 iPlanet Directory Server 中能够作为条目存储的信息类型的结构和语法的定义。当与方案不匹配的信息存储在目录中时，客户在试图访问目录时可能不能显示出恰当的结果。

搜索基 请参阅 **base DN**。

安全套接层 （SSL） 用于在双方 （客户机和服务器）之间建立安全连接的软件库。

安全模块数据库 一种文件，所含信息描述了 SSL 密码的硬件加速器情况。也叫做 `secmod`。

服务器管理员 执行服务器管理任务的人。服务器管理员依据任务 ACI 为特定服务器中的任务提供有限制的访问。配置管理员须指定用户对服务器的访问权限。一旦用户得到对服务器的访问许可，该用户就成了服务器管理员，并能向其他用户提供服务器访问权限。

服务器实例 代表特定服务器安装情况的目录、程序和实用程序。

服务器端规则 （SSR） 启用服务器端邮件过滤功能的一系列规则。基于邮件过滤器语言 Sieve。

服务 （1）服务器提供的一项功能。例如，iPlanet Messaging Server 提供的 SMTP、POP、IMAP 和 HTTP 服务。（2） Windows NT 上的一种后台进程，但没有用户界面。Windows NT 平台上的 iPlanet 服务器是作为一种服务而运行的。相当于**守护程序**。

会话 （期） 客户机 - 服务器连接的实例

共享文件夹 可由多人阅读的文件夹。共享文件夹的所有者能够指定文件夹的阅读访问权，并指定谁能从共享文件夹中删除邮件。共享文件夹的中介人能编辑、阻塞或转发来件。只有 IMAP 文件夹能共享。另请参见**个人文件夹**。

简单认证与安全层 （SASL） 控制机制的一种手段， POP、 IMAP 或 SMTP 的客户机可通过这一机制向服务器标识自己。 iPlanet Messaging Server 对 SMTP SASL 用途的支持功能符合 RFC 2554 （ESMTP AUTH）。 SASL 定义于 RFC 2222。

简单邮件传输协议 （SMTP） Internet 最常使用的电子邮件协议，也是 iPlanet Messaging Server 支持的协议之一。定义见 RFC 821，相关的邮件格式描述见 RFC 822。

单字段置换串 重写规则中的域模板部分，可动态地重写主机/域地址的特定地址标号。还可参见**域模板**。

单次登录 用户经一次认证即可访问多种服务 （邮件、目录、文件服务等）的能力。

从属通道程序 通道程序，可接收远程系统启动的传递。还可参见**主通道程序**。

智能型主机 指域中的一种邮件服务器，在其他邮件服务器不能辩识收件人时，即把邮件转发给该服务器。

电子欺骗 侵入网络的一种形式，其做法是试图以伪装的主机名访问服务器，或发送邮件给服务器。

静态组 通过列举每一个组成员而静态定义的邮件组。另请参阅**动态组**。

子域 域的一部分。例如，在域名 `corp.siroe.com` 中，`corp` 是 `siroe.com` 域的子域。还可参见**主机名、全限定域名**。

子网 IP 地址的一部分，可识别主机 ID 的信息块。

从属引用 命名上下文，即由 Directory Server 持有的命名上下文的产物。另请参阅**知识信息**。

同步 （1）由主机 Directory Server 实施的到备份 Directory Server 的数据更新。（2）MTA 目录高速缓存的更新。

线程 进程中的轻型执行实例。

最高层管理员 一个具有在整个邮件服务器域名空间中创建、更改、删除邮件用户、邮件发送列表、家庭帐户和域的管理权的用户。该管理员通过使用 Delegated Administrator for Messaging and Collaboration 程序的 GUI 或 CLI 实施这些管理操作。在默认情况下，该用户可以充当拓扑中所有 Messaging Server 的邮件存储库管理员。

瞬时失败 发生在邮件处理过程中的一种错误情形。邮件在传递时，远程 MTA 不能予以处理，但是过一会也许又能处理。本地 MTA 会把邮件退还到队列并重新安排，以便稍后再次传输。

传输控制协议 （TCP） Internet 协议序列中的基本传输协议，可在两个主机间提供可靠的、面向连接的信息流服务。

传输控制协议 /Internet 协议 （TCP/IP） Internet 协议序列使用的网络协议集的总称。该名称指网络协议序列的两个基本协议：TCP （传输控制协议），一种传输层协议和 IP （Internet 协议），一种网络层协议。

传输层安全性 （TLS） SSL 的标准格式。还可参见**安全套接层**。

传输协议 提供 MTA 之间的邮件传输。例如 SMTP 和 X.400。

一体化通信 使用单一邮件存储库提供电子邮件、声音邮件、传真以及其他形式通讯服务的概念。iPlanet Messaging Server 是全套一体化通信解决方案的基础。

大宗商业电子邮件 （UBE） 常常因商业目的而由大宗发行人发送的没要求也不需要的电子邮件。

上端引用 表示目录信息树 （DIT）中您所在 Directory Server 命名上下文之上的、持有命名上下文之 Directory Server。

用户帐户 可以访问服务器的帐户，在 Directory Server 中作为一个条目而保存。

用户代理 （UA） 客户机 （程序）组件 （如 Netscape Communicator），用户可用来创建、发送和接收邮件。

用户 / 用户组 Directory Server 在一个组织机构中保存用户和组信息的 Directory Server。

用户条目或用户目录文件 描述每一用户信息的字段，有些是必须输入的项目，有些是选项；例如：判别名、全名、标题、电话号码、传呼机号码、登录名、口令、主目录等。

用户文件夹 用户的电子邮件信箱

用户空间配额 由系统管理员配置的分配给用户的电子邮件空间限额。

自订域 与个人用户 （而不是特定的服务器或托管域）相关连的一种域名。自订域是通过 `MailAlternateAddress` 属性指定的。自订域的域名没有 LDAP 条目。自订域对于个人和小型组织很有用处，特别是希望自订域名，而又没有行政主管支持其自己的托管域的用户。自订域也叫做自定义域。

虚拟域 (1) 由 ISP 托管的域。(2) Messaging Multiplexor 在客户机的用户 ID 中添加的域名，用于 LDAP 搜索和登录到邮箱服务器。另请参见**域**、**托管域**。

通配符 搜索字符串中的特殊字符，表示有一个或更多其他字符或字符范围。

工作组 本地工作组环境，服务器在本地办公室或工作组范围内执行自己的路由选择和传递操作。部门间的邮件则通过路由选择传递到主干服务器。还可参见**主干**。

索引

符号

数字

A

B

C

D

E

F

G

J

L

M

N

O

P

Q

R

S

T

U

V

W

X