

目录结构

| | |
|------------------------------------------|------------------|
| 一、TurboMail 邮件系统环境准备 | 2 |
| 1、网络拓扑图..... | 2 |
| 2、硬件环境要求 | 2 |
| 3、带宽计算方法 | 3 |
| 二、Linux/unix 下的安装..... | 4 |
| 1、获取软件安装包 | 4 |
| 2、安装步骤 | 4 |
| 3、检查服务是否正常启动 | 5 |
| 4、Turbomail 服务关闭操作 | 6 |
| 三、安装完 TurboMail 邮件系统后的初始化设置..... | 7 |
| 1、进入“域管理”，添加域名， | 7 |
| 2、进入“系统设置” --- “一般参数” | 8 |
| 3、进入“系统设置” --- “smtp 服务” | 9 |
| 4、进入“系统设置” --- “投递服务” | 11 |
| 5、进入“系统设置” --- “POP3 服务” | 12 |
| 6、进入“系统设置” --- “WebMail 参数” | 12 |
| 7、进入“反垃圾/反病毒” --- “反垃圾引擎设置” | 13 |
| 8、进入“反垃圾/反病毒” --- “ClamAV 反病毒引擎设置” | 错误！未定义书签。 |
| 9、进入“反垃圾/反病毒” --- “过滤邮件摘要设置设置” | 15 |
| 四、Clamav 反病毒引擎 linux 下的安装 | 15 |

一、TurboMail 邮件系统环境准备

TurboMail 邮件系统支持公开下载测试，官网所发布的版本为 V4.3.0 。

1、网络拓扑图

此部署模式为单机部署模式



2、硬件环境要求

用户数：5000 个

| | |
|------|------------------------------------------------------------|
| 操作系统 | linux 操作系统 |
| 硬件配置 | CPU：二个四核处理器 内存：8G 以上 硬盘：1.25TB (raid5) 网卡：1 块千兆网卡 |

硬盘空间计算方法：每个用户容量为 1GB

| 参数项目 | 参数值 | 编号 |
|---------------|-----|----|
| 每用户存储量 | 1 G | A |
| 用户平均存储率（经验值） | 20% | B |
| 系统存储率(Raid 5) | 80% | D |

| 计算项目 | 公式 | 计算值 | 编号 |
|-----------|-----|------|----|
| 每用户平均存储需求 | A*B | 200M | C |
| 每用户存储需求 | C/D | 250M | E |

| 用户数量 | 邮件容量 | 总和 |
|------|-------|----------|
| 5000 | 250MB | 约 1.25 T |

5000 用户的硬盘容量约需要 1.25TB-2TB。

3、带宽计算方法

Turbomail 邮件系统 5000 用户配置说明

（根据每用户每天收发 20 封 100K 邮件计算）

1. SMTP/POP3 请求：

$100K \text{ (邮件)} * 20 \text{ 封} * 5000 \text{ (用户)} = 10\text{Gbyte} = 80\text{Gbit} / 86400 (24 \text{ 小时} * 60 \text{ 分钟} * 60 \text{ 秒}) = 0.925\text{Mbit} / 0.6 \text{ (以太网带宽利用率)} = 1.542\text{Mbit} * 4 \text{ (带宽峰值比例)} = 6.168\text{M}$ 。

2. WEB MAIL 请求：

$100K * 20 \text{ 封} * \text{(页面请求)} * 1500 \text{ 用户 (实际通过 WEB 方式访问比例 } 3/10) = 3\text{Gbyte} = 24\text{Gbit} / 86400 (24 \text{ 小时} * 60 \text{ 分钟} * 60 \text{ 秒}) = 0.278\text{Mbit} / 0.6 \text{ (以太网带宽利用率)} = 0.463\text{M} * 4 \text{ (带宽峰值比例)} = 1.85\text{M}$ 。

3. 建议：

5000 用户 Internet 接入带宽为 $6.168\text{M} + 1.85\text{M} = 8.018\text{M}$

二、Linux/unix 下的安装

1、获取软件安装包

点击 <http://www.turbomail.org/d1.html>，选择版本，点击下载。安装包的大小大概为 100M 左右。

```
#wget www.turbomail.org/turbomail\_linux\_x86\_430.tgz
```

2、安装步骤

2.1 安装 linux 前磁盘分区没有特别要求，但至少有一个存放邮件的分区要大些。如果 Turbomail 如果安装在 /home 分区下，/home 分区要至少 10G 以上。

2.2 安装需要以 root 用户登陆，下载 TurboMail 安装包到跟目录下，依次输入如下命令：

1) 解压 turbomail 安装包

```
#tar -zxvf turbomail_linux_x86_xxx.tgz
```

2) 启动 turbomail 服务

```
#cd /turbomail  
#nohup ./safestart.sh &  
#cd /turbomail/web/bin/  
#./startup.sh
```

3) 修改启动脚本/etc/rc.d/rc.local 使邮件服务器开机自动启动 加入以下几行：

```
#!/turbomail/starttm.sh &  
#!/turbomail/web/bin/startup.sh &  
#!/turbomail/safestart.sh &
```

Turbomail 如果不是安装在 /turbomail 目录下，请一定要修改 starttm.sh、safestart.sh、startup.sh、三个启动脚本文件中的路径。一定要设为绝对路径。

举例说明：如果 Turbomail 安装在 /home/turbomail

- 1) 修改 Turbomail/starttm.sh : 该脚本主要用于启动 Turbomail 核心服务 (smtp、pop3、imap 服务)。

```
TURBOMAIL_ROOT=/home/turbomail
```

- 2) 修改 turbomail/safestart.sh : 该脚本主要监控 Turbomail 核心服务进程。

```
cd /home/turbomail
```

- 3) 修改 web/bin/startup.sh : 该脚本主要启动 Turbomail web 服务, 即 webmail 和 webadmin。

```
JAVA_HOME="/home/turbomail/jdk"
```

- 4) 相应的 /etc/rc.d/rc.local 也要改为:

```
/home/turbomail/starttm.sh &  
  
/home/turbomail/web/bin/startup.sh &  
  
/home/turbomail/safestart.sh &
```

3、检查服务是否正常启动

- 1) 检查 smtp、pop3 服务是否正常启动

可以在命令行输入: #telnet localhost 25

如果显示: 220 Turbomail SMTP Service ready

说明 smtp 服务启动成功, 如果返回的不是这个信息, 可能有其它 smtp 服务已经占用的 25 号端口, 请先停止其它 smtp 服务。比较常见的是 sendmail 服务默认都是启动的, 可以用:

```
#ps -ef | grep sendmail #查看 sendmail 进程
```

```
#kill -9 进程号 (此进程号为上步所查看 sendmail 服务的进程号)
```

关闭 sendmail 服务。

杀掉系统自带的 sendmail 服务后, 在重新启动 turbomail 服务。启动后查看 turbomail 服务是否正常启动:

```
#ps -ef | grep turbomail
```

检查是否有

```
root      7326   7131   0 Aug21 ?          00:00:00 ./turbomail
root      7327   7131   0 Aug21 ?          00:00:00 ./turbomail
root      7328   7131   0 Aug21 ?          00:00:00 ./turbomail
root      7329   7131   0 Aug21 ?          00:00:00 ./turbomail
root      7330   7131   0 Aug21 ?          00:00:00 ./turbomail
root      7331   7131   0 Aug21 ?          00:00:00 ./turbomail
root      7332   7131   0 Aug21 ?          00:00:00 ./turbomail
```

2) 检查 webmail 服务是否正常启动

在命令行, 输入: `#ps -ef | grep java`

如果出现,

```
root      7342     1   0 Aug21 ?          00:01:57 /turbomail/jdk/bin/java -
Djava.awt.headless=true -Djava.endorsed.dirs=/turbomail/web/common/endorsed -
classpath /turbomail/jdk/lib/tools.jar:/turbomail/web/bin/bootstrap.jar:/
turbomail/web/bin/commons-logging-api.jar -Dcatalina.base=/turbomail/web -
Dcatalina.home=/turbomail/web -Djava.io.tmpdir=/turbomail/web/temp
org.apache.catalina.startup.Bootstrap start
```

说明 Turbomail web 服务进程已经启动。

这些是启动的服务进程, 如果没有, 请检查 `starttm.sh` 脚本中 `TURBOMAIL_ROOT` 路径设置是否正确, 或者查看 linux 自带的防火墙是否关闭, 若是没有关闭请关闭防火墙。

4、Turbomail 服务关闭操作

1) Mail 服务的关闭方法: 查看 turbomail 进程然后 kill 其进程, 若服务启动了, 将会有很多 turbomail 的进程, 杀掉进程的时候只需要 kill 第一个即可,

首先 `#ps -ef | grep safe` 查看一个 `safestart.sh` 的进程, 然后 `kill -9 进程号`, 杀毒 `safestart.sh` 的进程, 然后再进入 turbomail 的安装目录执行命令 `./shutdown.sh` 关闭 mail 服务。

2) webmail 服务的关闭方法: 查看 java 进程, 然后 kill 其进程

```
#ps -ef | grep java
```

```
#kill -9 进程号
```

执行以上两步之后执行命令 `ps -ef | grep turbomail` 确认是否已经完全停止了 TurboMail 服务。

三、安装完 TurboMail 邮件系统后的初始化设置

<http://ip:8080/maintlogin.jsp> 登入系统管理员 (postmaster)

1、进入“域管理”，添加域名，

“是否默认”启动，发送邮件默认保存到“已发送邮件”也启动。其他参数保持默认即可（或者根据具体需求进行调整）。

编辑域信息

其中带*号项，为必填项

普通属性 高级属性 企业信息 用户注册

域 *

存储目录 ▼

HELO命令域名

分配空间 M(负数表示无限制)

分配用户数 (负数表示无限制)

是否默认

状态 ▼

开通日期

域到期时间 (时间格式:YYYY-MM-DD, 不填表示)

接收域信息通知邮件地址

启用短信服务

启动彩信服务

如未收到邮件,则禁用该选项

域日发信数量

域发送邮件频率 格式: 发送次数/间隔秒数, 为空表示不控制

最大可建用户组数

允许域级邮件监控功能

允许域级邮件审批

允许域级黑名单

允许域级白名单

禁用域外发中继

启用域网络硬盘

启用域地址本

最大分配网络硬盘空间 M(负数表示无限制)

启动即时通讯服务

发送邮件默认保存到“已发送邮件”

2、进入“系统设置” --- “一般参数”

设置“自动清除垃圾/病毒事件间隔”一般保留一周的垃圾病毒邮件即可,即 168 小时。设置“清除超过(天)之前的日志”,一般保留一个月的日志即可。启动“邮件状态追踪”功能,此功能启动之后,用户可以在“邮箱服务”----“邮件跟踪”查看自己发送的邮件是否发送成功。其他参数保持默认即可。

| | | |
|------------------------------|-----|------------------------|
| 邮箱大小容量单位 | 000 | K (小于零表示不生成容量信息) |
| 自动清除垃圾/病毒时间间隔 | 168 | 小时 (小于或等于零表示不自动清除) |
| 未清理邮件提示天数 | 0 | 天 (-1 表示不提示) |
| 自动定时发送邮件间隔 | 1 | 分钟 (小于或等于零表示不自动定时发送邮件) |
| 清除postmaster@root超过(小时)之前的邮件 | 0 | 小时 (小于或等于零表示不自动清除) |
| 清除用户超过(小时)之前的邮件 | 0 | 小时 (小于或等于零表示不自动清除) |
| 清除超过(天)之前的日志 | 30 | 天 (小于或等于零表示不自动清除) |
| 清除超过(天)之前的邮件流量日志 | 0 | 天 (小于或等于零表示不自动清除) |
| 系统默认字符集 | GBK | |

邮件存储目录 邮件有五种: 单个目录、多个目录、...

| | | |
|-------------|---------------------------------------------------|-------------------------------------|
| 文本用户缓存时间 | <input type="text" value="0"/> | 秒 (小于或等于零表示无限缓存) |
| 单个日志文件最大值 | <input type="text" value="0"/> | M (单个日志文件不可超过2000M, 小于或等于0表示用2000M) |
| 不使用日志缓冲功能 | <input type="checkbox"/> | |
| 记录邮件流量 | <input checked="" type="checkbox"/> | |
| 记录用户级日志 | <input type="checkbox"/> | |
| 启用邮件状态追踪 | <input checked="" type="checkbox"/> | |
| 用户级过滤规则执行模式 | 默认 (最后) 发送到用户收件箱 <input type="button" value="v"/> | |
| 操作系统字节序 | 最低位字节在最前 <input type="button" value="v"/> | |
| 用户修改接口类 | <input type="text"/> | |

3、进入“系统设置” --- “smtp 服务”

3.1 “启动 smtp 验证” 这个必须启动，防止系统被利用发送垃圾邮件。“启动系统内互发需要 smtp 验证”及“启动系统内不同域强制 smtp 验证”两项可以根据实际情况启动，单域情况下没有必要“启动系统内容不同域强制 smtp 验证”服务。“启动 smtp 强制验证”服务不要启动，此功能应用在 TurboMail 邮件系统上级有专门的反垃圾网关产品的情况下。

系统设置 <==

| | |
|--------------------|-------------------------------------------------------------|
| 服务端口 | 端口列表 |
| SMTP欢迎信息 | <input type="text" value="TurboMail SMTP Service ready"/> |
| 服务器IP | <input type="text"/> |
| 启用SMTP验证 | <input checked="" type="checkbox"/> |
| 启用系统内互发需要SMTP验证 | <input checked="" type="checkbox"/> |
| 启用系统内不同域互发强制SMTP验证 | <input checked="" type="checkbox"/> |
| 启用SMTP强制验证 | <input type="checkbox"/> |
| 不做SMTP验证的IP | <input type="text"/> (多个IP用分号“;”分隔, IP地址可有两种格式: 1 |
| SMTP验证最大尝试次数 | <input type="text" value="5"/> |
| 登录错误间隔延时 | <input type="text" value="0"/> 秒 (小于或等于零表示使用默认值5) |
| 验证失败后锁定时间 | <input type="text" value="0"/> 秒 (小于等于零, 表示不锁定) |
| 最大的SMTP服务线程 | <input type="text" value="64"/> (小于或等于零表示使用默认值1024) |
| 端口最大侦听数 | <input type="text" value="32"/> (最大值为2048, 小于或等于零表示使用默认值64) |
| 最大RCPT命令数 | <input type="text" value="128"/> (小于或等于零表示使用默认值128) |
| 允许非法RCPT命令数 | <input type="text" value="0"/> (小于零表示不控制) |

3.2 设置“最大的 smtp 服务线程”，500 用户或以内建议设置 128 或小于 128 的服务线程。500 用户到 2000 用户建议设置在 128---256 的线程。

3.3 设置“用户异常登录控制”建议设置为“3/1800”，意为半个小时之内达到3个或3个以上的ip通过smtp发送邮件即为发送垃圾邮件，系统会自动锁定发件账号的smtp服务，锁定账号smtp服务后，当前账号就无法通过smtp在发送邮件，需要管理员在“系统监控”---“SMTP盗号发送垃圾邮件帐号列表”这里进行解锁，解锁之前请务必修改密码，密码最好有英文和数字或者更高的复杂度。

| | | |
|------------------|-------------------------------------|-------------------------------------|
| 允许邮件中转 | <input type="checkbox"/> | |
| 连续发送相同邮件控制 | <input type="text"/> | (格式：发送次数/间隔秒数/锁定时间(秒)，为空表示不控制) |
| 用户发件频率 | <input type="text"/> | (格式：发送次数/间隔秒数，为空表示不控制) |
| 防止smtp盗号发送垃圾邮件控制 | <input type="text"/> | (为空不控制，格式：邮件误差大小(字节数)/发送数量/统计周期(秒)) |
| 用户异常登录控制 | <input type="text" value="3/1800"/> | (格式：异地登录次数/间隔秒数，为空表示不控制) |
| 如有不存在收件人，则中断会话 | <input type="checkbox"/> | |
| 允许VRFY命令 | <input type="checkbox"/> | |
| 允许ETRN命令 | <input type="checkbox"/> | |
| 禁止RSET重复发送 | <input type="checkbox"/> | |
| 允许空的发送者 | <input type="checkbox"/> | |

3.4 “DNS服务器”建议设置为当地的dns服务器地址。“一分钟内同一IP访问次数”功能根据实际情况调整，一般情况下默认即可，有特殊情况的加入访问控制白名单。“启用防止伪装发送地址邮件”此功能启动下，此功能的作用是防止其他人伪装系统内的邮件地址发送垃圾邮件。

"mail from"与"from"不一致处理方式

收件人空间不足致处理方式

DNS 服务器 (如果有多个DNS 服务器,可用分号";"分隔)

如果不存在MX记录使用A记录

一分钟内同一IP允许访问次数 (负数表示无限制访问次数)

同一IP最大同时访问数 (负数表示无限制同时访问数)

访问控制白名单(IP) (多个IP用分号";"分隔,IP地址可有两种格式,如:192.168.168.0/255.255.255.0)

启用智能反垃圾IP功能

启用防止伪装发送地址邮件

启用同域发给同域需要验证

记录会话明细

允许nobody@root 邮箱的使用

4、进入“系统设置” --- “投递服务”

启动“记录发件会话明细”，方便之后的日志查询。

投递服务 红色参数表示该参数在服务器重启后才生效

[系统设置 <==](#)

最大投递线程数 (最大值为1024,小于或等于零表示使用默认值32)

投递尝试间隔时间 秒 (小于或等于零表示使用默认值600)

最大投递尝试次数 (小于或等于零表示使用默认值32)

投递间隔增加率 (小于或等于零表示使用默认值16)

外发绑定IP

轮流使用可用IP发送

网络连接超时 (小于或等于零表示使用默认值30)

投递失败是否转入用户Exception文件夹

对中转邮件执行过滤规则

不监控垃圾或病毒邮件

在审核前监控邮件

隐藏来源信息

记录发件会话明细

5、进入“系统设置” --- “POP3 服务”

设置“最大的 POP3 服务线程”，同上设置 SMTP 服务的最大 SMTP 线程方法去设置。启动“记录会话明细”方便事后的日志查询工作。“一分钟内同一 IP 访问次数”功能根据实际情况调整，一般情况下默认即可，有特殊情况的加入访问控制白名单。

| 服务端口 | 端口列表 |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| POP3欢迎信息 | TurboMail POP3 Service ready |
| 登录错误间隔延时 | 5 秒 (小于或等于零表示使用默认值5) |
| POP3验证最大尝试次数 | 5 |
| 验证失败后锁定时间 | 0 秒 (小于等于零, 表示不锁定) |
| 最大的POP3服务线程 | 64 (小于或等于零表示使用默认值1024) |
| 端口最大侦听数 | 64 (最大值为2048, 小于或等于零表示使用默认值64) |
| POP3客户连接超时值 | 30 秒 (小于或等于零表示使用默认值30) |
| 读取命令超时 | 0 秒 (小于或等于零表示不控制) |
| 验证前最大可执行命令数 | 12 (小于或等于零表示不控制) |
| 最大无效命令数 | 32 (小于或等于零表示不控制) |
| POP3服务最小使用内存限额 | -1 K (负数或者零表示不做控制) |
| 一分钟内同一IP允许访问次数 | 32 (负数表示无限制访问次数) |
| 同一IP最大同时访问数 | 32 (负数表示无限制同时访问数) |
| 访问控制白名单 (IP) | <div style="border: 1px solid black; height: 80px; width: 100%;"></div> <p>如:192.168.168.0/255.255.255.0) (多个IP用分号“;”分)</p> |
| POP3接收邮件后强制删除邮件 | <input type="checkbox"/> |
| 记录会话明细 | <input checked="" type="checkbox"/> |
| POP3收件服务执行间隔 | 60 秒 (负数表示不执行) |

6、进入“系统设置” ---- “WebMail 参数”

根据实际需求设置“允许 Web 上传最大的附近大小”。

WebMail参数 **红色参数表示该参数在服务器重起后才生效**

系统设置 <==

| | | |
|-----------------|-----------------------------------|------------------------------|
| 允许Web上传最大的附件大小 | <input type="text" value="5"/> | M (小于零表示不限制大小, 等于零表示不允许上传附件) |
| 会话非活动超时 | <input type="text" value="3600"/> | 秒 (小于或等于零表示使用默认值300) |
| 自动保存草稿间隔 | <input type="text" value="0"/> | 秒 (小于等于0表示不自动保存) |
| WebMail验证最大尝试次数 | <input type="text" value="0"/> | |
| 验证失败后锁定时间 | <input type="text" value="0"/> | 秒 (小于等于零, 表示不锁定) |
| 窗口显示模式 | <input type="text" value="嵌入窗口"/> | |
| 主页面风格 | <input type="text" value="多页面"/> | (仅适用于企业版) |

初始化系统主要就如何一些参数的调整, 其他的默认即可, 然后添加用户即可, 可在“系统设置” --- “用户初始化” 这里下载一个 csv 格式的表格, 通过这个表格批量导入用户。

7、进入“反垃圾/反病毒” ---- “反垃圾引擎设置”

1、启动反垃圾规则库自动升级服务, 配置 TMSPAMCHECK 服务器地址。

TMSPAMCHECK 服务器地址是: spamcheck.turbomail.org

2、启动“外发邮件也使用反垃圾引擎”设置, 设置“外发垃圾邮件锁定数”, 此功能的作用是比如设置“外发垃圾邮件锁定数”为“5”, 即如果系统检测到用户发送 5 封“垃圾邮件”, 系统会自动锁定账号的 smtp 服务, 防止用户被盗密码发送垃圾邮件。

反垃圾引擎设置

启用反垃圾引擎

同域内互发邮件也使用反垃圾引擎

系统内用户互发邮件不经过反垃圾过滤

外发邮件也使用反垃圾引擎

外发垃圾邮件锁定数 小于或等于零表示不锁定

是否发送外发垃圾邮件提示

外发垃圾邮件提示

启动自动更新规则库

更新规则库URL

更新规则库间隔 (小时)

标记为可能垃圾邮件值 (默认值为3, 小于或等于零表示使用默认值3)

标记主题前缀

判定为垃圾邮件值 (默认值为8, 小于或等于零表示使用默认值8)

垃圾邮件主题前缀

判定为系统自动删除值 (默认值为12, 小于或等于零表示使用默认值12)

垃圾邮件处理帐号

特殊规则

收件人不匹配评分

发件人与收件人相同评分

TMSpamCHECK设置

启用 TMSpamCHECK

TMSpamCHECK 服务器地址

TMSpamCHECK 服务器端口

主题分析设置

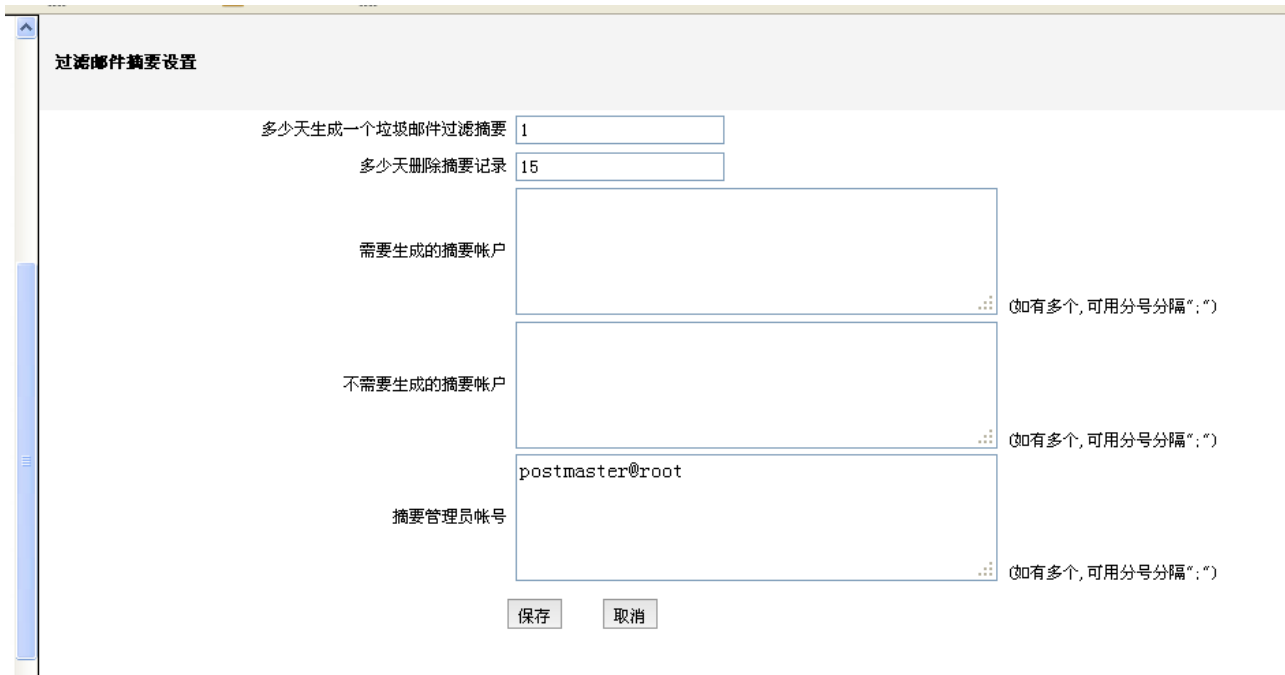
启用主题分析

主题列表 主题列表

SpamFilter 设置

8、进入“反垃圾/反病毒”----“过滤邮件摘要设置设置”

具体设置参照截图，每天用户会生成一封摘要邮件，定时清理 15 天以前的摘要邮件。



四、ClamAV 反病毒引擎 linux 下的安装

1、下载 ClamAV 反病毒

从 <http://packages.sw.be/clamav/> 下载合适的 linux 版本 clamav 版本
查看 linux 版本信息命令

```
cat /etc/redhat-release
```

以 el5 版本的 linux 为例

需要这三个文件 clamav-0.97.1-1.el5.rf.i386.rpm, clamav-db-0.97.1-1.el5.rf.i386.rpm

clamd-0.97.1-1.el5.rf.i386.rpm

2、安装 ClamAV 反病毒

2.1、然后执行以下命令安装

```
rpm -i clamav-db-0.97.1-1.el5.rf.i386.rpm
```

```
rpm -i clamav-0.97.1-1.el5.rf.i386.rpm
```

```
rpm -i clamd-0.97.1-1.el5.rf.i386.rpm
```

2.2、安装后，执行 命令启动 clamav 服务

```
clamd &
```

2.3、修改 turbomail/spool 目录属性

```
cd /turbomail
```

```
chmod -R 777 spool
```

2.4、登入邮件系统管理员，进入反垃圾/反病毒—反病毒引擎设置，启动 ClamAV 服务，如下图所示：

| | |
|------------------|-----------------------------------------------------|
| 启用ClamAV | <input checked="" type="checkbox"/> |
| 记录反病毒明细日志 | <input checked="" type="checkbox"/> |
| 同域内互发邮件也使用ClamAV | <input checked="" type="checkbox"/> |
| 外发邮件也使用ClamAV | <input checked="" type="checkbox"/> |
| 最大判断邮件大小 | <input type="text" value="0"/> 字节 (小于或等于零表示不判断邮件大小) |
| 病毒邮件处理帐号 | <input type="text" value="postmaster@root"/> |
| ClamAV服务器地址 | <input type="text" value="127.0.0.1"/> |
| ClamAV服务器端口 | <input type="text" value="3310"/> |
| 网络超时 | <input type="text" value="60"/> |
| 最大线程数 | <input type="text" value="12"/> |

配置完整后重启 mail 服务 ClamAV 生效，

五、ClamAV 反病毒引擎 Windows 下的安装

1、<http://oss.netfarm.it/clamav/> 下载 clamav 安装包，

- o clamav-win32-0.96.7z VS 2005 32bit build,
- o clamav-amd64-0.96.7z Win64 build, it nee
- o clamav-mingw-0.96.7z MinGW build, no e

2、将下载的 clamav 安装包放到 D 盘下，然后解压

注意：若安装目录不是 D 盘下，比如 E 盘。请修改 clamd.conf 文件，如图所示

```
TCPsocket 3310
MaxThreads 5
LogFile E:\Clamav\clamd.log
DatabaseDirectory E:\clamav\db
LogTime yes
CommandReadTimeout 120
TemporaryDirectory E:\clamav\temp
```

写成 clamav 安装的绝对路径

在 E:\clamav 下新建 db 文件夹，用于存放 clamav 运行后自动下载的病毒库文件。

3、启动 clamav 服务，双机 clamd.exe 即可，若双机启动是报错，如下图所示：



出现此报错说明操作系统缺少 Visual C++ 环境的支持，登入 <http://oss.netfarm.it/clamav/> 下载 clamav 安装需要的环境包，如下图所示：

- o [Redist]
- o Microsoft.VC80.8.0.50727.4053.CRT.x86.7z Archive for embedding x86
- o Microsoft.VC80.8.0.50727.4053.CRT.amd64.7z Archive for embedding amd64
- o vcredist_x86_8.0.50727.4053.exe Installer for x86
- o vcredist_x64_8.0.50727.4053.exe Installer for amd64

下载完毕后，双机安装即可，安装好，在进去 clamav 的安装目录，双击 freshclam.exe 下载病毒库，完

毕后双击 clamd.exe，启动 clamav 服务。

4、登入邮件系统管理员，进入反垃圾/反病毒—反病毒引擎设置，启动 clamav 服务，如下图所示：



The screenshot shows the ClamAV configuration window with the following settings:

| | |
|------------------|-------------------------------------|
| 启用ClamAV | <input checked="" type="checkbox"/> |
| 记录反病毒明细日志 | <input checked="" type="checkbox"/> |
| 同域内互发邮件也使用ClamAV | <input checked="" type="checkbox"/> |
| 外发邮件也使用ClamAV | <input checked="" type="checkbox"/> |
| 最大判断邮件大小 | 0 字节 (小于或等于零表示不判断邮件大小) |
| 病毒邮件处理帐号 | postmaster@root |
| ClamAV服务器地址 | 127.0.0.1 |
| ClamAV服务器端口 | 3310 |
| 网络超时 | 60 |
| 最大线程数 | 12 |

Buttons: 保存 (Save), 取消 (Cancel)

最好重启 mail 服务。

附：

1、加入系统自启动：新建.bat，输入 start d:\clamav\clamd.exe，保存。拉进开始—所有程序—启动文件夹。

2、clamd.exe 后台运行，不显示运行窗口：新建文本文档，输入以下内容：

```
set ws=wscript.createobject("wscript.shell")
```

```
ws.run "clamd.exe /start",0
```

保存为.vbe 文件。