

技术文档：快速搭建邮件系统

前言

搭建一个基于开源组件的邮件系统，其过程兼具简单与复杂性。简单之处在于，基础服务的安装可以通过几个简单的 `apt` 命令快速完成。然而，真正的难度在于邮件系统核心组件（如 Postfix, Dovecot, OpenDKIM, OpenSPF）之间的复杂配置、整合与协同工作。这些组件通常是独立开发的，要确保它们高效、安全且符合邮件传输标准地协同运行，需要细致的调整和大量的配置文件管理。

本文档旨在提供一个基于已知工作配置文件的快速部署流程，以最大限度地减少从零开始配置的精力消耗。

步骤 (一)：环境准备与先决条件

1. 操作系统要求

- 系统：** Ubuntu 22.04 LTS。
- 兼容性说明：** 建议使用 Ubuntu 22.04。高于此版本的系统可能因 Python 版本变化导致某些依赖服务（例如 `policyd-rate-limit`）无法正常安装或运行。

2. 主机名与 DNS 配置

正确的 DNS 配置对于邮件服务器的信誉度至关重要。

- 主机名 (FQDN)：** 假设使用 `mail.example.com`。
- IP 地址：** 假设为 `1.2.3.4`。

DNS 记录要求：

- A 记录 (正向解析)：** 必须将 `mail.example.com` 解析到 IP 地址 `1.2.3.4`。
- PTR 记录 (反向解析)：** 必须确保 IP 地址 `1.2.3.4` 的反向解析记录指向 `mail.example.com`。这是许多大型邮件服务商（如 Gmail, Outlook）验证发件人身份的关键步骤。

统一域名策略：

建议邮件系统涉及的所有主机名，包括 HELO 主机名、MX 记录、SMTP/IMAP 服务主机名，都统一使用此 FQDN (`mail.example.com`)。

3. SSL/TLS 证书配置

为了确保客户端（如 Thunderbird, Outlook）连接安全且不报错，必须配置有效的 SSL/TLS 证书。

- **工具：** 使用 certbot 工具。
- **证书来源：** 建议使用 Let's Encrypt 提供的免费证书，并配置自动更新功能，以确保证书始终有效。

步骤 (二)：搭建与初始化设置

1. 软件安装

使用 apt 包管理器安装核心邮件传输代理 (MTA)、邮件投递代理 (MDA) 以及安全增强组件。

```
# 安装 Postfix (MTA)
sudo apt install postfix postfix-pcre

# 安装 Dovecot (IMAP/POP3/LMTP)
sudo apt install dovecot-core dovecot-imapd dovecot-lmtpd

# 安装 Dovecot 邮件过滤/管理插件
sudo apt install dovecot-sieve dovecot-managesieved

# 安装 SPF 策略检查
sudo apt install postfix-policyd-spf-python

# 安装速率限制策略服务（确保系统为 Ubuntu 22.04 或更低）
sudo apt install policyd-rate-limit

# 安装 OpenDKIM (DKIM 签名)
sudo apt install opendkim opendkim-tools
```

2. Postfix 与 Dovecot 虚拟用户/目录设置

为虚拟邮箱用户创建专用的目录和系统用户/组，以隔离权限和存储邮件。

```
# 创建虚拟邮箱存储根目录
sudo mkdir -p /var/mail/vhosts/

# 创建 vmail 组和用户
sudo groupadd -g 5000 vmail
sudo useradd -r -g vmail -u 5000 vmail -d /var/mail/vhosts -c "virtual mail user"

# 设置目录权限
sudo chown -R vmail:vmail /var/mail/vhosts/
```

3. OpenDKIM 初始化设置

OpenDKIM 需要特定的权限和目录结构才能与 Postfix 协同工作。

```
# 将 postfix 用户添加到 opendkim 组, 以便 Postfix 可以访问 DKIM 套接字
sudo gpasswd -a postfix opendkim

# 创建 OpenDKIM 配置目录和密钥存储目录
sudo mkdir /etc/opendkim
sudo mkdir /etc/opendkim/keys

# 设置所有权
sudo chown -R opendkim:opendkim /etc/opendkim

# 限制密钥目录权限, 防止非授权访问
sudo chmod go-rw /etc/opendkim/keys

# 创建 Postfix 用于 OpenDKIM 交互的 spool 目录
sudo mkdir /var/spool/postfix/opendkim
sudo chown opendkim:postfix /var/spool/postfix/opendkim
```

4. Postfix 查找表文件创建

创建 Postfix 需要的查找表 (maps) 文件。这些文件通常是纯文本文件, 通过 postmap 命令转换为 Postfix 可识别的数据库格式 (.db) 。

```
# 创建必要的查找表文件 (注意: 这些文件最终需要填充内容)
sudo touch /etc/postfix/virtual_alias_domains
sudo touch /etc/postfix/virtual_alias_maps
sudo touch /etc/postfix/virtual_mailbox_domains
sudo touch /etc/postfix/header_checks_submission
sudo touch /etc/postfix/sender-access
sudo touch /etc/postfix/sender-regex
sudo touch /etc/postfix/controlled_envelope_senders

# 初始化部分查找表数据库文件
sudo postmap /etc/postfix/virtual_alias_maps
sudo postmap /etc/postfix/sender-access
sudo postmap /etc/postfix/controlled_envelope_senders
```

关键查找表文件作用说明:

文件名	作用	备注
virtual_mailbox_domains	定义邮件系统负责接收邮件的主域名列表。	必须提供。
virtual_alias_domains	定义邮件系统负责处理别名映射的域名列表。	可选。

文件名	作用	备注
virtual_alias_maps	定义邮箱地址的别名映射关系。	可选。
header_checks_submission	定义在邮件提交阶段（发送时）对邮件头进行检查和执行相应动作的规则。	常用于移除发送者 IP 等敏感信息。
sender-access	基于 SMTP 级别，拒绝特定发件人地址或域名的访问。	基于精确匹配。
sender-regex	基于 SMTP 级别，使用正则表达式拒绝特定发件人地址或域名的访问。	基于正则表达式匹配。
controlled_envelope_senders	SASL 授权映射表。定义哪些邮件地址被授权使用特定的 SASL 用户进行发信。	用于限制发信权限，防止滥用。

步骤 (三)：配置与服务启动

正确配置邮件系统是一项耗费精力的工作，涉及到数百个参数的调整。为了实现快速部署，我们采用复制已知稳定配置文件的策略。

1. 配置文件替换

将一套已配置好的、在生产环境中运行的邮件系统的配置文件，复制并替换掉新安装系统中的对应文件。

涉及的关键配置文件列表：

组件	文件名	描述
Postfix	main.cf	Postfix 的核心配置，定义邮件发送、接收行为和策略。
	master.cf	Postfix 的进程配置，定义服务（如 SMTP, SMTPS, Submission）的启用和运行方式。
	controlled_envelope_senders	SASL 授权映射表（已在步骤二创建，此处指填充内容）。
Dovecot	10-auth.conf	认证配置。
	10-mail.conf	邮件存储路径和格式配置。
	10-master.conf	服务主配置。
	10-ssl.conf	SSL/TLS 配置。

组件	文件名	描述
	15-mailboxes.conf	邮箱结构配置。
	20-imap.conf	IMAP 服务配置。
	20-lmtp.conf	LMTP 服务配置（用于 Dovecot 接收 Postfix 投递的邮件）。
	20-managesieve.conf	邮件过滤服务配置。
	90-quota.conf	配额管理配置。
	auth-passwdfile.conf.ext	密码文件认证扩展配置。
	dovecot-users	虚拟用户列表（如果使用 passwdfile 认证）。
OpenDKIM	opendkim.conf	OpenDKIM 核心配置。

操作： 将上述配置文件复制到 `/etc/postfix/` , `/etc/dovecot/` , `/etc/opendkim/` 等对应目录下, 覆盖默认文件。

2. 服务重启

替换配置后，重启所有相关服务以加载新配置。

```
sudo systemctl restart postfix dovecot opendkim policyd-rate-limit
```

3. DKIM 签名配置与 DNS 发布

为了提高邮件送达率和防止伪造，需要为域名配置 DKIM 签名。

运行 DKIM 管理脚本（假设该脚本已存在并配置好密钥生成路径）：

```
sudo ./dkim-manage.sh example.com
```

该脚本将生成公钥和私钥。私钥由 OpenDKIM 使用，公钥需要发布到域名的 DNS 记录中。

DNS TXT 记录示例：

如果脚本生成的 DKIM selector 是 `sec2025`，则需要添加如下 TXT 记录：

```
主机名: sec2025._domainkey.example.com.  
TTL: 300  
类型: TXT  
值: "v=DKIM1;h=sha256;k=rsa;p=..."（此处为生成的公钥字符串）
```

步骤 (四)：其他事项与优化

1. 完善 DNS 记录

除了 DKIM 记录外，为了确保邮件信誉度，必须配置 SPF 和 DMARC 记录：

- **SPF (Sender Policy Framework)**：定义允许代表您的域名发送邮件的服务器 IP 地址。
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**：结合 SPF 和 DKIM，定义接收方如何处理认证失败的邮件，并提供报告机制。

2. Postfix 核心调整

- **master.cf**：该文件决定了 Postfix 启用或禁用哪些全局服务，例如是否启用 SMTPS (465 端口) 或 Submissions (587 端口)。
- **main.cf**：该文件控制一系列复杂的邮件发送行为、访问控制列表 (ACL) 和组件交互。由于其复杂性，建议依赖步骤三中复制的成熟配置，仅进行必要的域名和路径修改。

3. Dovecot 配置调整

需要仔细调整 Dovecot 的一系列配置，包括：

- **Ports**：确保 IMAP (143/993) 和 POP3 (110/995) 端口正确配置。
- **SSL**：确保证书路径正确，并强制使用安全连接。
- **Auth**：认证机制（如 `auth-passwdfile.conf.ext` 或 SQL 认证）的配置。
- **Sieve/Quota**：邮件过滤规则和用户配额管理。

4. 反垃圾邮件 (Anti-Spam) 策略

即使不安装 Rspamd 或 SpamAssassin 等专业反垃圾邮件软件，Postfix 自带的访问控制语句（定义在 `main.cf` 中）也能提供良好的 Anti-Spam 和 Anti-Abuse 作用。这些控制通常基于发件人、接收人、HELO/EHLO 字符串、客户端 IP 等进行限制。

5. 服务功能验证

必须测试邮件系统的核心功能和安全组件是否正常工作：

1. **收发信测试**：确保内部和外部邮件收发流程畅通。
2. **策略服务验证**：
 - **policyd-rate-limit**：检查速率限制是否生效，防止短时间内大量发送。
 - **policyd-spf**：检查 SPF 策略是否正确验证传入邮件。
3. **DKIM 验证**：检查发送的邮件是否带有有效的 DKIM 签名。

注意： `policyd-rate-limit` 和 `policyd-spf` 通常采用默认配置即可工作。OpenDKIM 作为 Milter 服务，其配置和与 Postfix 的交互（通过 `main.cf` 定义）需要仔细检查。

6. 客户端和 Webmail 接入

如果 SMTP (发送) 和 IMAP (接收) 服务测试正常，则邮件系统基础搭建完成。

最后一步是为用户提供便捷的访问界面。可以安装开源的 Webmail 客户端，例如：

- Roundcube
- SnappyMail
- Squirrelmail

选择合适的 Webmail 客户端，并将其配置指向新搭建的 IMAP/SMTP 服务即可。