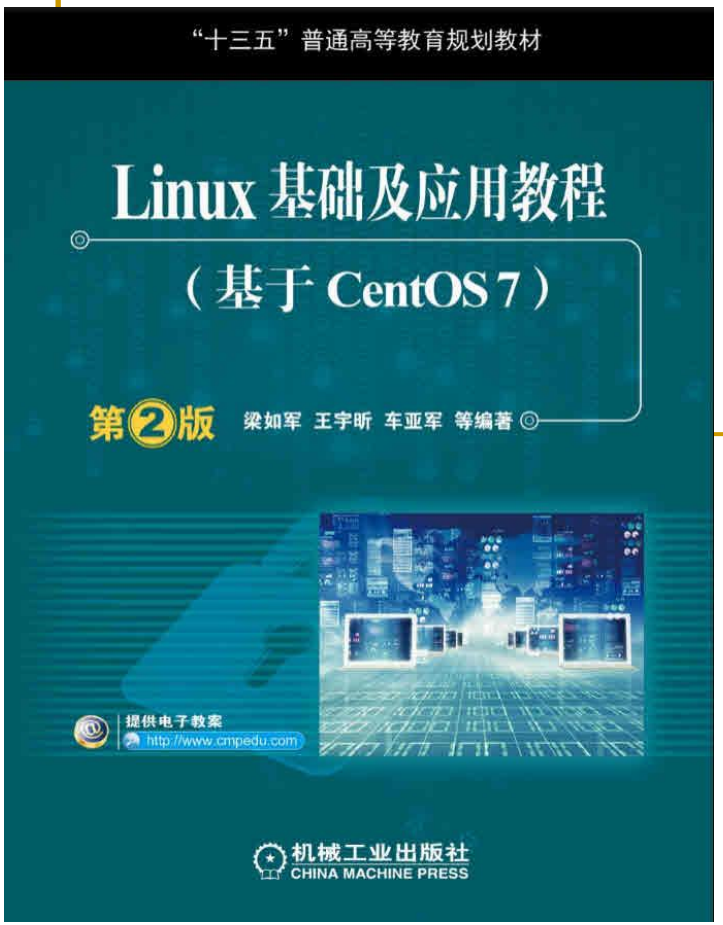


第16章 E-mail服务

主讲人： 梁如军

2015-05-05

本章内容要点

- 电子邮件系统的组成及相关协议
- 邮件消息的传输流程
- Postfix的体系结构及工作流程
- Postfix的安装和配置
- Dovecot的安装和配置
- SASL与TLS

梁如军（linuxbooks@126.com）

本章学习目标

- 理解电子邮件系统的组成
- 熟悉电子邮件相关协议
- 熟悉Postfix的体系结构及功能实现
- 掌握邮件消息的传输流程
- 熟悉Postfix映射表的功能及类型
- 学会配置和使用access/aliases/virtual映射表
- 掌握Postfix UCE控制的基本配置方法
- 学会安装和配置Dovecot
- 学会配置带有SMTP认证的MTA
- 学会配置带有SSL/TLS支持的邮件服务

梁如军（linuxbooks@126.com）

CentOS
The Community ENTerprise Operating System

邮件系统与邮件协议

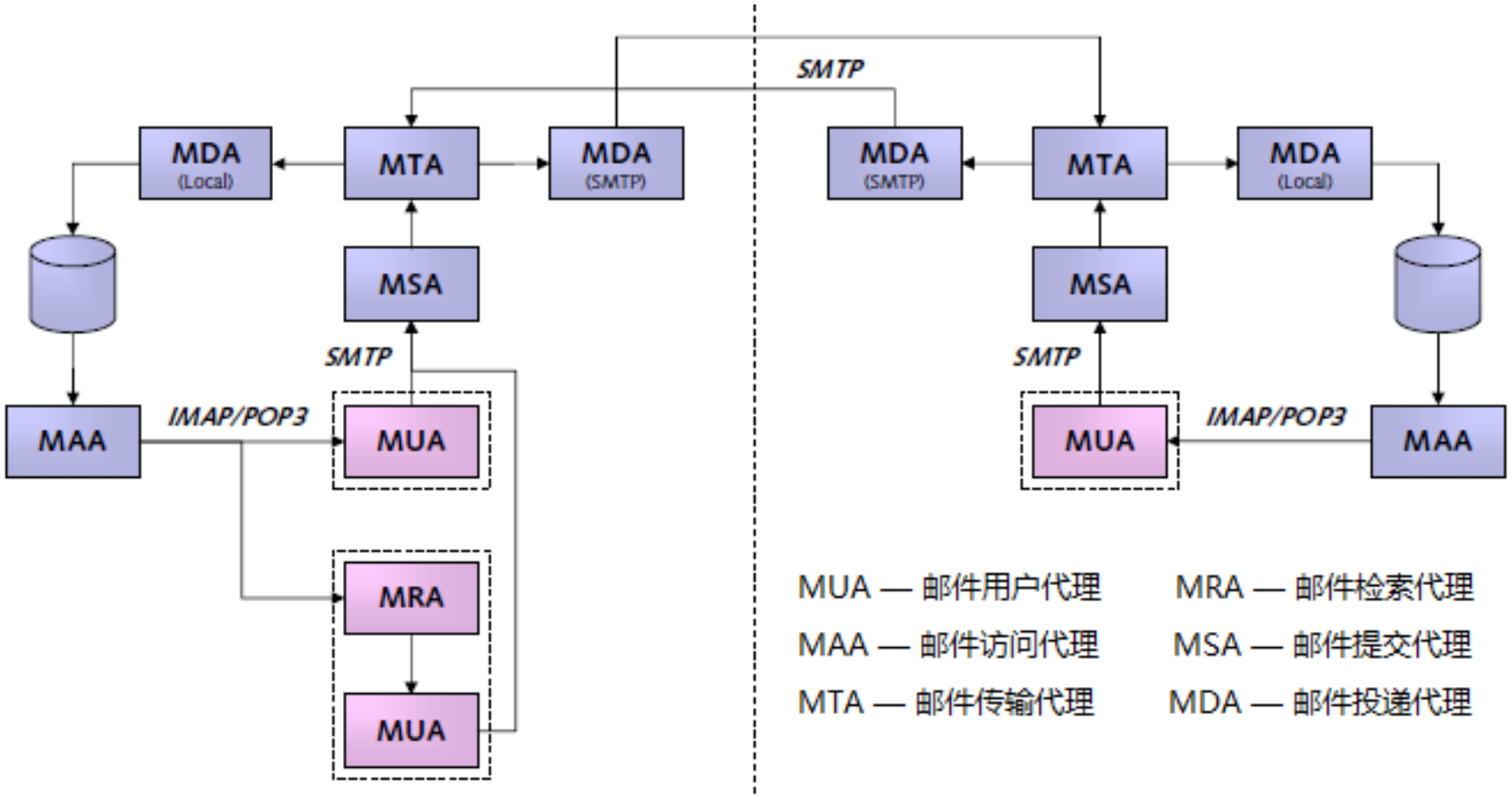
梁如军（linuxbooks@126.com）

邮件系统与邮件协议

- 电子邮件系统的组成
- 邮件消息的传输流程
- 电子邮件相关协议

梁如军（linuxbooks@126.com）

电子邮件系统组成



梁如军（linuxbooks@126.com）

MUA（邮件用户代理）

- Mail User Agent
  - 提供发送和接收电子邮件的用户接口
    - 使用SMTP协议向MTA发送邮件
    - 读取由MDA递送的或由MRA检索的邮件
  - 提供给用户方便的阅读和撰写邮件的编辑环境
- Examples
  - **Mozilla Thunderbird**
  - **Microsoft Outlook Express**
  - **Foxmail**
  - **DreamMail**

MRA（邮件检索代理）

- Mail Retrieval Agent
  - MRA从MAA检索或获取邮件
  - 与MDA协同工作将邮件投递到本地或远程的邮箱（MailBox）
  - 为MUA读取邮件做好准备
- Examples
  - 独立的应用程序：如 **fetchmail**和 **getmail**
  - 构建到MUA中，如在Mozilla Thunderbird中整合的MSA功能

梁如军（linuxbooks@126.com）

MAA（邮件访问代理）

- Mail Access Agent
  - 将用户连接到系统邮件库，为MUA提供用户认证
  - 为MUA使用POP或IMAP协议从用户邮箱读取邮件做好准备
- Examples
  - **Dovecot**
  - **Cyrus-IMAP**
  - **Courier-IMAP**
  - **UW-IMAP**

梁如军（linuxbooks@126.com）

MSA（邮件提交代理）

- Mail Submission Agent
  - 接受来自 MUA 的邮件
  - 负责消息由MTA发送之前必须完成的所有准备工作和错误检测
- Examples
  - Postfix 的 **postdrop+pickup**
  - Sendmail 的 **sendmail-msa**

MTA（邮件传输代理）

- Mail Transfer Agent
  - 根据邮件的目标地址进行入站路由
  - 管理邮件队列将接收到的邮件进行缓冲
  - 决定将邮件发往不同的MDA，还可能会改变邮件路由
- Examples
  - Postfix **cleanup+qmgr+trivial-rewrite**
  - **Sendmail**

梁如军（linuxbooks@126.com）

MDA（邮件投递代理）

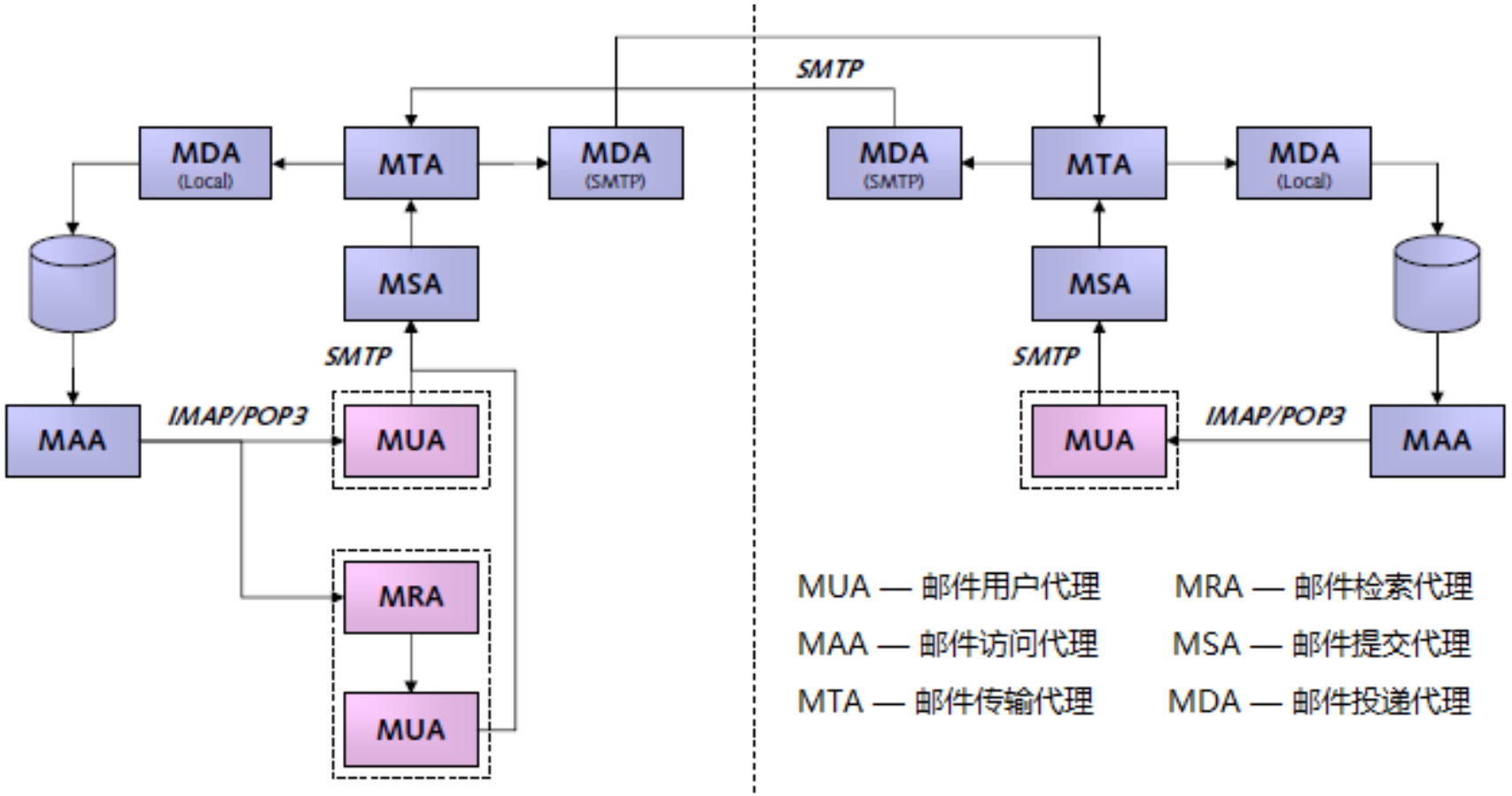
- Mail Delivery Agent
  - 从MTA接收邮件
  - 投递邮件到本地邮箱、邮件列表、文件或程序
  - 投递邮件到其他的MTA
- Examples
  - Postfix 的**local**, **smtp**, **pipe**
  - Sendmail本身包含了MDA的功能

梁如军（linuxbooks@126.com）

LDA（本地投递代理）

- Local Delivery Agent
  - 当接收者的地址与本地主机一致时，负责投递的MDA也称本地投递代理（LDA）
  - LDA是MDA的特例
- Examples
  - **procmail**（www.procmail.org）
  - **maildrop**（http://www.courier-mta.org/maildrop/）
  - **Sieve**（http://wiki.dovecot.org/LDA/Sieve）
  - Sendmail 提供的 **mail.local** 和 **smrsh**

邮件消息的传输流程



梁如军（linuxbooks@126.com）

邮件消息的传输流程（1）

1.撰写新邮件

- 使用MUA撰写邮件
- 将撰写的邮件提交给MSA

2.MSA接受邮件消息

- MSA 验证用户
- MSA允许授权用户提交邮件消息
- MSA 根据需要重写消息头
- MSA 将消息提交给MTA
- MSA 向MUA发送成功报告

3.MTA接受邮件消息

- MTA检查邮件的发送者和接收者是否有效以及是否被允许
- MTA检查邮件内容是否有效以及是否被允许
- MTA可能会运行邮件内容过滤
- MTA根据需要重写消息头
- MTA根据邮件头决定提交给哪个MDA（smtp，local 等）
- MTA 提交给适当的MDA
- 若提交失败，MTA将其放入适当的邮件队列以便稍后重新提交

梁如军（linuxbooks@126.com）

邮件消息的传输流程（2）

4.MDA接受邮件消息

- MDA 使用SMTP协议发送邮件到远程MTA，实现邮件中继（Relay）

5.远程MTA接受邮件消息

- 操作流程与3.相同
- 邮件消息提交给LDA

6.LDA接受邮件消息

- LDA 可能会执行邮件过滤规则
- LDA 将邮件消息投递到本地用户邮箱

7.MAA 检测新邮件消息

- MAA 接受MUA的用户认证授权
- MUA 通过MAA索取邮件消息

8.阅读邮件消息

- MUA 将邮件消息展示给用户

梁如军（linuxbooks@126.com）

电子邮件相关协议
——简单邮件传输协议（SMTP）

- Simple Message Transfer Protocol
  - 默认端口：25（TCP）
  - Text-based 协议，RFC2821
  - 定义了SMTP命令
  - 无加密（No encryption）
  - 无认证（No authentication）
- 用于
  - 发送邮件的MUA与MTA建立连接并发送邮件
  - MTA之间也使用STMP进行电子邮件的转发

梁如军（linuxbooks@126.com）

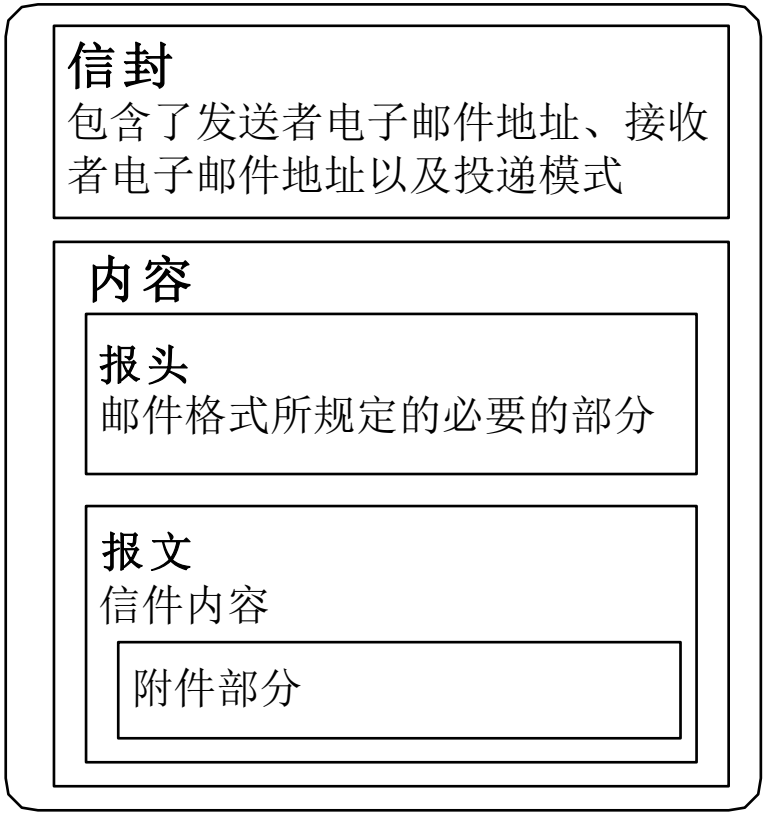
电子邮件相关协议——扩展的SMTP协议（ESMTP）

- Extended SMTP
  - RFC1869、RFC1870、RFC1891和RFC1985
  - 提供了如身份认证和传输加密等功能

梁如军（linuxbooks@126.com）

电子邮件格式及标准

- RFC2822/RFC822
- MIME
  - RFC2045、RFC2046
  - RFC2047、RFC4288
  - RFC4289、RFC2049



梁如军（linuxbooks@126.com）

电子邮件相关协议
—多用途互联网邮件扩展（MIME）

- Multipurpose Internet Mail Extension
  - 提供了一个扩展的邮件格式标准，使消息在不同的邮件系统内进行交换
  - MIME的主要功能
    - 支持除了ASCII之外的字符集文本
    - 支持非ASCII字符集的头信息
    - 支持多种类型的非文本（图象、声音、视频及应用程序）附件
  - 复合消息体包含多个部分
    - 复合消息的目录信头设有分界标志
    - 分界标志出现在各部之间以及消息体的开始和结束处
    - 分界标志绝不可出现在消息的其它位置

梁如军（linuxbooks@126.com）

电子邮件相关协议
——邮局协议（POP）

- Post Office Protocol
  - RFC1939（默认端口：110）
  - 所有数据（包括密码）都被明文传输
  - 功能
    - 检测用户的登录名和口令
    - 下载服务器上的邮件到本地硬盘（同时删除保存在邮件服务器上的邮件），用户可以在本机上进行离线邮件阅读，用户不必长时间地与邮件服务器连接
  - 当前使用的POP协议的版本是POP3
  - 可以通过TCP:995端口传递POP3的基于SSL的加密数据（POPS）

梁如军（linuxbooks@126.com）

POP的缺点和IMAP引入

- 用户几乎没有对邮件接收的控制决定权
  - 在整个收信过程中，用户无法知道邮件的具体信息，只有全部收入硬盘后，才能慢慢浏览和删除
  - 一旦碰上邮箱被轰炸，或有比较大的邮件，用户不能通过分析邮件的内容及发信人地址来决定是否下载或删除，从而造成系统资源的浪费
- IMAP协议可以克服POP协议的缺陷，同时提供更强大的功能

梁如军（linuxbooks@126.com）

电子邮件相关协议——互联网邮件存取协议（IMAP）

- Internet Message Access Protocol
  - RFC2060（默认端口：143）
  - 所有数据（包括密码）都被明文传输
  - 功能
    - 实现了POP协议的功能
    - 在线从远程邮件服务器上获取E-mail信息
    - 提供了如何远程维护服务器上的邮箱的功能
    - 具有高性能和可扩展性的优点
  - 当前使用的IMAP协议的版本是IMAP4
  - 可以通过TCP:993端口传递IMAP4的基于SSL的加密数据（IMAPS）

梁如军（linuxbooks@126.com）

IMAP提供三种操作模式

- 在线方式
  - 邮件保留在服务器端，客户端可以对其进行管理
  - 使用方式与WebMail相类似
- 离线方式
  - 邮件保留在服务器端，客户端可以对其进行管理
  - 与POP协议一样
- 分离方式
  - 邮件的一部分在服务器端，一部分在客户端
  - 与一些成熟的组件包应用（如LotusNotes/Domino）的方式类似

梁如军（linuxbooks@126.com）

POSTFIX及其工作原理

梁如军（linuxbooks@126.com）

Postfix及其工作原理

- Postfix简介
- Postfix的体系结构
  - 多进程协同工作
  - 邮件队列及其管理器
- Postfix邮件传输流程
- Postfix的MTA功能实现

梁如军（linuxbooks@126.com）

Postfix起源

- Wietse Zweitze Venema 博士到IBM公司的T. J. Watson研究中心做学术休假的1998年时
- 启动了Postfix项目：“设计一个可以取代Sendmail的软件，可以为网站管理员提供一个更快速、 更安全、而且完全兼容于Sendmail的邮件服务器软件！”
- Postfix项目一直由IBM资助并成为开源的自由软件项目，其主站在 http://www.postfix.org

梁如军（linuxbooks@126.com）

Postfix的设计目标

- **高性能：** Postfix要比同类的服务器产品速度快三倍以上
- **兼容性：** 保持与Sendmail的兼容性
- **健壮性：** 在过量负载情况下仍然保证程序的可靠性
- **灵活性：** Postfix结构上由十多个小的子模块组成，每个子模块完成特定的任务
- **安全性：** Postfix使用多层防护措施防范攻击者来保护本地系统
- **开放性：** 遵从IBM的开放源代码版权许可证

梁如军（linuxbooks@126.com）

Postfix的特点

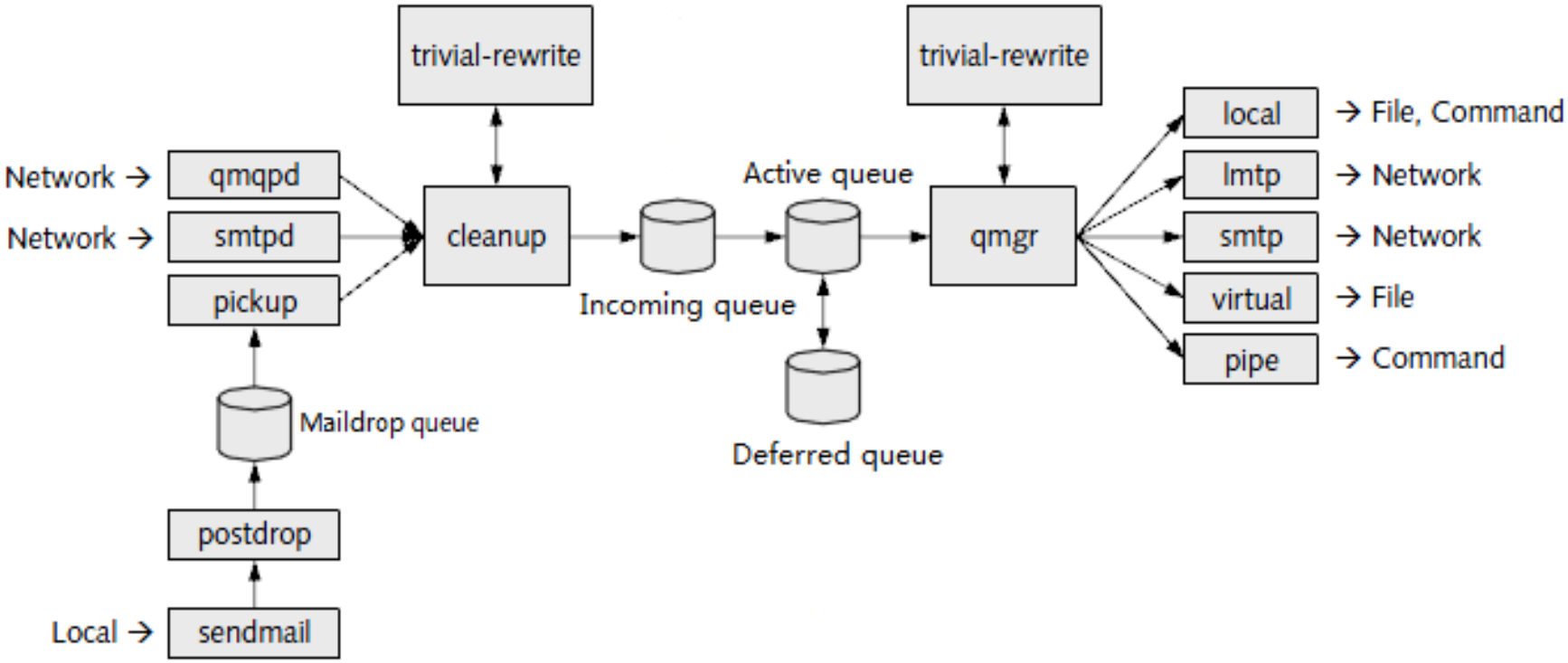
- 配置简单
- 虚拟域支持
- UCE（Unsolicited Commercial Email）控制
  - 黑名单列表、RBL查找、HELO/发送者DNS核实
  - 邮件头和邮件内容过滤
- 表查询
  - 使用一种扩展的表查询来实现地址重写功能
- 跨平台
  - Postfix 可以运行在类UNIX平台上（AIX、Solaris、HP-UX、IRIX、Linux、FreeBSD、MacOS X）

梁如军（linuxbooks@126.com）

Postfix在邮件系统中的角色

- Postfix在邮件系统中担任MTA的角色
- Postfix负责在服务器之间传递邮件，并收下其他系统寄到本地系统的邮件
- Postfix**不处理**任何POP或IMAP通信内容

Postfix的体系结构



梁如军（linuxbooks@126.com）

Postfix的多进程协作

- 基于模块化的互操作的多进程体系结构设计
- 每个独立的进程完成不同的任务，这些独立的进程称为组件（component）
- Postfix的组件之间没有任何特定的进程衍生关系（父子关系）
- 优点
  - 具有更好的隔离性
  - 便于审计和排错
  - 减少进程创建开销

梁如军（linuxbooks@126.com）

Postfix协同工作的组件

- pickup
- smtpd
- qmqpd
- cleanup
- qmgr
- trivial-rewrite
- local
- lmtp
- smtp
- virtual
- pipe

梁如军（linuxbooks@126.com）

Postfix组件的运行方式

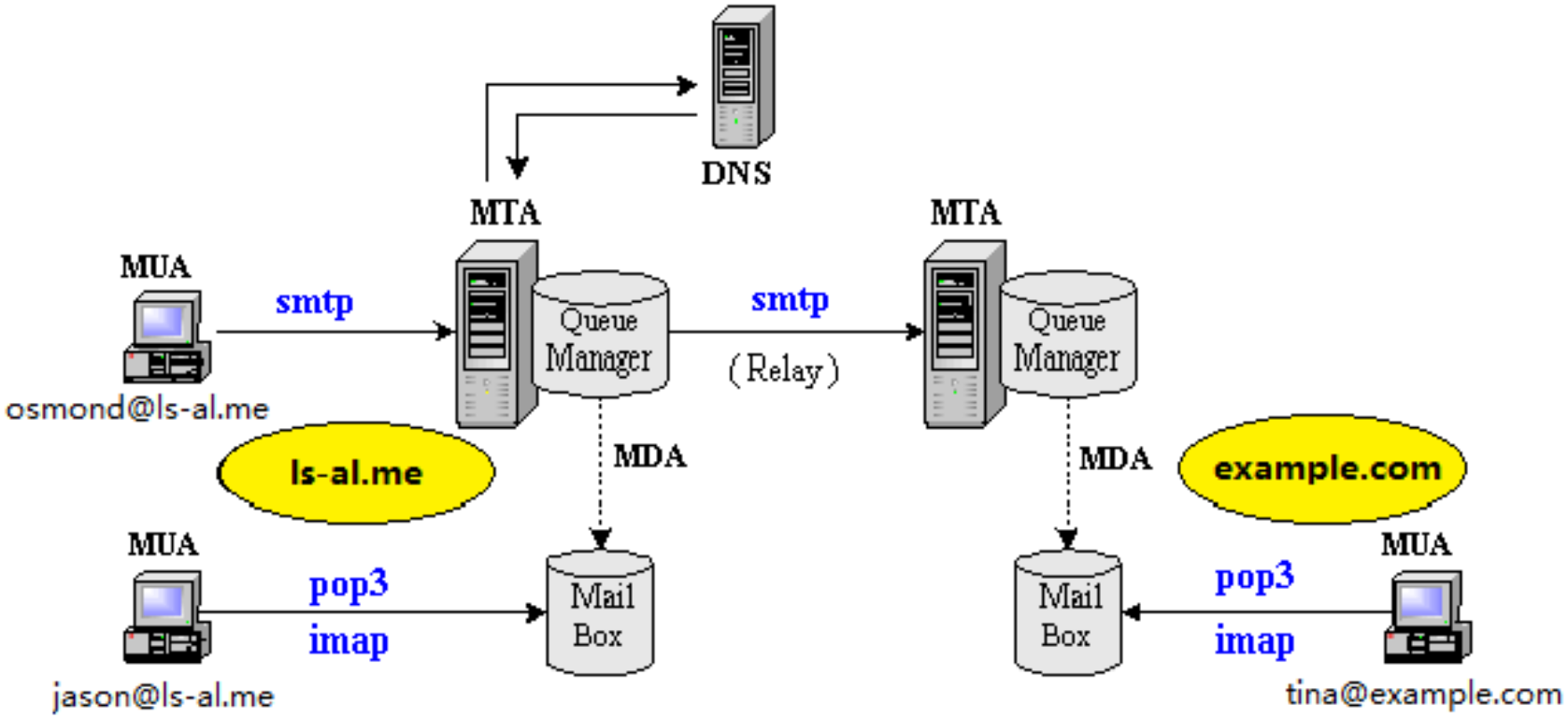
- Postfix 的各个组件以半驻留方式运行（每隔一段时间执行一次）
- Postfix的各个组件由一个**常驻内存**的**主控守护进程**（master）控制
  - 主导邮件的处理流程，是Postfix其他组件的总管
  - 配置文件为 **master.cf**
  - 只有master以root身份运行的，其他Postfix组件以postfix用户身份运行
- Postfix的组件之间通过UNIX的套接字（**Socket** ）或受保护的目录之下的先入先出命名管道（**FIFO**）进行通信

邮件队列及其管理器

- Postfix的各个组件之间通过队列管理器（Queue Manager）交换邮件
- 等候投递的邮件由qmgr进程控制
- 由**qmgr**管理的邮件队列
  - **Incoming**（收件队列）
  - **Active**（活动队列）
  - **Deferred**（延迟队列）
  - **Corrupt**（故障队列）
  - Hold（保留队列）

梁如军（linuxbooks@126.com）

Postfix邮件传输流程



梁如军（linuxbooks@126.com）

Postfix的MTA功能实现

- Postfix 实现了 **MTA** 的核心功能
  - 邮件路由 （Mail routing）
  - 邮件头重写 （Header rewriting）
  - 授权 （Authorization）
  - 内容过滤 （Content filtering）

Postfix功能——邮件路由

- 查找收件人地址的服务器
- 选择适当的MDA/LDA投递邮件
- 为提交的邮件排队等待处理
- 重新提交失败的邮件消息
- 发送投递状态通知

梁如军（linuxbooks@126.com）

邮件路由与DNS

```
example.com  MX  10 mail1.example.com.
example.com  MX  20 mail2.example.com.
example.com  MX  30 mx.nodomain.org.
```

- **Problem:** 邮件路由过程中信件要投递给哪个服务器?
- **Solution:** 查询 DNS 服务的 MX 记录
  - 以MX记录优先数的升序进行选用
  - 若没有找到MX记录，则查询邮件地址的A记录

梁如军（linuxbooks@126.com）

LDA与用户邮箱

- 当邮件的目标地址是Postfix的**mydestination**参数指定的网域之一时，Postfix由本地投递代理（local）将邮件投递到服务器上用户的邮箱。
- 用户邮箱主要有两种格式
  - 传统的mbox：**/var/spool/mail/$USER**
  - 新型的maildir：**$HOME/mail/***
- CentOS 中 Postfix 默认配置使用mbox格式

Postfix功能——邮件头重写

- 添加邮件的消息头
- 添加 Message-ID
- 实现地址重写
- 例如：
  - 移除主机名
  - 添加域名
  - osmond → osmond.liang

Postfix功能——授权

- 检查提交的主机的IP或域名
- 检查发件人地址
- 检查收件人地址
- 检查内容

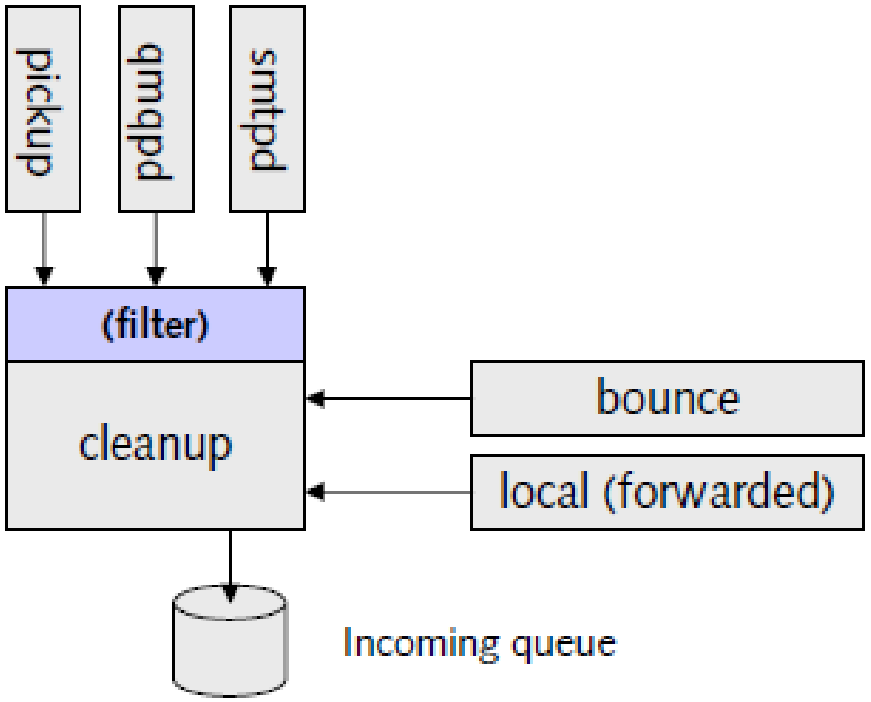
- 通常情况下允许
  - 来自本地系统的邮件
  - 发送到本地系统的邮件
  - 来自可信主机并发往任何系统的邮件

邮件中继（relay）

- 当需要把邮件从一个MTA传送到另一个MTA时，这个邮件中转的动作称为邮件中继。
- **中继限制（Relay restrictions）**
  - 为了避免本地MTA成为垃圾邮件的中转站，通常本地MTA直接禁止其他不明身份的主机利用本地服务器投递邮件。
  - 这种情况下，一个非本地主机使用本地服务器进行投递时会产生“550 relay denied” 错误。

Postfix功能——内容过滤

- 内置的内容检查
  - Header checks
  - Body checks
  - Regexp checks



- 与其他内容过滤软件配合实现内容过滤
  - 可以实现各种功能的重型的内容过滤
  - 分为**入队后过滤**和**入队前过滤**两种实现方式

梁如军（linuxbooks@126.com）

Postfix与其他软件配合——实现各种内容过滤

- 病毒（ virus ）内容扫描
- 检查附件的有效性
- 检查邮件的大小
- 检查垃圾邮件（spam）
  - 关键字过滤（Keyword filters）
  - 基于规则的过滤（rule filters）
  - 基于IP地址黑名单（IP address blacklists）
  - 基于DNS的黑名单（DNS-based blocklists）
  - 灰名单（Greylisting）

梁如军（linuxbooks@126.com）

RHEL/CENTOS 下的POSTFIX

梁如军（linuxbooks@126.com）

安装和启用Postfix

- 安装Postfix

  # yum install postfix

- 管理Postfix服务

  # systemctl {enable|disable} postfix

  # systemctl {start|stop|status|restart|reload} postfix

  - 或

  # postfix {start|stop|reload}

梁如军（linuxbooks@126.com）

Postfix服务概览

- 软件包：postfix
- 服务类型：由Systemd启动的守护进程
- 配置单元：/usr/lib/systemd/system/postfix.service
- 守护进程：/usr/libexec/postfix/master
- 端口：25 (smtp)， 465 (smtps)
- 配置文件
  - 主控守护进程配置文件：**/etc/postfix/master.cf**
  - 主配置文件：**/etc/postfix/main.cf**
- 相关软件包：procmail , openssl

Postfix的命令工具

- 管理工具
  - **/usr/sbin/postfix**：Postfix的控制程序，类似于Apache的apachectl
  - **/usr/sbin/postconf**：显示和编辑 /etc/postfix/main.cf的配置工具
  - **/usr/sbin/postalias**：构造、修改和查询别名表
  - **/usr/sbin/postmap**：构造、修改或者查询查找表
  - **/usr/sbin/postcat**：打印队列文件的内容
  - **/usr/sbin/postqueue**：邮件队列管理工具
  - **/usr/sbin/postsuper**：系统管理员的邮件队列管理工具
  - **/usr/sbin/postlog**：一个向邮件日志直接写入信息的工具

梁如军（linuxbooks@126.com）

Postfix的命令工具（续）

- 与Sendmail兼容的工具
  - **/usr/sbin/sendmail**
    - 与Sendmail兼容的邮件发送替代工具
    - 链接到 **/usr/sbin/sendmail.postfix**
  - **/usr/bin/newaliases**
    - 与Sendmail兼容的别名数据库生成替代工具
    - 链接到 **/usr/bin/newaliases.postfix**
  - **/usr/bin/mailq**
    - 与Sendmail兼容的邮件队列查询替代工具
    - 链接到 **/usr/bin/mailq.postfix**

梁如军（linuxbooks@126.com）

控制和监视Postfix

- 控制Postfix

  # postfix {abort|flush|check}

  - abort：立即退出
  - flush： 强制将目前正在邮件队列的邮件寄出
  - check：检查Postfix的目录及文件的权限并创建丢失的目录
- 队列管理
  - 查看延期的消息：**postqueue -p**
  - 发送延期消息：**postqueue -f**
- 监视Postfix日志

  # tail -f /var/log/maillog

  # egrep '(reject|warning|error|fatal|panic):' /var/log/maillog

梁如军（linuxbooks@126.com）

CentOS中Postfix的默认配置

- 在127.0.0.1网络接口上监听25号端口
- 可以接收发往本地主机和本地域的邮件

```
# service postfix start
# ps -ef|grep postfix
root      4755     1  0 Apr11 ?  00:00:00 /usr/libexec/postfix/master
postfix   4758  4755  0 Apr11 ?  00:00:00 qmgr -l -t fifo -u
postfix   6935  4755  0 02:33 ?  00:00:00 pickup -l -t fifo -u
# postconf -n |grep inet_interfaces
inet_interfaces = localhost
# postconf -n |grep mydestination
mydestination = $myhostname, localhost.$mydomain, localhost
# netstat -lunpt|grep :25
tcp    0   0  127.0.0.1:25   0.0.0.0:*   LISTEN    4755/master
```


梁如军（linuxbooks@126.com）

测试Postfix的默认配置

- 使用邮件客户工具
  - mail 或 mutt
  - 对SMTP协议是透明的
- 使用telnet或nc命令

  # nc localhost 25

  # telnet localhost 25
  - 需要熟悉SMTP/ESMTP协议命令
- 使用自动化测试工具

梁如军（linuxbooks@126.com）

swaks

- swaks（**SW**iss **A**rmy **K**nife **S**MTP）
  - 一个专门的SMTP/ESMTP自动化测试工具
  - 用 Perl 语言编写
  - 主页：http://www.jetmore.org/john/code/swaks
  - 在EPEL仓库里提供了其RPM包

    # yum install swaks
- 使用方法

$ man swaks

$ swaks --to osmond@localhost

梁如军（linuxbooks@126.com）

POSTFIX的配置文件

梁如军（linuxbooks@126.com）

Postfix 的配置文件

- **/etc/postfix/master.cf**
  - postfix的master进程的配置文件
  - 每一行配置一个postfix组件进程的运行方式
  - 默认的master.cf文件即可良好的工作，通常无需修改
  - 一般地，只有当Postfix需要配合其他软件协同工作时才需要修改
- **/etc/postfix/main.cf**
  - postfix的主配置文件
  - 每一行指定一个参数的值

梁如军（linuxbooks@126.com）

main.cf的配置语法

parameter = value1 [value2] [value3] [……]

- Postfix提供了800多个可供配置的参数
- 说明
  - 等号左右两端紧跟的空格不是必须的。
  - 一个参数的多个值之间以空格间隔或以逗号和空格作为间隔。
  - 以空格开始的行为上一配置行的继续。
  - 每个参数的值必须直接书写，不能使用单引号或双引号将其括起。

梁如军（linuxbooks@126.com）

main.cf的配置语法（续）

parameter = value1 [value2] [value3] [……]

- 说明
  - 不要在参数行后使用#号添加注释，所有以#号开始的注释行必须单独成行。
  - 可以在等号右边的参数名前加$字符引用其他参数的值。
  - 若重复设定某一参数的值，则以最后出现的设定值为准。
  - 可将参数值写在另一个文本文件中，并把文件名提供给参数，任何以 / 字符开始的字符串都会被视为文件名。

梁如军（linuxbooks@126.com）

main.cf的常用参数

参数	说明
inet_interfaces	指定Postfix监听的网络接口。all 表示所有网络接口
myhostname	指定运行Postfix服务的邮件主机名称（FQDN名）
mydomain	指定运行Postfix服务的邮件主机的域名
myorigin	指定由本台邮件主机寄出的每封邮件的邮件头中mail from的地址
mydestination	指定可接收邮件的主机名或域名，只有当发来的邮件的收件人地址与该参数值相匹配时，Postfix才会将该邮件接收下来
mynetworks	设置可转发（Relay）哪些IP网段的邮件
relay_domains	设置可转发（Relay）哪些网域的邮件

- 更多参数参见手册：**$ man 5 postconf**

Postfix的配置方法

- 修改主配置文件**main.cf**的两种方法
  - 使用文本编辑器直接修改主配置文件
  - 使用 **postconf -e** 命令修改主配置文件的配置参数
- 使配置生效

  # postfix reload

梁如军（linuxbooks@126.com）

postconf 的常用功能

- 显示默认设置
  - **postconf -d**
- 显示当前的非默认设置
  - **postconf -n**
- 修改main.cf 的配置参数
  - **postconf -e <key>=<value...>**
- 显示支持的映射表类型
  - **postconf -m**
- 显示支持用哪些程序做SASL身份认证
  - **postconf -a**

配置基本功能的MTA

CentOS
The Community ENTerprise Operating System

 # vim /etc/postfix/main.cf

```
inet_interfaces = all
myhostname = centos1.ls-al.me
mydomain = ls-al.me
myorigin = $mydomain
mydestination = $myhostname, localhost.$mydomain,
   localhost, mail.$mydomain, $mydomain
mynetworks = 127.0.0.0/8, 192.168.0.0/24
relay_domains = $mydestination
```

 # postfix reload

梁如军（linuxbooks@126.com）

POSTFIX的映射表及其应用

梁如军（linuxbooks@126.com）

Postfix的映射表

- 映射表（Maps）是Postfix用于查询信息的文件和数据库。
- 映射表可被用于多种不同的用途。
- Postfix使用映射表查询来实现各种地址重写功能。
- Postfix支持多种不同的映射类型，可用的格式依赖于Postfix的编译情况。
- 查看Postfix支持哪些类型的映射

```
# postconf -m
```


梁如军（linuxbooks@126.com）

Postfix的映射表类型

- 索引映射表（Indexed Maps）
  - 是从普通文本文件通过工具生成的二进制数据库postmap/postalias/newaliases
  - 这种键值数据库可以加快Postfix通过键来查找其对应值的速度
  - 常用的映射类型为hash（Postfix默认的映射类型）、btree、dbm
- 线性映射表（Linear Maps）
- 数据库（Databases）

Postfix的映射表类型（续）

- 线性映射表（Linear Maps）
  - 线性映射表是常规的文本文件
  - 无需也无法生成线性映射表对应的二进制文件
  - 常用的映射类型为pcre、regexp、cidr
- 数据库（Databases）
  - Postfix对待数据库的处理类似于索引映射表
  - 常用的映射类型为：LDAP、MySQL、PostgreSQL

梁如军（linuxbooks@126.com）

Postfix重要的映射表

- **access**：SMTP存取控制映射表
- **aliases**：别名映射表
- **virtual**：虚拟别名映射表
- **canonical**：
  - 对传入的邮件进行地址改写的映射表
- **generic**：
  - 对传出的邮件进行地址改写的映射表
- **header_checks**：过滤邮件头使用的映射表
- **body_checks**：过滤邮件内容使用的映射表

梁如军（linuxbooks@126.com）

access映射表

- access映射表
  - 用于实现SMTP访问限制
  - 是索引映射表（Indexed Maps）
    - 编辑纯文本文件 /etc/postfix/access
    - 生成散列数据库

    # postmap /etc/postfix/access

    # postfix reload
- 在主配置文件 main.cf中配置使用access映射表

  smtpd_**TAG**_restrictions = check_**TAG**_access hash:/etc/postfix/access, …
  - **TAG可以是 sender, recipient, client, helo**

梁如军（linuxbooks@126.com）

access映射表的格式

- 每一行的格式为

<地址> <动作>

- 地址字段常用格式

格　式	举　例
domain	yourdomain.com
	.yourdomain.com
ip address	192.168.12
	192.168.11.11
username@domain	someone@somedomain.com
username@	someone@

梁如军（linuxbooks@126.com）

access映射表的格式（续）

- 每一行的格式为

<地址> <动作>

- 动作字段常用格式

动作	说明
OK	无条件接受或发送
RELAY	允许中继代理投递(SMTP RELAY)
REJECT	拒绝接受并发布错误信息
DISCARD	丢弃邮件，无错误信息发布
HOLD	将邮件阻止在邮件队列中
4nn text	返回临时错误码4nn及消息
5nn text	返回临时错误码5nn及消息

梁如军（linuxbooks@126.com）

access映射表的使用时机

语句	说明
smtpd_client_restrictions	使用**check_client_access**选项指定要检查的access映射表，**用于SMTP建立连接请求的阶段**
smtpd_helo_restrictions	使用**check_helo_access**选项指定要检查的access映射表，**用于SMTP启动会话的HELO/EHLO命令阶段**
smtpd_sender_restrictions	使用**check_sender_access**选项指定要检查的access映射表，**用于SMTP发件人说明的MAIL FROM命令阶段**
smtpd_recipient_restrictions	使用**check_recipient_access**选项指定要检查的access映射表，**用于SMTP收件人说明的RCPT TO命令阶段**

梁如军（linuxbooks@126.com）

access映射表配置举例

- 限制向Postfix发起SMTP连接的客户
- 通过收件人地址限制Postfix的转发

参见教材的操作步骤

梁如军（linuxbooks@126.com）

aliases映射表

- aliases映射表
  - 用于实现Postfix的本地别名机制，与Sendmail兼容
  - 是索引映射表（Indexed Maps）
    - 编辑纯文本文件 /etc/aliases
    - 生成散列数据库

    # postalias /etc/aliases

    # postfix reload
- 在主配置文件 main.cf中配置使用aliases映射表

```
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```


梁如军（linuxbooks@126.com）

aliases映射表的格式

- 每一行的格式为

alias：recipient [，recipient，…]

- /etc/aliases举例

```
lrj:osmond
osmond:sinosmond,  sinosmond@domian.tld
net_group:osmond, tom, stillman, patrcko
ourlist:include: /etc/postfix/ourmailinglist
```

```
# newaliases
# service postfix reload
```


梁如军（linuxbooks@126.com）

virtual映射表

- virtual映射表
  - 用于实现Postfix的虚拟别名机制
    - 将发给虚拟域的邮件投递到真实域的用户邮箱中
    - 也可以实现邮件列表的功能
  - 是索引映射表（Indexed Maps）
    - 编辑纯文本文件 /etc/postfix/virtual
    - 生成散列数据库

```
# postalias /etc/postfix/virtual
# postfix reload
```

- 在主配置文件 main.cf中配置使用virtual映射表

```
virtual_alias_maps = hash:/etc/postfix/virtual
virtual_alias_domains = olabs.org，olabs.net，olabs.com
```

virtual映射表的格式

- 每一行的格式为

<虚拟域地址> <真实域地址>

- /etc/postfix/virtual举例

```
@olabs.net          @ls-al.me
@olabs.org          @ls-al.me
sales@olabs.net     sinosmond
sales@olabs.org     sinosmond
sales@olabs.com     sinosmond
admin@olabs.com     osmond, osmond@domian.tld
web@olabs.com       webmaster，osmond
```

```
# postalias /etc/postfix/virtual
# postfix reload
```


梁如军（linuxbooks@126.com）

POSTFIX的UCE控制

梁如军（linuxbooks@126.com）

Postfix默认的传输限制

- 接受符合以下条件的邮件
  - 目的地为**$inet_interfaces**的邮件
  - 目的地为**$mydestination**的邮件
  - 目的地为**$virtual_maps**的邮件
- 转发符合以下条件的邮件
  - 来自客户端IP地址符合**$mynetworks**的邮件
  - 来自客户端主机名符合**$relay_domains**及其子域的邮件
  - 目的地为**$relay_domains**及其子域的邮件

Postfix的UCE控制简介

- UCE（Unsolicited Commercial Email）控制
  - **控制 Postfix 接收或转发来自于什么地方的邮件**
  - **控制 Postfix 接收或转发内容与设置相符的邮件**
- UCE控制的功能
  - 白名单（允许）列表、黑名单（拒绝）列表
  - 实时黑名单列表（Real-time Blackhole List，RBL）
    - DNSRBL——Domain Name System Real-time Blackhole List
  - 发送者DNS核实
  - 邮件头检查过滤
  - 邮件内容检查过滤

梁如军（linuxbooks@126.com）

实现强大的UCE控制功能

- 通过SMTP限制（**smtpd restrictions**）实现
  - 在SMTP会话的各个阶段进行限制
    - **smtpd_*_restrictions**
  - 通过严格SMTP会话标准进行限制
    - **smtpd_helo_required = no|yes**
- 通过Postfix内置的内容检查实现
  - 通过邮件头是否符合RFC标准进行限制
    - **strict_rfc821_envelopes = no|yes**
  - 通过**邮件头过滤**进行限制（ **header_checks**）
  - 通过**邮件内容过滤**进行限制（**body_checks**）

实现SMTP限制的参数

参数	说明
smtpd_client_restrictions	限制可以向Postfix发起SMTP 连接的客户端的主机名或IP地址
smtpd_helo_restrictions	指定客户端在执行**HELO**命令时发送给Postfix的主机名
smtpd_sender_restrictions	通过发件人在执行**MAIL FROM**命令时提供的地址进行限制
smtpd_recipient_restrictions	通过发件人在执行**RCPT TO**命令时提供的地址进行限制

- 每个参数均可以同时指定一个或多个限制规则（多个规则用逗号分隔）
- Postfix按顺序查询每一个限制规则，第一条符合条件的规则将被执行

使用 **man 5 postconf** 命令查看上述参数可使用的规则

梁如军（linuxbooks@126.com）

SMTP会话一例

CentOS
The Community ENTerprise Operating System

```
# swaks --to osmond@localhost
=== Trying localhost:25...
=== Connected to localhost.
← 220 centos1.ls-al.me ESMTP Postfix
→ EHLO centos1.ls-al.me
← 250-centos1.ls-al.me
← 250-PIPELINING
← 250-SIZE 10240000
← 250-VRFY
← 250-ETRN
← 250-ENHANCEDSTATUSCODES
← 250-8BITMIME
← 250 DSN
 → MAIL FROM:<root@centos1.ls-al.me>
← 250 2.1.0 Ok
```

client

helo/ehlo

sender

梁如军（linuxbooks@126.com）

SMTP会话一例（续）

→ **RCPT TO:**<osmond@localhost>
← 250 2.1.5 Ok
→ **DATA**
← 354 End data with <CR><LF>.<CR><LF>
→ Date: Wed, 13 Apr 2011 04:07:33 +0800
→ To: osmond@localhost
→ From: root@centos1.ls-al.me
→ Subject: test Wed, 13 Apr 2011 04:07:33 +0800
→
→ This is a test mailing
→
→ .
← 250 2.0.0 Ok: queued as 40FD39004B
→ QUIT
← 221 2.0.0 Bye
=== Connection closed with remote host.

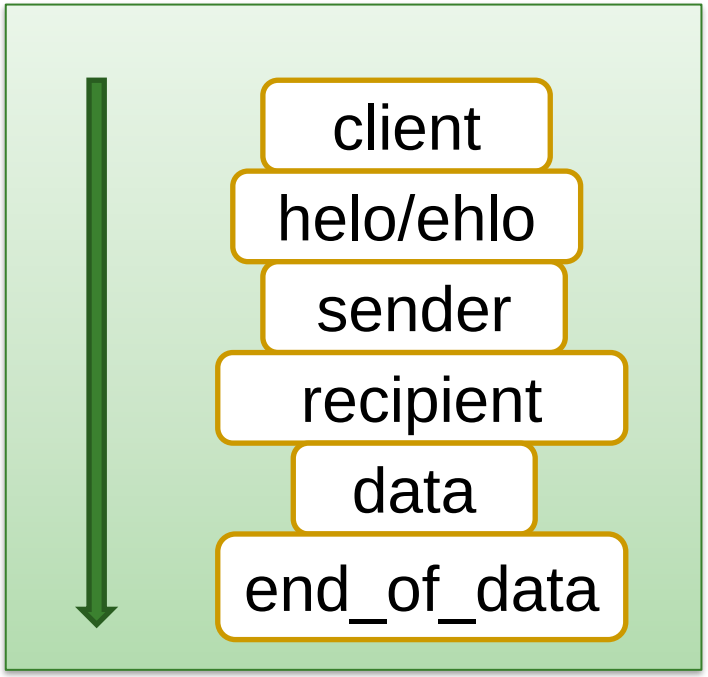
recipient

data

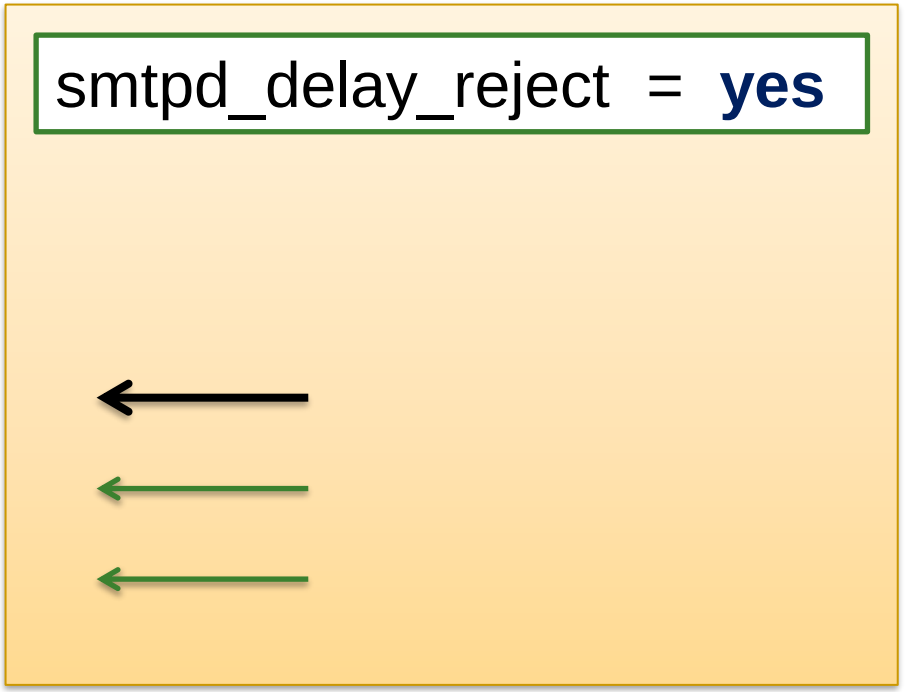
end_of_data

SMTP限制的检查顺序和检查时机

- 检查顺序



- 检查时机



梁如军（linuxbooks@126.com）

smtpd_client_restrictions

- 缺省值为空，即接收来自任何客户端的SMTP连接
- 常用的限制规则

限制规则	说明
permit_mynetworks	接受$mynetworks参数定义的客户端连接
permit_sasl_authenticated	接受已经过SMTP认证的客户端连接
reject_unknown_client_hostname	若客户端的IP反向解析失败，或主机名正向解析失败，或以主机名解析的IP与客户端IP不符则拒绝连接
reject_unknown_reverse_client_hostname	若客户端的IP反向解析失败则拒绝连接
reject_rbl_client rbl_domain	使用客户端的反向IP查询RBL，若在RBL中出现则拒绝连接
check_client_access type:table	根据客户端的主机名、父域名、IP地址或所属网段搜索Access映射表进行连接限制

梁如军（linuxbooks@126.com）

中国反垃圾邮件联盟(CASA)——http://anti-spam.org.cn/

- 提供免费的实时黑名单列表（RBL）服务

类型	说明	网址
CBL	中国国内的主要垃圾邮件发送源	**cbl.anti-spam.org.cn**
CDL	中国国内动态分配地址	**cdl.anti-spam.org.cn**
CBL+	CBL和CDL的合集	**cblplus.anti-spam.org.cn**
CBL-	CBL+中去除了中国邮件服务运营商白名单（CML）的内容后的黑名单	**cblless.anti-spam.org.cn**

- 配置Postfix使用CASA的RBL

```
smtpd_client_restrictions = ...
    reject_rbl_client cblless.anti-spam.org.cn, ...
```


梁如军（linuxbooks@126.com）

smtpd_client_restrictions举例


```
smtpd_client_restrictions =  permit_mynetworks,
    permit_sasl_authenticated
    reject_unknown_client_hostname
```

```
smtpd_client_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    check_client_access hash:/etc/postfix/client_access,
    reject_rbl_client cblless.anti-spam.org.cn,
    reject_rbl_client bl.spamcop.net,
    reject_rbl_client t1.dnsbl.net.au,
    reject_rbl_client xbl.spamhaus.org
```

```
smtpd_client_restrictions =  permit_mynetworks,
    permit_sasl_authenticated, reject
```


梁如军（linuxbooks@126.com）

smtpd_helo_restrictions

- 缺省值为空，即接收客户端发送的任意形式的主机名
- 常用的限制规则

限制规则	说明
permit_mynetworks	若HELO命令所带的主机名参数包含在$mynetworks参数中则允许客户端连接
reject_invalid_helo_hostname	若HELO命令所带的主机名参数不符合语法规范则拒绝客户机的连接请求
reject_non_fqdn_helo_hostname	若客户端执行HELO命令时的主机名不是RFC规定的FQDN则拒绝客户端的连接请求
reject_unknown_helo_hostname	若客户端执行HELO命令时的主机名在DNS中没有相应的A 或 MX记录则拒绝该客户端的连接请求
reject_rhsbl_helo rbl_domain	若执行HELO命令时的主机名在RBL中出现则拒绝连接
check_helo_access type:table	根据执行HELO命令时的主机名、父域名搜索Access映射表进行连接限制

smtpd_helo_restrictions举例


```
smtpd_helo_restrictions =
    permit_mynetworks
    reject_invalid_helo_hostname
    reject_non_fqdn_helo_hostname
    reject_unknown_helo_hostname
    check_helo_access hash:/etc/postfix/helo_access
```


梁如军（linuxbooks@126.com）

smtpd_sender_restrictions

- 缺省值为空，即接受来自任何发件人的邮件
- 常用的限制规则

限制规则	说明
permit_mynetworks	若MAIL FROM命令提供的主机名所对应的网段包含在$mynetworks参数中则允许连接
reject_non_fqdn_sender	若执行MAIL FROM命令提供的主机名不是RFC规定的FQDN则拒绝客户端的连接请求
reject_unknown_sender_domain	若执行MAIL FROM命令提供的主机名在DNS中没有相应的A 或 MX 记录则拒绝该客户端的连接请求
reject_rhsbl_sender rbl_domain	若执行MAIL FROM命令时的主机名在RBL中出现则拒绝连接
check_sender_access type:table	根据执行MAIL FROM命令时的主机名、父域名或发件用户搜索Access映射表进行连接限制

梁如军（linuxbooks@126.com）

smtpd_sender_restrictions 举例

```
smtpd_sender_restrictions =
    permit_mynetworks
    reject_non_fqdn_sender
    reject_unknown_sender_domain
    check_sender_access hash:/etc/postfix/sender_access
```


梁如军（linuxbooks@126.com）

smtpd_recipient_restrictions

- 缺省值为
  - **permit_mynetworks, reject_unauth_destination**
- 常用的限制规则

限制规则	说明
reject_non_fqdn_recipient	若执行RCPT TO命令提供的主机名不是RFC规定的FQDN则拒绝客户端的连接请求
reject_unknown_recipient_domain	若执行RCPT TO命令提供的主机名在DNS中没有相应的A 或 MX 记录则拒绝该客户端的连接请求
reject_rhsbl_recipient rbl_domain	若执行RCPT TO命令时的主机名在RBL中出现则拒绝连接
check_recipient_access type:table	根据执行RCPT TO命令时的主机名、父域名或收件用户搜索Access映射表进行连接限制

梁如军（linuxbooks@126.com）

smtpd_recipient_restrictions

- 缺省值为
  - **permit_mynetworks, reject_unauth_destination**
- 常用的限制规则（续）

限制规则	说明
permit_mynetworks	若RCPT TO命令提供的主机名所对应的网段包含在$mynetworks参数中则允许连接
permit_sasl_authenticated	允许已经通过SMTP认证的客户端连接
permit_auth_destination	若收件者域名符合$relay_domains及其子域或收件者的目的地为本机（即域名列于$inet_interfaces, $proxy_interfaces, $mydestination, $virtual_alias_domains, $virtual_mailbox_domains）则接受连接
reject_unauth_destination	与上一规则的逻辑相反

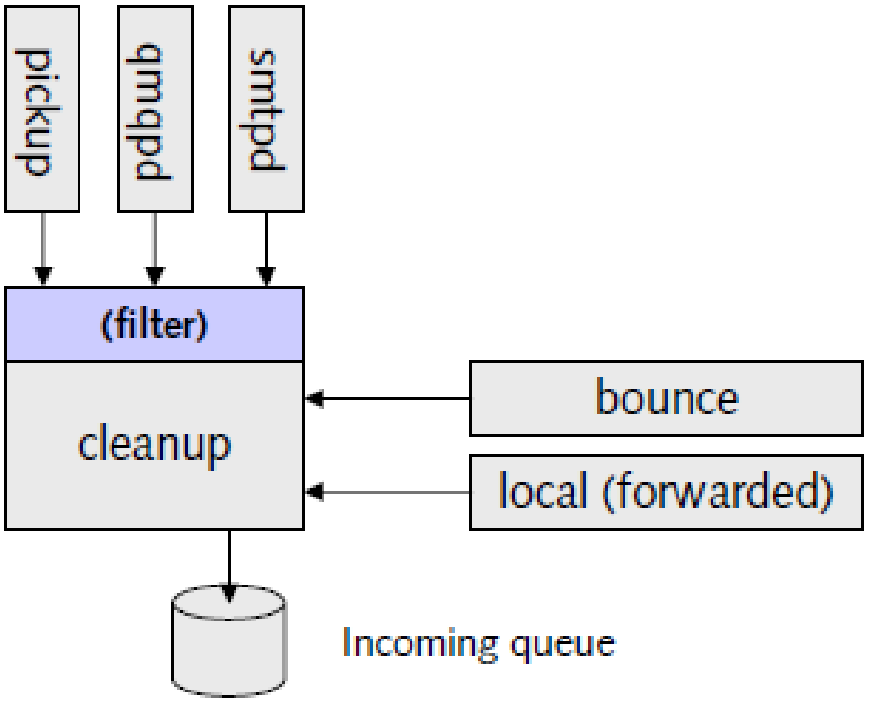
smtpd_recipient_restrictions 举例

```
smtpd_recipient_restrictions =
    reject_unknown_recipient_domain
    permit_mynetworks
    permit_sasl_authenticated
    reject_unauth_destination
    check_recipient_access hash:/etc/postfix/recipient_access
```


梁如军（linuxbooks@126.com）

Postfix内置的内容检查

- 内置的内容检查可以实现邮件头和邮件内容过滤
- 在邮件入队（调入incoming队列）之前由**cleanup**组件负责处理内容检查
  - 仅接受pickup、smtpd、qmqpd组件接收的邮件
  - 通过查询pcre或regeap类型的映射表实现



梁如军（linuxbooks@126.com）

实现内置内容检查的参数

- 参数

参数	说明
header_checks type:table	通过**邮件头过滤**进行限制
body_checks type:table	通过**邮件内容过滤**进行限制

- 举例

```
header_checks = pcre:/etc/postfix/header_checks
body_checks   = pcre:/etc/postfix/body_checks
```

- 有关pcre映射表的书写语法参见手册

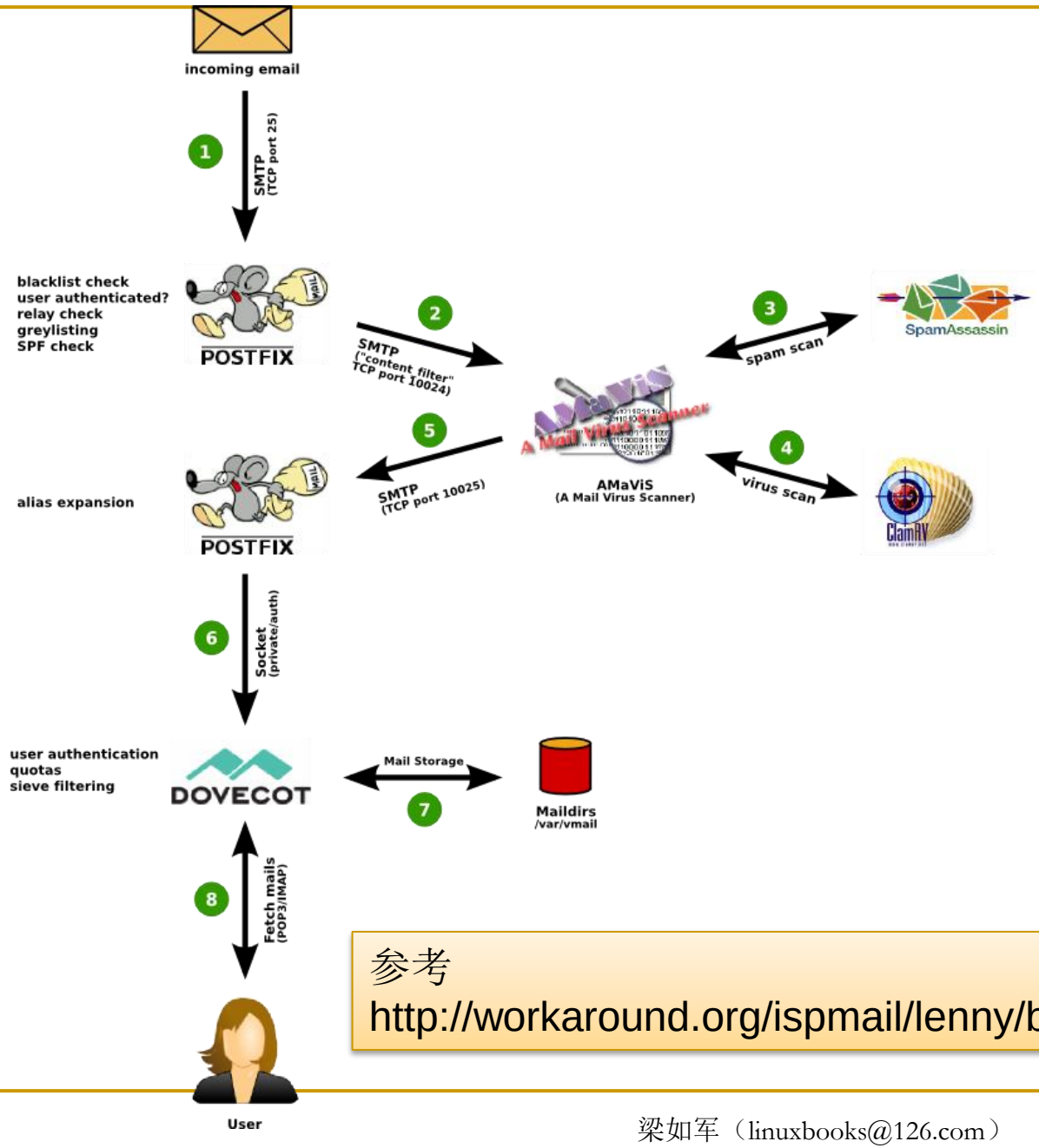
梁如军（linuxbooks@126.com）

Postfix内置内容检查的缺点及解决方法

- 缺点
  - 采用一系列的RE匹配比对，相当耗费系统资源
  - 只能实现轻量级的过滤规则处理
  - 会导致 cleanup 组件因等待大量过滤规则检查的完成而超时
  - 不适合在生产环境中用于垃圾邮件和病毒邮件处理
- 解决
  - 采用入队后的过滤处理避免cleanup 组件因等待而超时
  - 将邮件传给更专业的外部软件进行垃圾邮件和病毒邮件处理

梁如军（linuxbooks@126.com）

Postfix与外部软件配合实现垃圾邮件和病毒邮件处理



参考
http://workaround.org/ispmail/lenny/bigpicture

梁如军（linuxbooks@126.com）

DOVECOT的安装和配置

梁如军（linuxbooks@126.com）

Docecot简介

- Dovecot 实现了从邮件服务器中读取邮件时使用的POP/POPS、IMAP/IMAPS 协议
- Dovecot 由 Timo Sirainen 开发，最初发布于2002年7月
- Dovecot 在安全性方面比较出众
- Dovecot 执行速度快、内存用量少
- Dovecot 支持多种认证方式
- Dovecot 配置简单

Docecot的特点

- 采用模块化设计
- 完全兼容 UW IMAP 和 Courier IMAP
- 包含内置的 LDA 和 LMTP 服务，并提供可选的 Sieve 过滤支持
- 支持标准的 mbox、Maildir以及 其自己开发的高性能的 dbox 邮箱格式
- 支持对 IMAP 和 POP 的多种验证模式，如：CRAM-MD5 和 DIGEST-MD5等
- 支持多种账户存储方式，如：口令文件、PAM、SQL、LDAP等
- 支持 SASL 和 TLS

梁如军（linuxbooks@126.com）

Docecot的系统结构——重要进程组件

- **dovecot**：Dovecot 常驻内存的主守护进程
- **anvil**：用于跟踪用户的连接
- **log**：为除了主守护进程之外的所有进程组件记录日志到日志文件
- **config**：解析配置文件并为其他进程组件发送配置
- **auth**：用于处理所有认证
- **auth -w**：用于处理后台数据库（如：MySQL）验证的“认证工作者”进程，这样的进程会随需要创建更多
- **imap-login/pop3-login**：在用户登录之前处理新的 IMAP/POP3 连接，甚至会在登录之后处理代理的SSL连接
- **imap/pop3**：在用户登录后处理 IMAP/POP3 连接

梁如军（linuxbooks@126.com）

Dovecot服务概览

- 软件包： dovecot
- 服务类型：由Systemd启动的守护进程
- 配置单元：/usr/lib/systemd/system/dovecot.service
- 守护进程： /usr/sbin/dovecot
- 端口： 110 (pop), 995 (pop3s), 143 (imap), 993 (imaps)
- 配置文件： /etc/dovecot.conf
- 相关软件包： procmail, fetchmail, openssl

梁如军（linuxbooks@126.com）

Dovecot的安装和启动

- 安装

  # yum install dovecot

- 使用systemctl命令管理Dovecot服务

  # systemctl {start|stop|status|restart|reload} dovecot

  # systemctl {enable|disable} dovecot

- 使用doveadm命令控制Dovecot

  # doveadm stop|reload

- 查看Dovecot监听的网络端口

  # netstat -lnpt|grep dovecot

梁如军（linuxbooks@126.com）

使用doveconf 显示Dovecot的配置

- doveconf -d　　显示所有参数的默认值
- doveconf -a　　显示所有参数的当前值
- doveconf -n　　显示所有修改了默认值的参数

- doveconf -d <parameter>　显示指定参数的默认值
- doveconf <parameter>　　显示指定参数的当前值
- doveconf -N　　显示所有修改了默认值的参数以及明确设置了默认值的参数

梁如军（linuxbooks@126.com）

Dovecot 的配置文件

- 主配置文件 /etc/dovecot/dovecot.conf
- 守护进程配置文件/etc/dovecot/conf.d/10-master.conf
- 配置文件 /etc/dovecot/conf.d/[129][05]-*conf 用于配置模块参数
- 被 /etc/dovecot/conf.d/10-auth.conf包含的 /etc/dovecot/conf.d/auth-*.conf.ext文件为不同的认证模块提供配置参数

梁如军（linuxbooks@126.com）

Dovecot的基本配置——实现POP3/IMAP服务

- 修改主配置文件 /etc/dovecot/dovecot.conf

  protocols = imap pop3

  listen = *

- 编辑认证模块配置文件 /etc/dovecot/conf.d/10-auth.conf

  disable_plaintext_auth = no

  auth_mechanisms = plain login

  !include auth-system.conf.ext

- 编辑邮箱模块配置文件/etc/dovecot/conf.d/10-mail.conf

  mail_location = maildir:~/Maildir

- 编辑ssl默认配置文件 /etc/dovecot/conf.d/10-ssl.conf

  ssl = no

梁如军（linuxbooks@126.com）

检测POP和IMAP配置

- 图形工具
  - Thunderbird
  - Evolution
  - Outlook
  - Foxmail
- 字符工具 Mutt

mutt -f pop://user@server[:port]

mutt -f pop://osmond@centos1.ls-al.me

mutt -f imap://user@server[:port]

mutt -f imap://osmond@centos1.ls-al.me

POSTFIX的SMTP认证

梁如军（linuxbooks@126.com）

开放中继和中继控制

- 开放中继（Open Relay）
  - 邮件服务器可以将不认识的客户机发来的邮件转发给其他服务器
  - Postfix默认配置相当严格，默认不会做开放中继，而仅对本机（localhost）开放转发功能
- 中继控制
  - 使用 mynetworks、relay_domains 参数开放一些可信任的网段或网域的中继
  - 使用 access 映射表实现中继控制
  - 使用SMTP认证

SMTP认证的引入和实现

- 引入
  - 解决移动用户使用邮件服务器的发信问题
  - SMTP认证机制可以实现用户级别的邮件中继控制
    - 对要求转发邮件的客户进行用户身份验证（用户名/口令）
    - 只有通过了验证才能接收该用户寄来的邮件并转发
- 实现
  - 通过简单认证与安全层（Simple Authentication and Security Layer，SASL）实现
    - 允许使用多种类型的身份验证隐藏在SASL协议的后端
    - 实现验证的后端服务可以是PAM，用户和口令数据库、LDAP等

Postfix的SMTP认证

- Postfix支持用于实现SMTP认证的SASL
- Postfix本身并没有内置SASL库程序，需要继承其他程序提供的SASL功能
- Postfix支持cyrus和dovecot提供的SASL功能
- Postfix支持用哪些程序做SASL身份认证

```
# postconf -a
cyrus
dovecot
```


梁如军（linuxbooks@126.com）

配置Postfix启用SMTP认证1

- **步骤1：**配置Dovecot 实现SMTP认证的监听进程（可以是UNIX套接字或TCP端口）

/etc/dovecot/conf.d/10-master.conf

```
service auth {
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660    # 指定套接字文件权限
    user = postfix    # 指定套接字文件的属主
    group = postfix   # 指定套接字文件的组
  }
  …
}
```


梁如军（linuxbooks@126.com）

配置Postfix启用SMTP认证2

- **步骤2：**配置Postfix启用基于Dovecot的 SASL（并设置与SASL相关的配置参数）

/etc/postfix/main.cf

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
```


梁如军（linuxbooks@126.com）

Postfix的main.cf中与SASL相关的配置参数

- **smtpd_sasl_type**：指定SASL插件类型，默认为cyrus。
- **smtpd_sasl_auth_enable**：指定是否启用SASL作为SMTP认证方式。
- **smtpd_sasl_security_options**：用来限制某些登录的方式。
  - 若设置为“noanonymous”，则表示禁止采用匿名登录方式。
- **broken_sasl_auth_clients**：表示是否兼容非标准的SMTP认证。用于M$早期的SMTP客户端。

梁如军（linuxbooks@126.com）

Postfix的main.cf中与SASL相关的配置参数（续）

- **smtpd_recipient_restrictions**：通过收件人地址对客户端发来的邮件进行过滤
  - 选项 **permit_sasl_authenticated** 表示允许通过SASL认证的客户转发邮件
  - 选项 **permit_mynetworks** 表示只要收件人地址位于mynetworks参数中指定的网段就可以转发邮件
  - 选项 **reject_unauth_destination** 表示拒绝转发含不可信任的目标地址的邮件
- **smtpd_client_restrictions**：限制可以向Postfix发起SMTP连接的客户端

梁如军（linuxbooks@126.com）

配置Postfix的SMTP认证

CentOS
The Community ENTerprise Operating System

vim /etc/postfix/main.cf

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
broken_sasl_auth_clients = yes

smtpd_recipient_restrictions =
  permit_sasl_authenticated,
  permit_mynetworks,
  reject_unauth_destination
```

postfix reload

检测Postfix的SMTP认证

CentOS
The Community ENTerprise Operating System

**# swaks -a -au osmond -ap <passwd> **

--to root@ls-al.me --from osmond@ls-al.me

```
.............
<-  250-AUTH LOGIN PLAIN
<-  250-AUTH=LOGIN PLAIN
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250 DSN
 -> AUTH LOGIN
<-  334 VXNlcm5hbWU6
 -> b3Ntb25k
<-  334 UGFzc3dvcmQ6
 -> d2xseXNobWxq
<-  235 2.0.0 Authentication successful
.............
```


梁如军（linuxbooks@126.com）

基于TLS/SSL的邮件服务

梁如军（linuxbooks@126.com）

邮件服务与TLS/SSL

- Postfix和Dovecot使用OpenSSL提供的库实现基于TLS/SSL的连接
- 使用基于TLS/SSL的连接可以提供如下功能
  - 对通信数据进行加密（对于支持PLAIN认证的邮件服务器尤其需要加密通信）
  - 实现基于用户TLS证书的认证
- SMTP/POP3/IMAP4支持两种TLS/SSL连接
  - SMTP/POP3/IMAP4 over TLS：
    - 使用与SMTP/POP3/IMAP4独立的端口作加密连接。
    - 客户端连接465/995/993端口直接进行加密传输。
  - 通过STARTTLS将纯文本协议SMTP/POP3/IMAP4连接升级为TLS/SSL加密连接。

创建自签名证书

```
# cd /etc/pki/tls

# openssl req -new -x509 -days 365 -sha256 -nodes -newkey rsa:2048 \
-keyout private/mail.olabs.lan.key -out certs/mail.olabs.lan.crt \
-subj
'/O=olabs/L=Beijing/C=CN/emailAddress=root@olabs.lan/CN=mail.olabs.lan'
```


梁如军（linuxbooks@126.com）

配置基于TLS的Postfix

CentOS
The Community ENTerprise Operating System

/etc/postfix/main.cf

```
smtpd_tls_security_level = may
#smtpd_tls_security_level = encrypt
smtpd_tls_protocols = !SSLv2, !SSLv3

smtpd_tls_auth_only = yes

smtpd_tls_cert_file = /etc/pki/tls/certs/mail.olabs.lan.crt
smtpd_tls_key_file = /etc/pki/tls/private/mail.olabs.lan.key

smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache
```


梁如军（linuxbooks@126.com）

配置基于TLS的Dovecot

/etc/dovecot/conf.d/10-ssl.conf

```
ssl = yes

ssl_cert = </etc/pki/tls/certs/mail.olabs.lan.crt
ssl_key = </etc/pki/tls/private/mail.olabs.lan.key

ssl_protocols = !SSLv2 !SSLv3
```


梁如军（linuxbooks@126.com）

本章思考题

- 简述电子邮件系统的组成。
- 简述几种电子邮件协议。
- 什么是邮件中继？
- MTA与DNS是如何协同工作的？
- 简述Postfix的工作原理。
- Postfix如何实现SMTP认证？
- Postfix 如何实现UCE控制？

梁如军（linuxbooks@126.com）

本章实验

- 学会配置带SMTP认证的邮件服务器
- 学会配置Postfix常用的映射表
  - access映射表
  - aliases映射表
  - virtual映射表
- 学会配置Postfix基于SMTP限制的UCE控制
- 学会配置Dovecot
- 学会配置基于SSL/TLS协议的邮件服务器

梁如军（linuxbooks@126.com）

进一步学习

- 学习配置Postfix的基于TLS的SMTP服务（SMTPS）。
- 学习配置Dovecot的基于SSL的POP/IMAP服务（POPS/IMAPS）。
- 学习配置Postfix+MySQL+Dovecot实现的虚拟用户邮件服务器。
- 学习配置Postfix+LDAP+Dovecot实现的虚拟用户邮件服务器。
- 学习Anti-Spam和Anti-Virus的相关概念及技术。
- 学习Postfix+Amavisd-new+ClamAV+Spamassassin的实现方法。
- 学习使用pflogsumm分析邮件日志。
- 学习配置Awstats分析和统计邮件日志。

进一步学习（续）

- 学习如下Webmail的配置和使用。
  - RoundCube（http://roundcube.net）
  - SquirrelMail（http://squirrelmail.org）
  - RainLoop （http://www.rainloop.net）
- 学习如下邮件系统解决方案的安装、配置和使用。
  - iRedMail（http://www.iredmail.org/）
  - ExtMail（http://www.extmail.org/）