Linux邮件服务器架设

> *主要关于CentOS中邮件服务器postfix的设置及邮件服务器相关的原理。*

0x01邮件服务器架设的前提条件

1. 邮件服务器一定要有一个合法注册过的主机名才行。
2. 目前收信端的邮件服务器会针对邮件来源的IP进行反解，而如果你的网络环境是由拨号得来的而非固定的IP，该种IP会被视为垃圾邮件。
3. 需要DNS的MX及A标志。如果没有上游服务器，可以将自己的服务器设置为MX，利用自己当MX服务器。

0x02邮件传输所需要的组件

1. 电子邮件的传输过程示意图

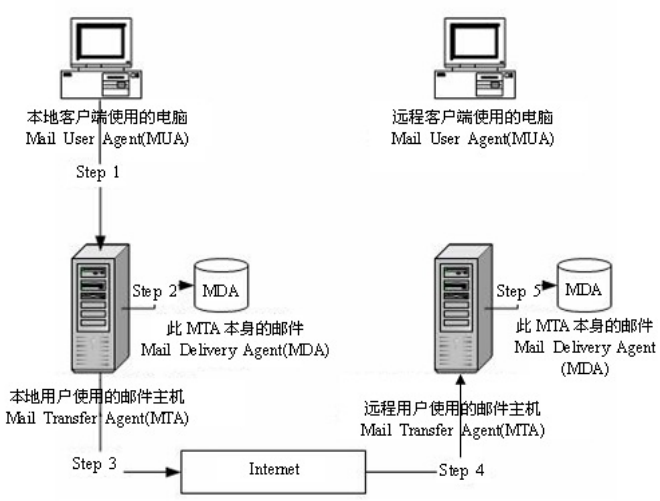

图 20-1　电子邮件从邮件主机寄送信件示意图

2. 相关组件介绍：

> 1. *MUA: 邮件用户代理人。主要的功能是收取邮件主机的电子邮件，以及提供用户浏览与编写邮件。比如雷鸟。*
> 2. *MTA: 邮件发送代理人。主要的功能是接受邮件，使用简单的邮件传送协议（SMTP）；转发邮件。注：我们一般提到的Mail Server就是MTA。严格说来，MTA启示仅是指SMTP这个协议。*
> 3. *MDA: 邮件传送代理人。主要功能是分析由MTA所收到的邮件表头或内容等数据，来决定这封邮件的去向。过滤垃圾邮件；自动回复。注：各主要的MTA程序都有自己的MDA功能。*
> 4. *Mailbox: Linux系统默认的邮箱都是放在/var/spool/mail/邮箱账号中。*

0x03用户收信时服务器端所提供的相关协议：MRA

1. MRA: 用户可以通过MRA服务器提供的邮政服务协议（POP）来接受自己的邮件，也可以通过IMAP协议将自己的邮件保留在邮件主机上面。
2. POP:
   1）MUA通过POP3协议连接到MRA的110端口，并且输入正确的用户名和密码来取得正确的认证和授权。
   2）取得授权后，MRA会前往该用户的Mailbox，取得相应的邮件并发送至MUA中。
   3）当所有的邮件发送完毕后，用户的Mailbox内的数据会被清空。
3. IMAP：这个协议可以将Mailbox的数据存储到你主机上的用户主目录。
4. 要假设一台可以使用MUA进行首发邮件的MTA、MRA服务器，至少需要启动SMTP以及POP3这两个协议才行。
5. SMTP、POP3、IMAP都是明文进行传输的，加密传输需要使用POP3s和IMAPs。

0x04MTA服务器：Postfix基础设定

1. 所需要的软件与软件结构：
   1）CentOS 6.x默认提供了postfix软件，所以不需要再手动进行安装了。
   2）它主要的配置文件都在/etc/postfix文件夹中。

> */etc/postfix/main.cf是主要的postfix的配置文件，几乎所有的配置文件选项都在该文件中完成。*

/etc/postfix/master.cf主要规定了postfix每个程序的工作的参数，这个配置文件默认已经配置好了，不需要再进行配置。
/etc/postfix/access可以设置开发Relay或拒绝来源和目标地址等信息的外部配置文件，需要再main.cf文件中开启。且设置完毕后需要使用postmap来处理成数据库文件。
/etc/aliases作为邮件别名的设置，也可以作为邮件组的设置。

2. postfix程序的使用：

> “

postconf: 查阅postfix的设置数据。
postfix: start/stop check:检查postfix 的相关文件和数据库是否正确 flush:强制将正在邮件队列中的邮件寄出 reload:重新载入配置文件。
postalias: postalias hash:/etc/aliases 设置别名数据库。
postcat: 主要用于检查放在queue当中的邮件内容。
postmap: postmap hash:/etc/postfix/access。
postqueue: 用于查看邮件队列中的邮件。postqueue - p。

0x05postfix邮件服务器的设定

22.2.3 一个邮件服务器的设定案例

前面谈到 Mail server 与 DNS 系统有很大的相关性，所以当你想要搭建一台可以连上 Internet 的邮件服务器时，你必须要已经取得合法的Ⓐ与 MX 主机名，而且最好反解也已经向你的 ISP 申请修改设置了，这可是个大前提，不要忽略。在下面的练习当中鸟哥以之前 19 章 DNS 内的设置为依据，主要的参数是这样的：

- 邮件服务器的主要名称为： www.centos.vbird。
- 邮件服务器尚有别名为 linux.centos.vbird 及 ftp.centos.vbird 也可以收发邮件。
- 此邮件服务器已有 MX 设置，直接指向自己（www.centos.vbird）。
- 这个 www.centos.vbird 有个 A 的标志指向 192.168.100.254。

在实际的邮件服务器设置当中，上述的几个标志是很重要的，请自行参考 DNS 章节的介绍。下面就让我们来实际设置 Postfix 服务器。

22.2.4 让 Postfix 可监听 Internet 来收发邮件

在默认的情况下，CentOS 6.x 的 MTA 仅针对本机进行监听，测测看：

```
[root@www ~]# netstat -tlnp | grep :25
Proto Recv-Q Send-Q Local Address   Foreign Address   State    PID/Program name
tcp        0      0 127.0.0.1:25    0.0.0.0:*         LISTEN   3167/master
```

所以如果你要对整个 Internet 开放的话，就需要努力搞定几个简单的设置。而几乎所有的设置你都可以通过 /etc/postfix/main.cf 这个文件搞定。修改前你需要注意的项目有：

- “#”符号是注释的意思。
- 所有设置值以类似变量的设置方法来处理，例如 myhostname = www.centos.vbird，请注意等号的两边要给予空格符，且第一个字符不可以是空白，也就是“my..”要由行首写起。
- 可以使用“$”来延伸使用变量设置，例如 myorigin = $myhostname，会等于 myorigin = www.centos.vbird。
- 如果该变量支持两个以上的数据，则使用空格符来分隔，不过建议使用逗号加空格符来处理。例如：mydestination = $myhostname, $mydomain, linux.centos.vbird，意指 mydestination 支持三个数据内容之意。
- 可使用多行来表示同一个设置值，只要在第一行最后有逗号，且第二行开头为空格符，即可将数据延伸到第二行继续书写（所以上面第二点才说，开头不能留白）。

- **若重复设置某一项目，则以较晚出现的设置值为准！**

要让你的 postfix 可以收发邮件时，你必须要启动的设置数据有下面这些：

myhostname：设置主机名，需使用 FQDN

这个项目在于设置你的主机名，且这个设置值会被后续很多其他的参数所引用，所以必须要设置正确才行。你应该要设置成为完整的主机名。在鸟哥的这个练习当中，应该设置为：myhostname = www.centos.vbird 才对。除了这个设置值之外，还有一个 mydomain 的设置项目，这个项目默认会取 $myhostname 第一个“.”之后的名称。举例来说上头设置完毕后，默认的 mydomain 就是 centos.vbird。你也可以自行设置它。

- **myorigin：发信时所显示的“发信源主机”项目**

  这个项目在设置“邮件头上面的 mail from 的那个地址”，也就是代表本 MTA 传出去的邮件将以此设置值为准。如果你在本机寄信时忘记加上 Mail from 字样的话，那么就以此值为准了。默认这个项目以 $myhostname 为主，例如：myorigin = $myhostname。

- **inet_interfaces：设置 Postfix 的监听接口（极重要）**

  在默认的情况下你的 Postfix 只会监听本机接口的 lo（127.0.0.1）而已，如果你想要监听整个 Internet 的话，请开放成为对外的接口，或者是开放给全部的接口，常见的设置方法为：inet_interfaces = all。由于如果有重复设置项目时，会以最晚出现的设置值为准，所以最好只保留一组 inet_interfaces 的设置。

- **inet_protocols：设置 Postfix 监听 IP 协议**

  默认 CentOS 的 Postfix 会去同时监听 IPv4、IPv6 两个版本的 IP，如果你的网络环境里面仅有 IPv4，那可以直接指定 inet_protocols = ipv4 就会避免看到“ :::1”之类的 IP 出现了。

- **mydestination：设置“能够收信的主机名”（极重要）**

  这个设置项目很重要，因为我们的主机有非常多的名字，那么对方填写的 mail to 到底要写哪个主机名字我们才能将该邮件收下？ 就是在这里规范的。也就是说，你的许多主机名当中，仅有写入这个设置值的名称才能作为 E-mail 的主机地址。在我们这个练习当中这部主机有三个名字，所以写法为： mydestination = $myhostname, localhost, linux.centos.vbird, ftp.centos.vbird。

  如果你想要将此设置值移动到外部文件，那可以使用类似下面的做法：mydestination = /etc/postfix/local-host-names，然后在 local-host-names 里面将可收信的主机名写入即可。一般来说，不建议你额外建立 local-host-names 这个文件，直接写入 main.cf 即可。特别留意的是，**如果你的 DNS 里的设置有 MX 标志的话，那么请将 MX 指向的**

那个主机名一定要写在这个 mydestination 内，否则很容易出现错误信息。一般来说，用户最常发生错误的地方就在这个设置里。

- mynetworks_style ：设置“信任网络”的一项指标

  这个设置值在规定与主机在同一个网络的可信任客户端。举例来说，鸟哥的主机 IP 是 192.168.100.254，如果我相信整个局域网络内（192.168.100.0/24）的用户的话，那我可规定此设置值为 subnet。不过，一般来说，因为下面的 mynetworks 会取代这个设置值，所以不设置也没有关系。如果要设置的话，最好设置成为 host 即可（亦即仅信任这部 MTA 主机而已）。

- mynetworks ：规定信任的客户端（极重要）

  你的 MTA 能不能帮忙进行 Relay 与这个设置值有很大关系。举例来说，当我要开放本机与内部网络的 IP 时，就可以这样进行设置：mynetworks = 127.0.0.0/8, 192.168.100.0/24。如果你想要以 /etc/postfix/access 这个文件来控制 relay 的用户时，那鸟哥可以建议你将上述的数据改写成这样：mynetworks = 127.0.0.0/8, 192.168.100.0/24, hash:/etc/ postfix/access，然后你只要再建立 access 重整成数据库后，就能够设置 Relay 的用户了。

- relay_domains ：规范可以帮忙 relay 的下一台 MTA 主机地址

  相对于 mynetworks 是针对“信任的客户端”而设置的，这个 relay_domains 则可以视为“针对下游 MTA 服务器”而设置的。举例来说，如果你这台主机是 www.niki.centos.vbird 的 MX 主机时，那你就需要在 relay_domains 设置针对整个 niki.centos.vbird 这个领域的目标邮件进行转发才行。在默认的情况下，这个设置值是 $mydestination。

  需要注意的是，Postfix 默认并不会转发 MX 主机的邮件，即如果你有两台主机，一台是上游的 MTAup，一台是下游的 MTAdown，而 MTAdown 规范的 MX 主机是 MTAup，由 22.1.2 节谈到的 DNS 的 MX 设置值与邮件传递方向，我们知道任何想要寄给 MTAdown 主机的邮件，都会先经过 MTAup 来转发才行。此时如果那台 MTAup 没有开启帮 MTAdown 进行 Relay 的权限时，那么任何传给 MTAdown 的邮件将全部都被 MTAup 所退回，从此 MTAdown 就无法收到任何邮件了。

  请你再想一想上一段的说明，因为如果你在大公司服务而且你的公司上、下游均有 Mail server 时，并且也已经设置 MX 的状况下，这个 relay_domains 就很重要。上游的 MTA 主机必须要启动这个设置。一般来说除非你是某台 MTA 主机的 MX 源头，否则这个设置项目可以忽略不设置。而如果你想要帮你的客户端转发邮件到某台特定的 MTA 主机时，这个设置项目也是可以设置的。一般情况下保留默认值即可。

- alias_maps ：设置邮件别名

  这是设置邮件别名的设置项目，只要指定到正确的文件去即可，这个设置值可以保留

默认值。

在了解上述的设置后，以鸟哥的范例来看，鸟哥对更动过或注明重要的设置值以及相关文件是这样处理的：

```
[root@www ~]# vim /etc/postfix/main.cf
myhostname = www.centos.vbird                    <==约在第  77 行
myorigin = $myhostname                           <==约在第  99 行
inet_interfaces = all                            <==约在第 114 行，117 行要注释掉
inet_protocols = ipv4                            <==约在第 120 行
mydestination = $myhostname, localhost.$mydomain, localhost,
  linux.centos.vbird, ftp.centos.vbird <==约在第 165,166 行
mynetworks = 127.0.0.0/8, 192.168.100.0/24, hash:/etc/postfix/access <==约在 269
relay_domains = $mydestination                   <==约在第 299 行
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases               <==约在第 389, 400 行
# 其他的设置值就先保留默认值即可

[root@www ~]# postmap hash:/etc/postfix/access
[root@www ~]# postalias hash:/etc/aliases
```

因为在 main.cf 当中我们额外加入了两个外部配置文件（mynetworks 及 alias_maps）所以才会额外进行 postmap 及 postalias。然后就准备来启动了。你可以这样处理：

```
# 1. 先检查配置文件的语法是否有错误
[root@www ~]# /etc/init.d/postfix check   <==没有信息，表示没有问题

# 2. 启动与观察 port number
[root@www ~]# /etc/init.d/postfix restart
[root@www ~]# netstat -tlunp | grep ':25'
Proto Recv-Q Send-Q Local Address  Foreign Address   State   PID/Program n
tcp        0      0 0.0.0.0:25     0.0.0.0:*         LISTEN  13697/maste
```

22.3 MRA 服务器： dovecot 设定

除非你想要在 MTA 上架设 Webmail，否则，你的 MTA 收下了邮件，你总需要
去收信的。那么收信要用的是哪个通信协议？就是 22.1.4 节里面谈到的 POP3 以
这就是所谓的 MRA 服务器。CentOS 6.x 使用的是 dovecot 这个软件来实现 MRA
信协议的。但由于 POP3/IMAP 还有数据加密的版本，下面我们就依据是否加密（S
置 dovecot。

22.3.1 基础的 POP3/IMAP 设定

启动单纯的 POP3/IMAP 是很简单的，你需要先确定已经安装了 dovecot 这个
这个软件的配置文件只有一个，就是 /etc/dovecot/dovecot.conf。我们仅要启动 PO
而已，所以这样设置即可：

```
[root@www ~]# yum install dovecot
[root@www ~]# vim /etc/dovecot/dovecot.conf
# 找到下面这一行，大约是在第 25 行左右的地方，复制新增一行内容如下：
#protocols = imap pop3 lmtp
protocols = imap pop3

[root@www ~]# vim /etc/dovecot/conf.d/10-ssl.conf
ssl = no   <==将第 6 行改成这样
```