首先这里要明确，搭建服务器，是为了钓鱼发邮件方便。
因为如果用公共邮箱来发很容易被 ban，所以自己搭建比较方便。

但是搭建环境真的是深坑很多。
邮件服务器，听起来很简单，看起来也很简单的一个东西，但其实网上大多数教程都有坑，很浪费时间。

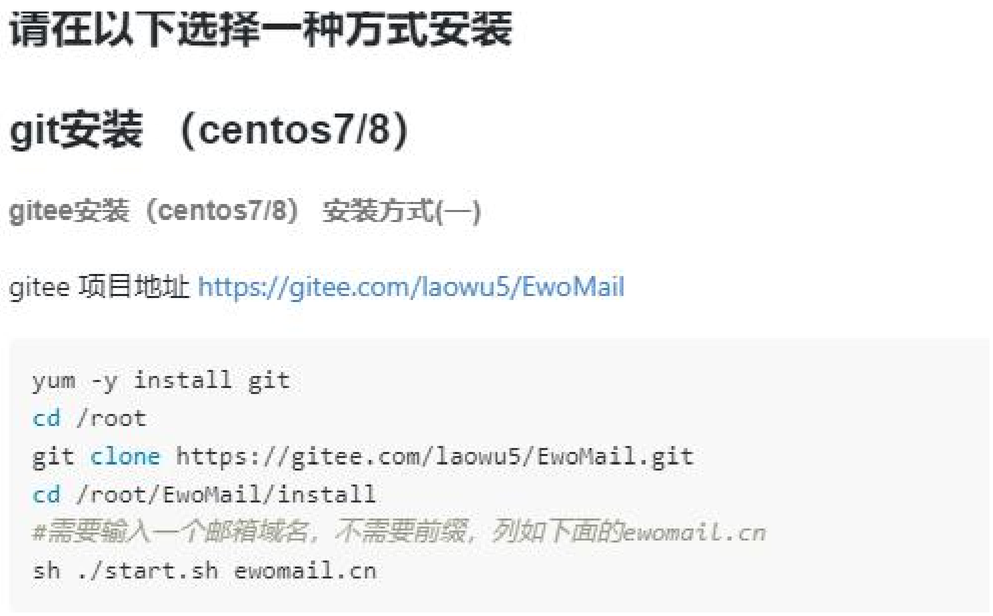
我个人觉得，其实这种搭建环境的教程，有视频素材，一定要去看视频，不要看文章，尤其是早期的文章，深坑特别多。

环境遇到了一个问题，系统报错，然后又去百度，然后又去解决，最后发现还是解决不了，这个过程真的特别折磨，尤其是最后你也不知道你能不能搭成功，整个搞下来，时间被大量浪费。

99%的问题都能够自己在网上能够解决，这句话是没错。
只是看你要花多少时间而已。。。

这里先说坑，再说解决方法
1、centos 搭建 EwoMail 的坑

按照官网文档安装



请在以下选择一种方式安装

git安装 （centos7/8）

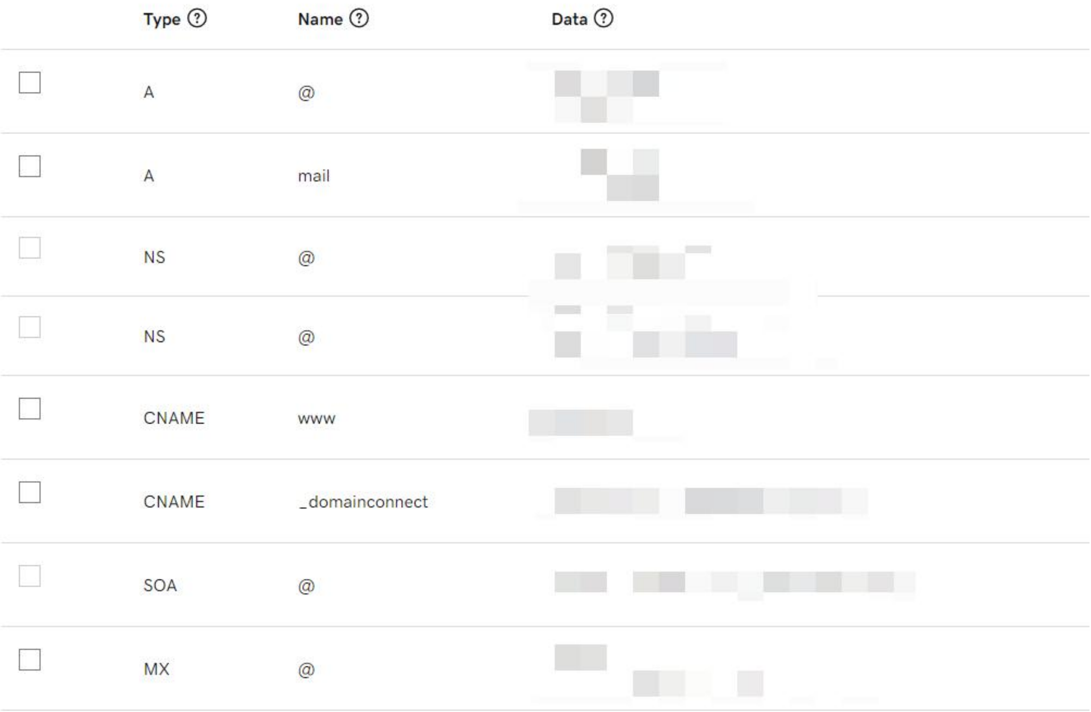
gitee安装（centos7/8） 安装方式(一)

gitee 项目地址 https://gitee.com/laowu5/EwoMail

```
yum -y install git
cd /root
git clone https://gitee.com/laowu5/EwoMail.git
cd /root/EwoMail/install
#需要输入一个邮箱域名，不需要前缀，列如下面的ewomail.cn
sh ./start.sh ewomail.cn
```

这里我用 centos 搭建 EwoMail 就没成功过，因为总是有个 epel 的包下载不成功，难受。
其中换了源，换了 centos 的版本（7/8），换了 vps 的供应商（腾讯云/vultr），依然没有成功，依旧存在哪个 epel 的仓库问题。
这里是直接安装都安装不成功，懒得搞了，拜拜。

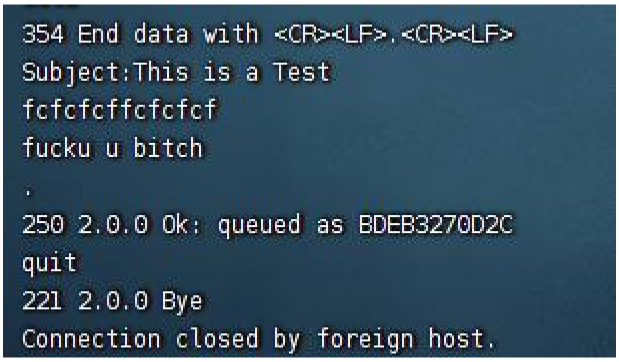
2、关于 Postfix+mailutils 搭建的坑，这里用的 debian11
这里搭建倒是挺成功的，就是收不到邮件，然后我进行排错：
A 记录，mx 记录，都没啥问题



	Type ?	Name ?	Data ?
□	A	@	[redacted]
□	A	mail	[redacted]
□	NS	@	[redacted]
□	NS	@	[redacted]
□	CNAME	www	[redacted]
□	CNAME	_domainconnect	[redacted]
□	SOA	@	[redacted]
□	MX	@	[redacted]

这里排除。

发送过程：



```
354 End data with <CR><LF>.<CR><LF>
Subject:This is a Test
fcfcfcffcfcfcf
fucku u bitch
.
250 2.0.0 Ok: queued as BDEB3270D2C
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

显示没啥问题，但是我的邮箱并没有收到邮件。

整了半天，还是找不到原因，有点累了，不想搞了，想找一套成熟的解决方案。

其间因为搭建环境不顺，就在 github 上浏览，还找到了一些好东西：

https://github.com/ffffffff0x/f8x //红队自动搭建渗透环境的东西

https://github.com/QAX-A-Team/LuWu //qianxin 开源的一套基础环境搭建的东西 看起来不错 就是官方文档不够保姆级 懒得研究了

最终的解决办法

宝塔面板

参考 b 站教程

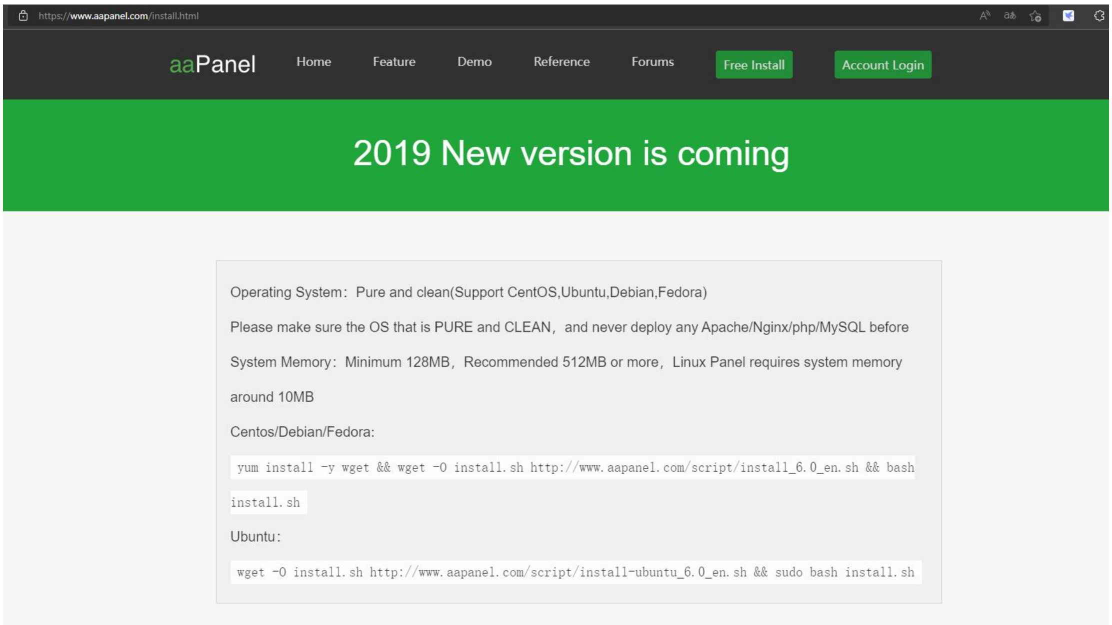
//https://www.bilibili.com/video/BV1ya411C72p/?spm_id_from=333.788

我是一个喜欢偷懒的人，秉承的原则就是花最少的力气，做最多的事情，别人成熟的东西能借鉴就借鉴，实在没办法了再自己想。

邮件服务搭建这个东西，为什么需要我来排错，这东西不是应该很成熟了吗。。。

是很成熟，宝塔点两下就搞定了。。。

宝塔搭建：



2019 New version is coming

Operating System：Pure and clean(Support CentOS,Ubuntu,Debian,Fedora)

Please make sure the OS that is PURE and CLEAN，and never deploy any Apache/Nginx/php/MySQL before

System Memory：Minimum 128MB，Recommended 512MB or more，Linux Panel requires system memory around 10MB

Centos/Debian/Fedora:

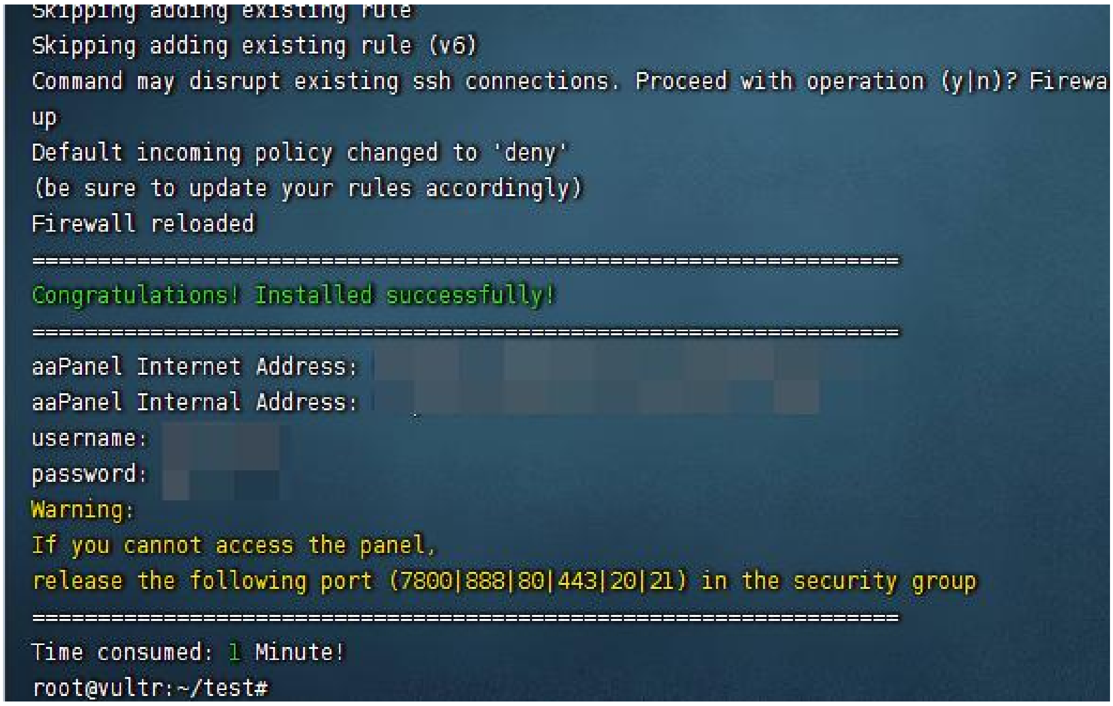
```
yum install -y wget && wget -O install.sh http://www.aapanel.com/script/install_6.0_en.sh && bash install.sh
```

Ubuntu：

```
wget -O install.sh http://www.aapanel.com/script/install-ubuntu_6.0_en.sh && sudo bash install.sh
```

这里使用的是宝塔国际版 aapanel，这里我的 vps 是 debian11，这里根据自己 vps 版本的不同选择不同的命令。

然后安装：

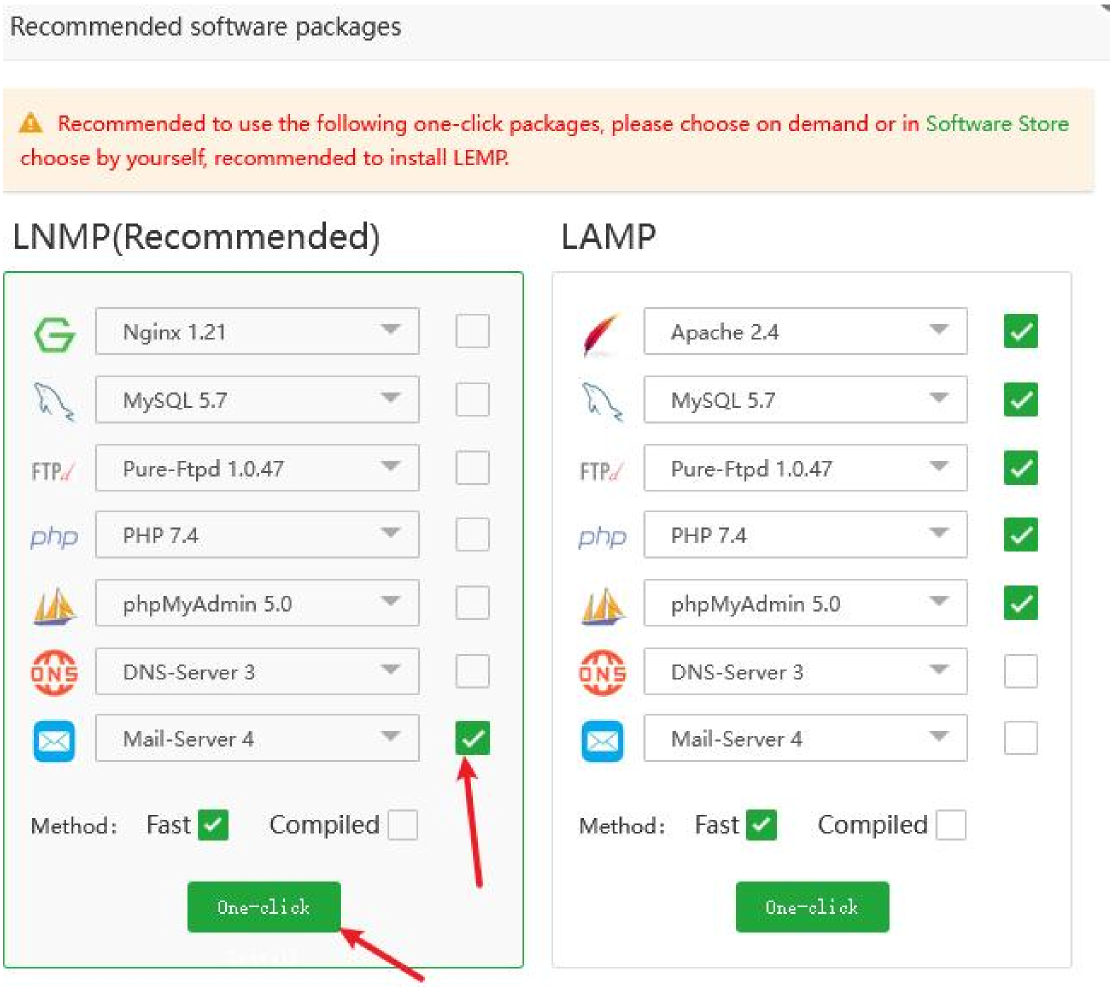


```
Skipping adding existing rule
Skipping adding existing rule (v6)
Command may disrupt existing ssh connections. Proceed with operation (y|n)? Firewa
up
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Firewall reloaded
==================================================================
Congratulations! Installed successfully!
==================================================================
aaPanel Internet Address: [redacted]
aaPanel Internal Address: [redacted]
username: [redacted]
password: [redacted]
Warning:
If you cannot access the panel,
release the following port (7800|888|80|443|20|21) in the security group
==================================================================
Time consumed: 1 Minute!
root@vultr:~/test#
```

这里就是装好了

现在其实宝塔的初始账号密码都是随机密码了，还是有点东西

然后我们进行登录



Recommended software packages

⚠ Recommended to use the following one-click packages, please choose on demand or in Software Store choose by yourself, recommended to install LEMP.

LNMP(Recommended)

Nginx 1.21 □
MySQL 5.7 □
Pure-Ftpd 1.0.47 □
PHP 7.4 □
phpMyAdmin 5.0 □
DNS-Server 3 □
Mail-Server 4 ☑

Method: Fast ☑ Compiled □

One-click

LAMP

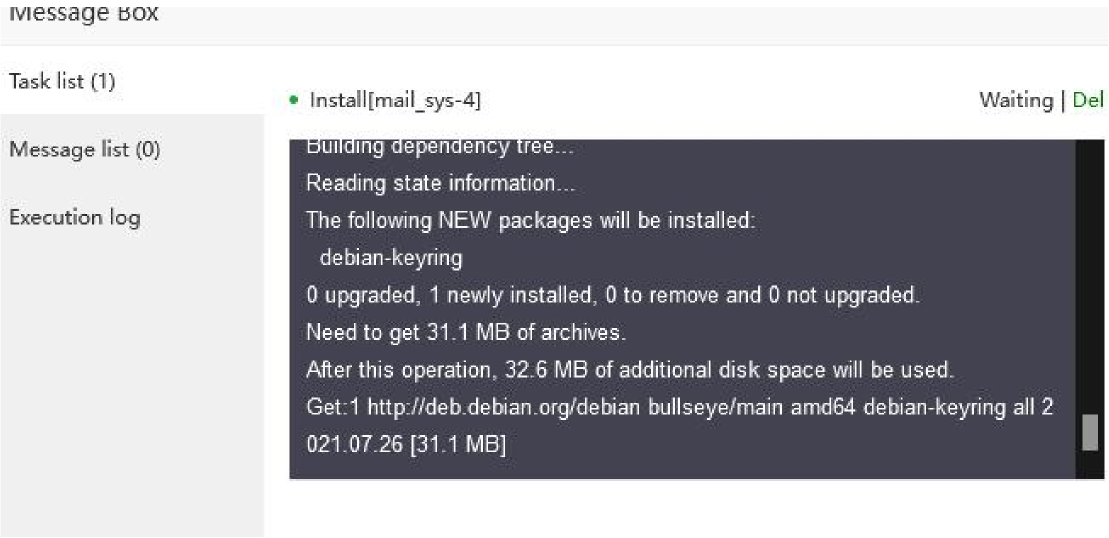
Apache 2.4 ☑
MySQL 5.7 ☑
Pure-Ftpd 1.0.47 ☑
PHP 7.4 ☑
phpMyAdmin 5.0 ☑
DNS-Server 3 □
Mail-Server 4 □

Method: Fast ☑ Compiled □

One-click

登录进来之后会有个弹窗，就勾选一个 mail-Server 即可，因为我们暂时只需要邮件服务。

然后就开始自动安装了。



Message Box

Task list (1)

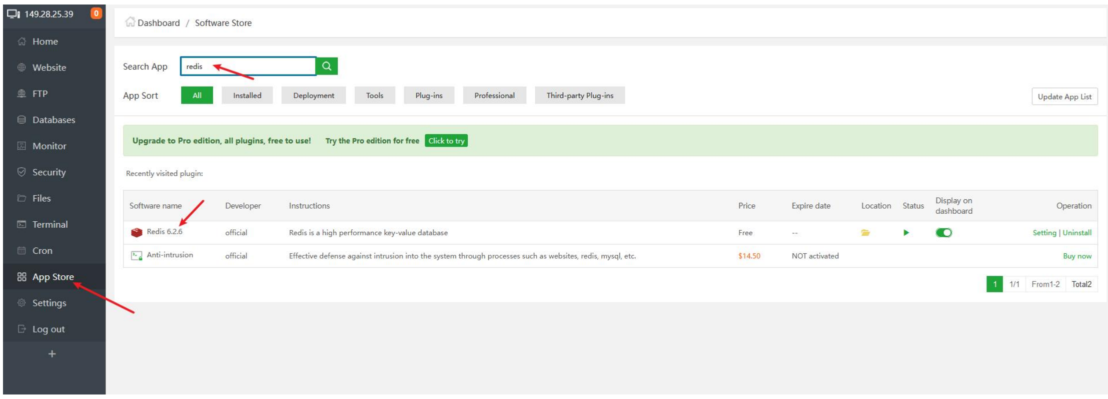
Message list (0)

Execution log

• Install[mail_sys-4] Waiting | Del

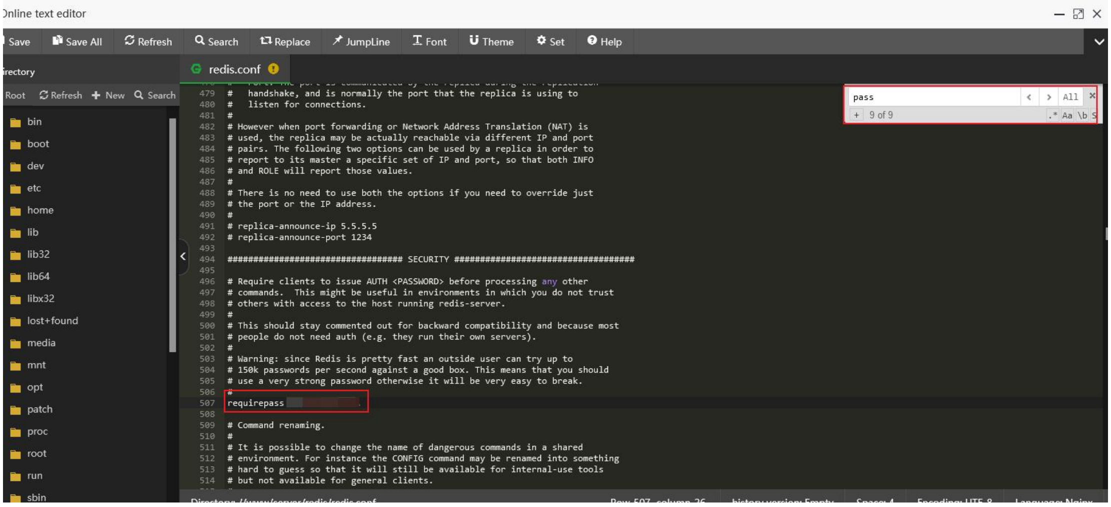
```
Building dependency tree...
Reading state information...
The following NEW packages will be installed:
  debian-keyring
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 31.1 MB of archives.
After this operation, 32.6 MB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 debian-keyring all 2
021.07.26 [31.1 MB]
```

再装一个 redis



Software name	Developer	Instructions	Price	Expire date	Location	Status	Display on dashboard	Operation
Redis 6.2.6	official	Redis is a high performance key-value database	Free	--		▶	●	Setting | Uninstall
Anti-intrusion	official	Effective defense against intrusion into the system through processes such as websites, redis, mysql, etc.	$14.50	NOT activated				Buy now

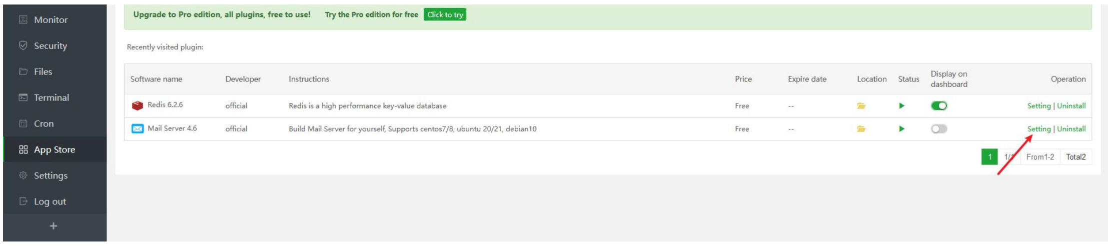
配置 redis，找到 redis.conf 文件，取消未授权访问，设置密码



```
#   handshake, and is normally the port that the replica is using to
#   listen for connections.
#
# However when port forwarding or Network Address Translation (NAT) is
# used, the replica may be actually reachable via different IP and port
# pairs. The following two options can be used by a replica in order to
# report to its master a specific set of IP and port, so that both INFO
# and ROLE will report those values.
#
# There is no need to use both the options if you need to override just
# the port or the IP address.
#
# replica-announce-ip 5.5.5.5
# replica-announce-port 1234

################################## SECURITY ###################################

# Require clients to issue AUTH <PASSWORD> before processing any other
# commands.  This might be useful in environments in which you do not trust
# others with access to the host running redis-server.
#
# This should stay commented out for backward compatibility and because most
# people do not need auth (e.g. they run their own servers).
#
# Warning: since Redis is pretty fast an outside user can try up to
# 150k passwords per second against a good box. This means that you should
# use a very strong password otherwise it will be very easy to break.
#
requirepass [redacted]

# Command renaming.
#
# It is possible to change the name of dangerous commands in a shared
# environment. For instance the CONFIG command may be renamed into something
# hard to guess so that it will still be available for internal-use tools
# but not available for general clients.
```

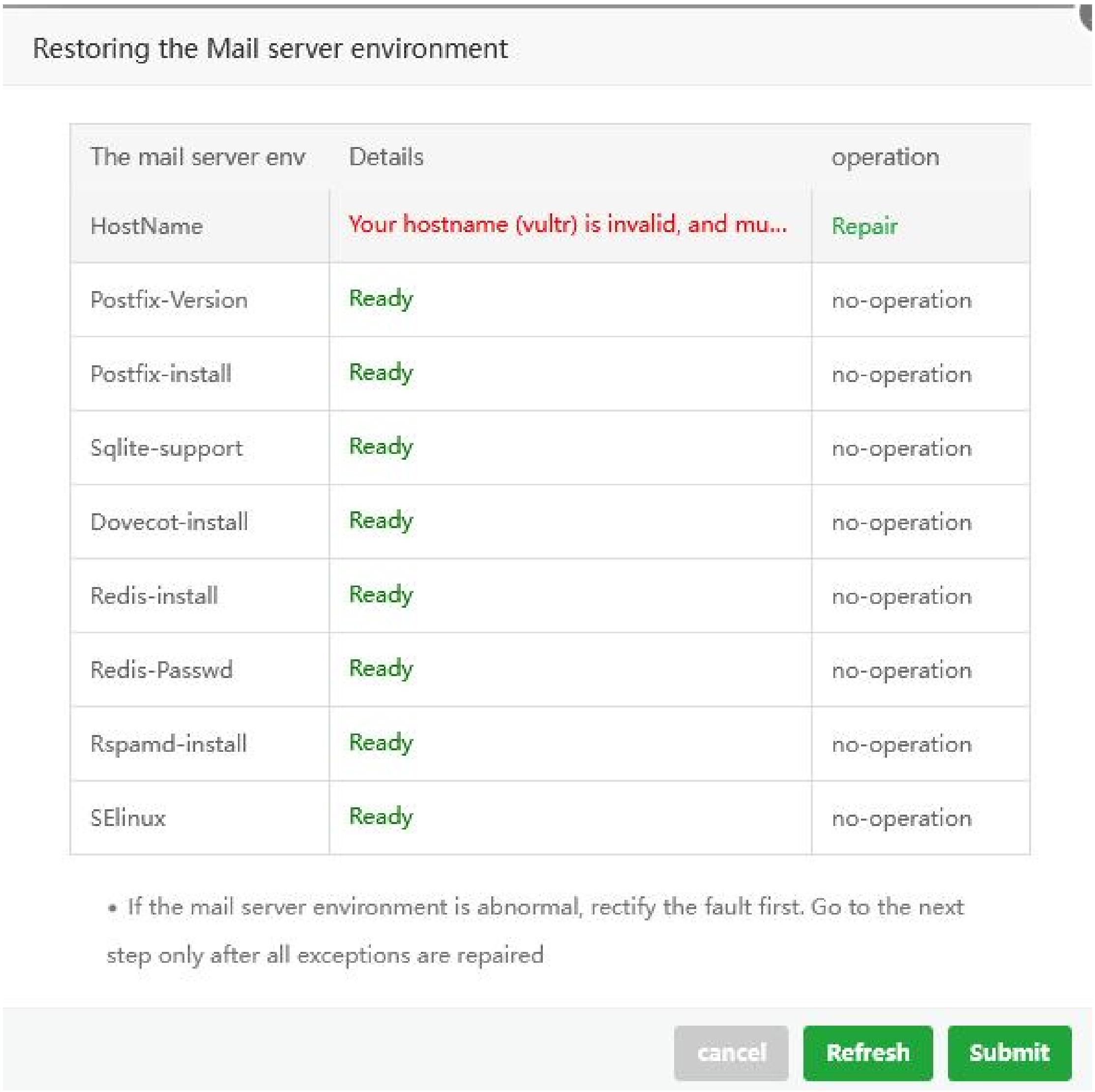
设置完成

配置 mailserver



Software name	Developer	Instructions	Price	Expire date	Location	Status	Display on dashboard	Operation
Redis 6.2.6	official	Redis is a high performance key-value database	Free	--		▶	●	Setting | Uninstall
Mail Server 4.6	official	Build Mail Server for yourself, Supports centos7/8, ubuntu 20/21, debian10	Free	--		▶	○	Setting | Uninstall

把所有的配置项都变成 ready 即可

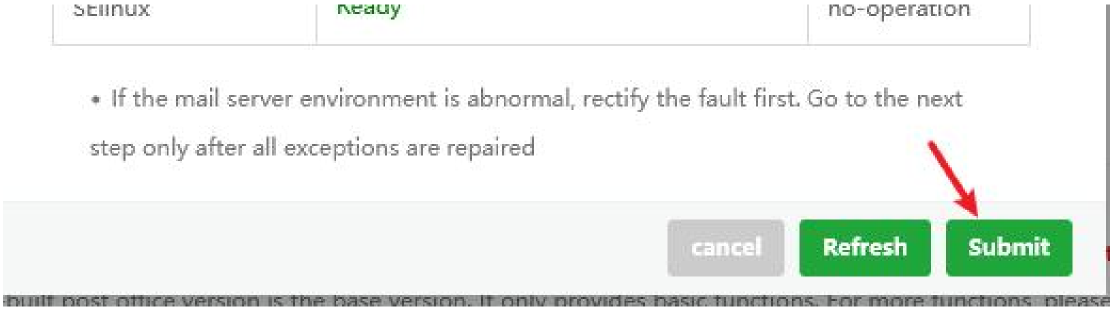


Restoring the Mail server environment

The mail server env	Details	operation
HostName	Your hostname (vultr) is invalid, and mu...	Repair
Postfix-Version	Ready	no-operation
Postfix-install	Ready	no-operation
Sqlite-support	Ready	no-operation
Dovecot-install	Ready	no-operation
Redis-install	Ready	no-operation
Redis-Passwd	Ready	no-operation
Rspamd-install	Ready	no-operation
SElinux	Ready	no-operation

- If the mail server environment is abnormal, rectify the fault first. Go to the next step only after all exceptions are repaired

点击提交

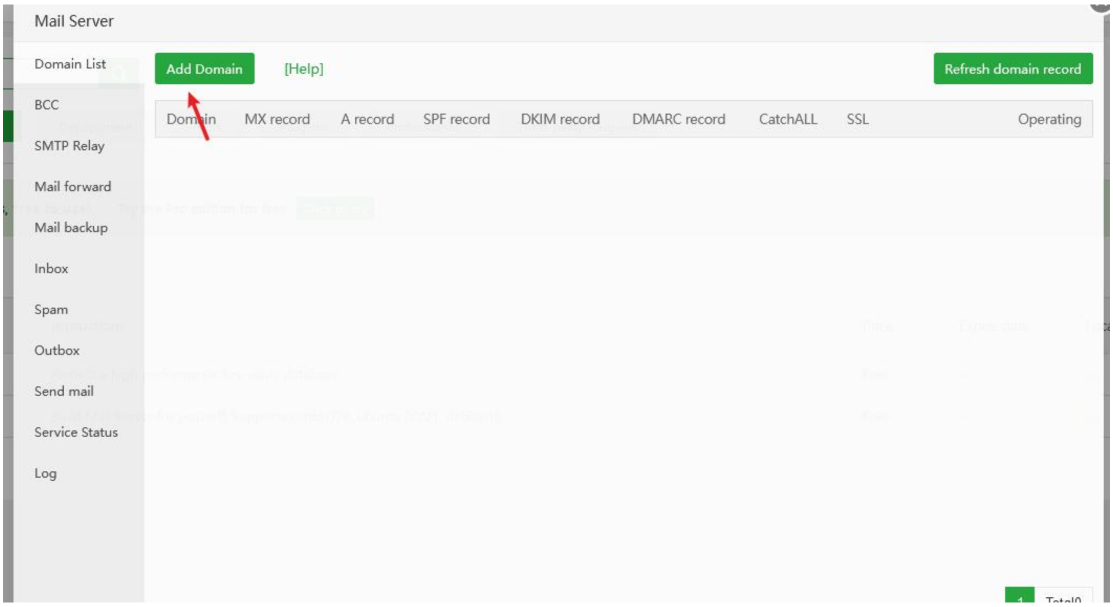


SElinux	Ready	no-operation

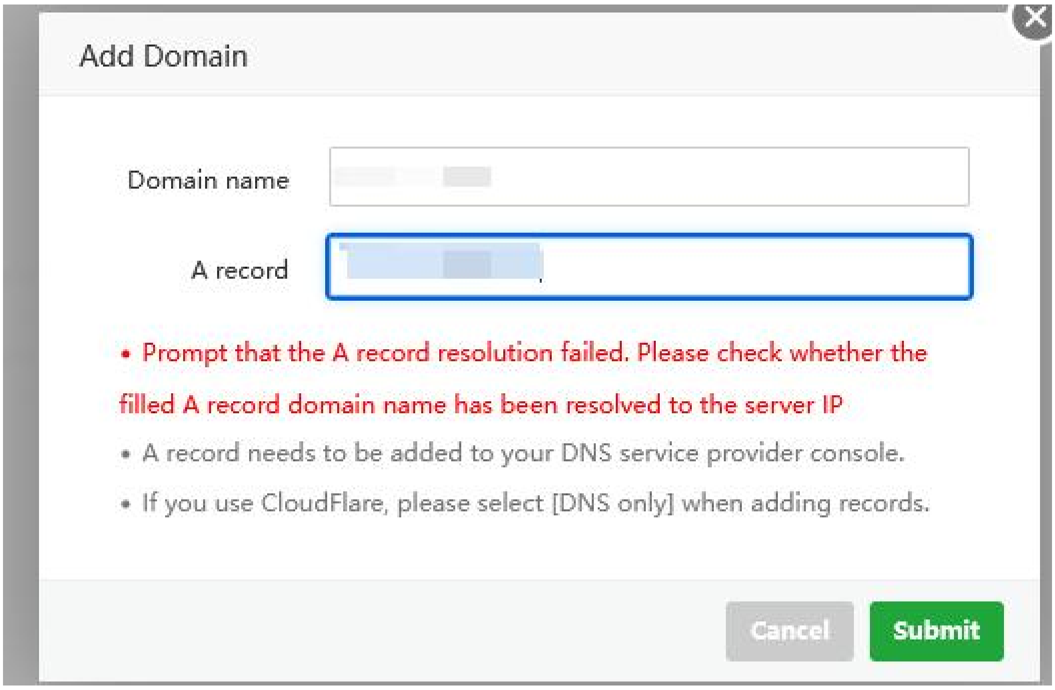
- If the mail server environment is abnormal, rectify the fault first. Go to the next step only after all exceptions are repaired

built post office version is the base version. It only provides basic functions. For more functions, please

完成后，设置域名



填写自己的即可

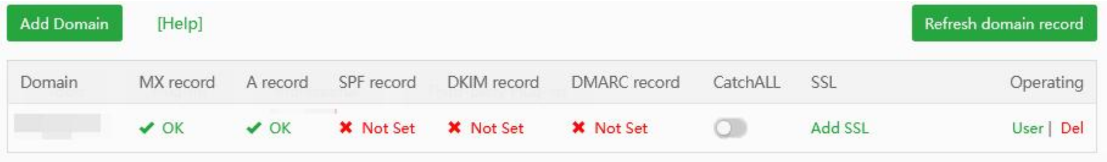


Domain name

A record

- Prompt that the A record resolution failed. Please check whether the filled A record domain name has been resolved to the server IP
- A record needs to be added to your DNS service provider console.
- If you use CloudFlare, please select [DNS only] when adding records.

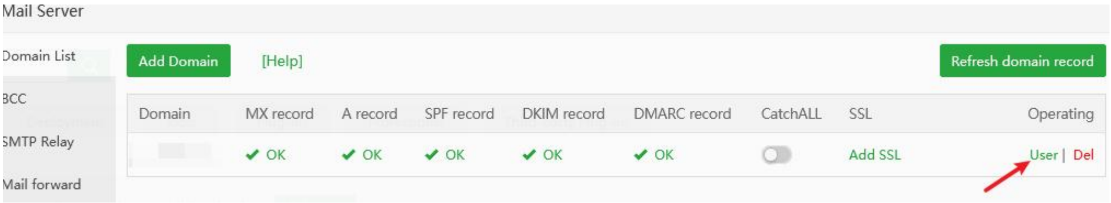
然后进行配置



Domain	MX record	A record	SPF record	DKIM record	DMARC record	CatchALL	SSL	Operating
	✓ OK	✓ OK	✖ Not Set	✖ Not Set	✖ Not Set	○	Add SSL	User | Del

上面的标红项目，都需要变绿才行，那么一个个点击，按照他的要求来完成

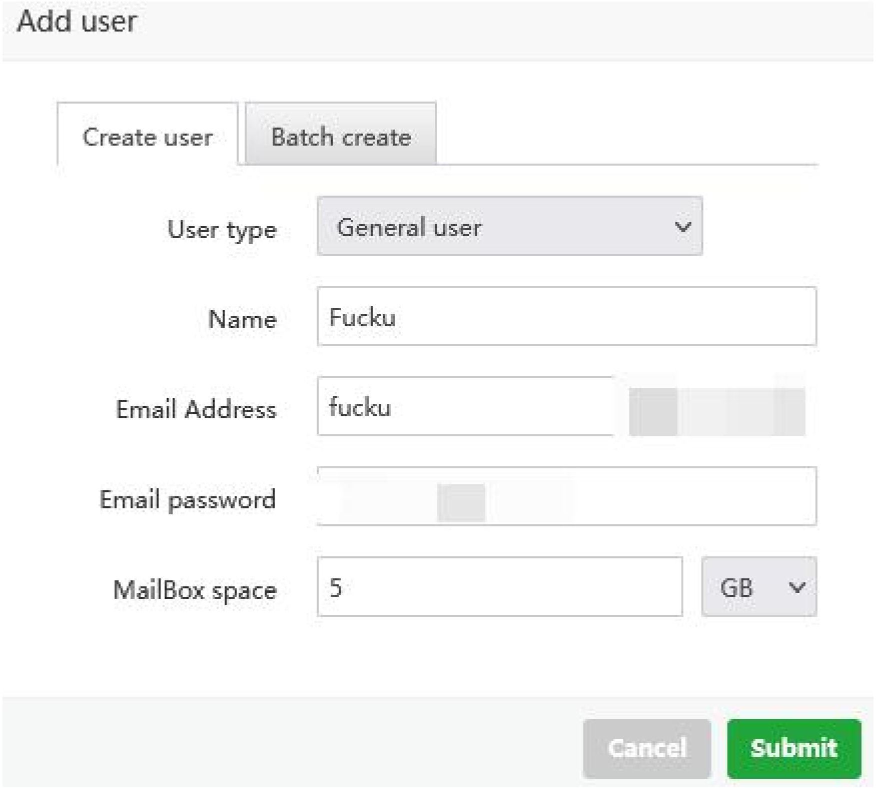
这里已经成功完成



Mail Server

Domain	MX record	A record	SPF record	DKIM record	DMARC record	CatchALL	SSL	Operating
[redacted]	✓ OK	✓ OK	✓ OK	✓ OK	✓ OK	○	Add SSL	User | Del

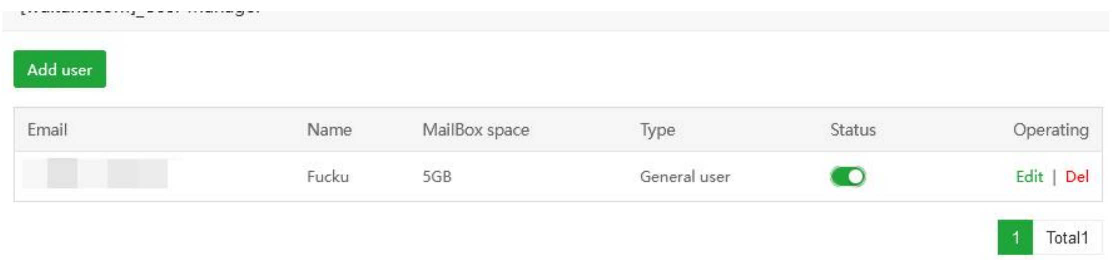
添加用户



Add user

User type	General user
Name	Fucku
Email Address	fucku [redacted]
Email password	[redacted]
MailBox space	5 GB

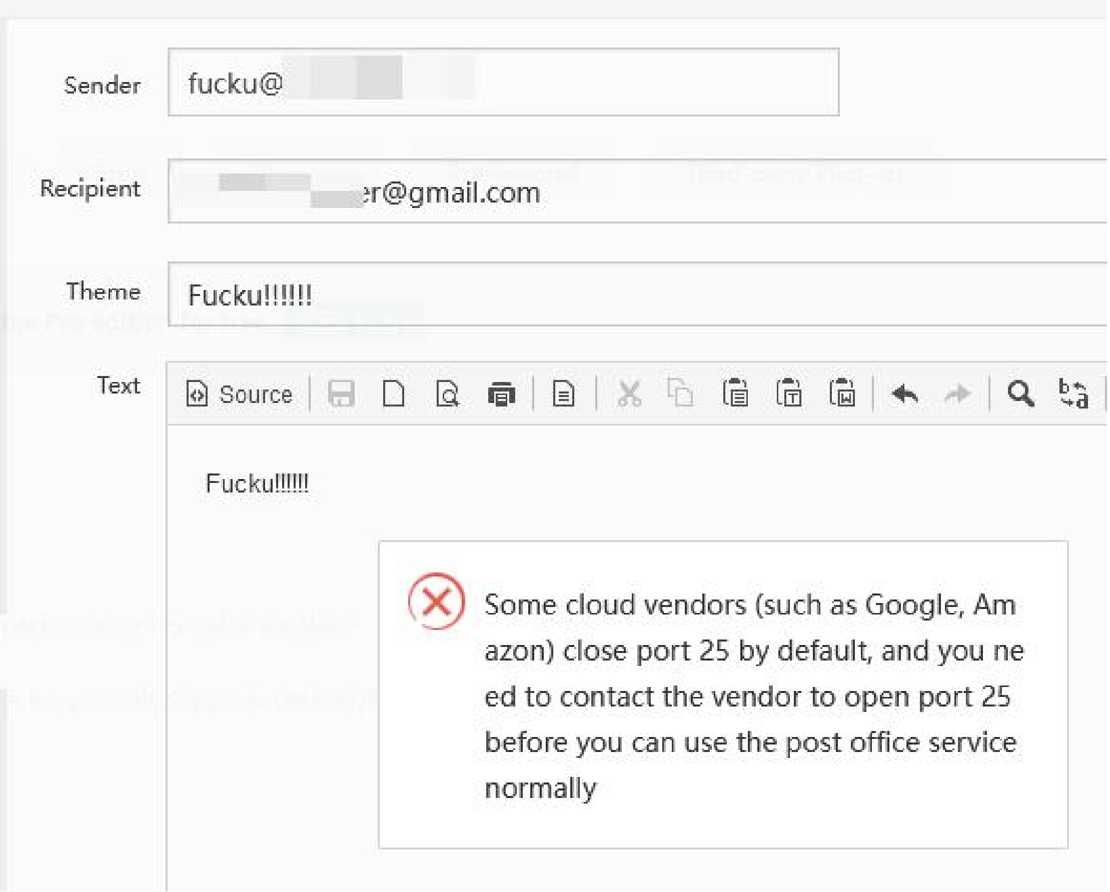
添加成功



Email	Name	MailBox space	Type	Status	Operating
[redacted]	Fucku	5GB	General user	●	Edit | Del

测试邮件发送

然后厂商给我回信了，说要转交技术



Sender fucku@[redacted]

Recipient [redacted]r@gmail.com

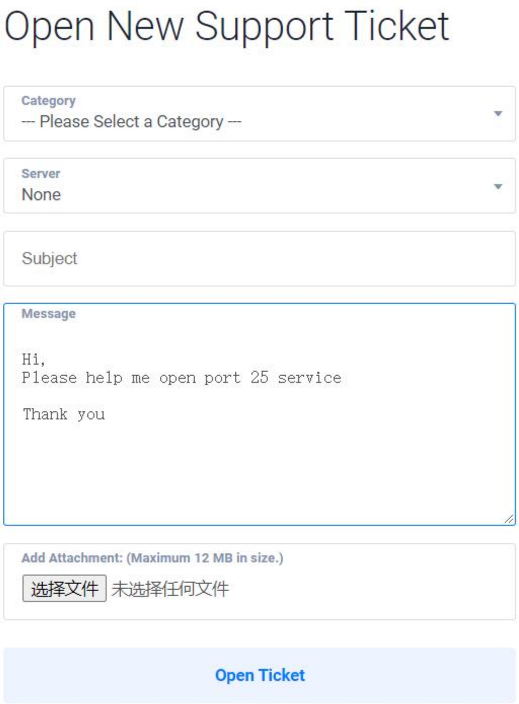
Theme Fucku!!!!!!

Text

Fucku!!!!!!

Some cloud vendors (such as Google, Amazon) close port 25 by default, and you need to contact the vendor to open port 25 before you can use the post office service normally

并不能发出去，因为 25 被关闭了
这里还需要联系你的云服务器厂商发个工单，我这里用的是 vultr



Open New Support Ticket

Category
— Please Select a Category —

Server
None

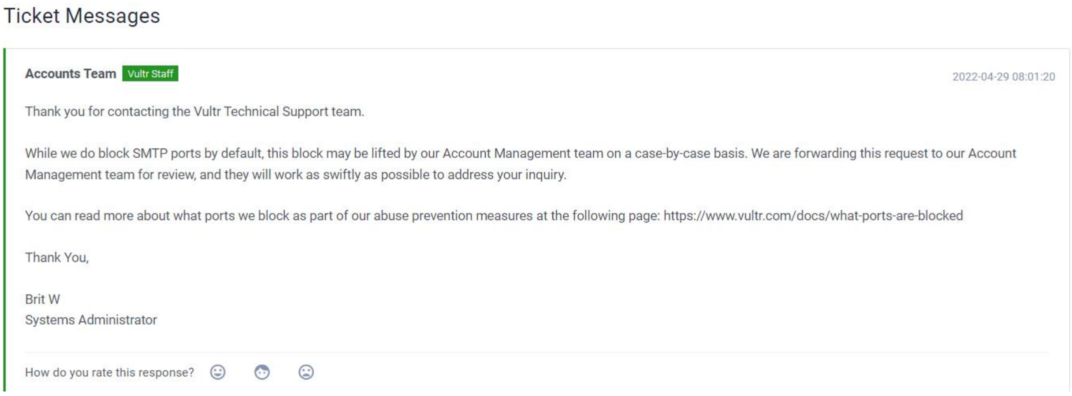
Subject

Message

```
Hi,
Please help me open port 25 service

Thank you
```

Add Attachment: (Maximum 12 MB in size.)

然后厂商给我回信了，说要转交技术



Ticket Messages

Accounts Team Vultr Staff 2022-04-29 08:01:20

Thank you for contacting the Vultr Technical Support team.

While we do block SMTP ports by default, this block may be lifted by our Account Management team on a case-by-case basis. We are forwarding this request to our Account Management team for review, and they will work as swiftly as possible to address your inquiry.

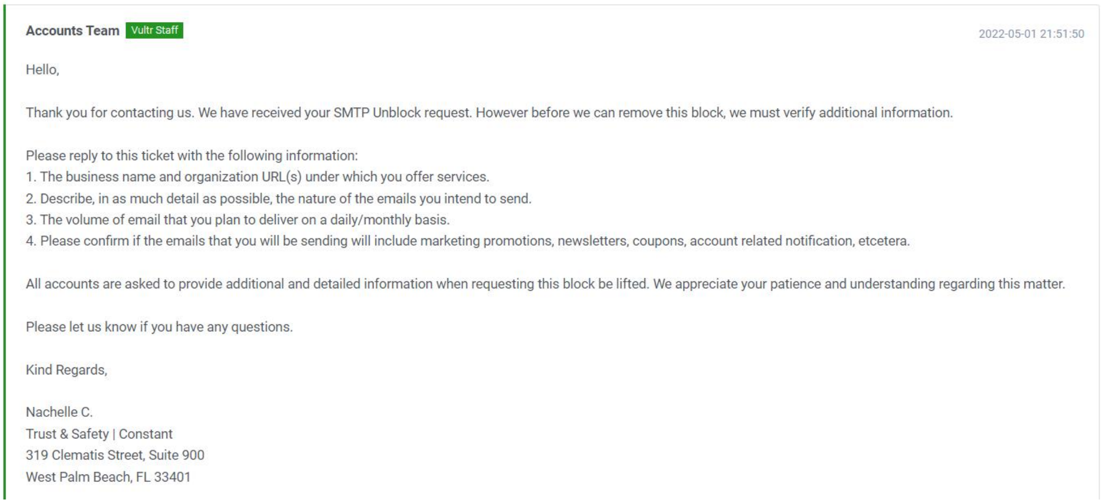
You can read more about what ports we block as part of our abuse prevention measures at the following page: https://www.vultr.com/docs/what-ports-are-blocked

Thank You,

Brit W
Systems Administrator

How do you rate this response? 🙂 😐 🙁

过了一段时间，又给我发了一封邮件，说要提交详细资料：



Accounts Team Vultr Staff 2022-05-01 21:51:50

Hello,

Thank you for contacting us. We have received your SMTP Unblock request. However before we can remove this block, we must verify additional information.

Please reply to this ticket with the following information:
1. The business name and organization URL(s) under which you offer services.
2. Describe, in as much detail as possible, the nature of the emails you intend to send.
3. The volume of email that you plan to deliver on a daily/monthly basis.
4. Please confirm if the emails that you will be sending will include marketing promotions, newsletters, coupons, account related notification, etcetera.

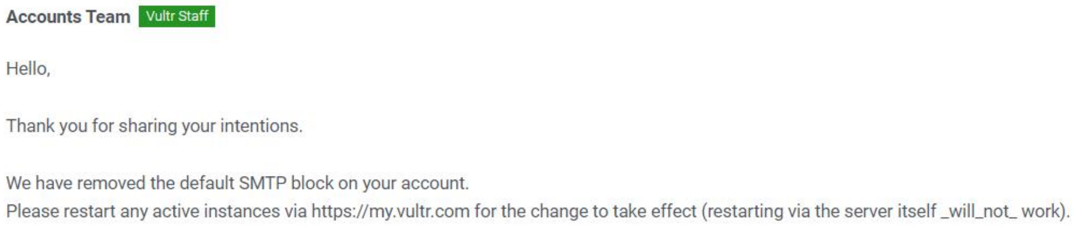
All accounts are asked to provide additional and detailed information when requesting this block be lifted. We appreciate your patience and understanding regarding this matter.

Please let us know if you have any questions.

Kind Regards,

Nachelle C.
Trust & Safety | Constant
319 Clematis Street, Suite 900
West Palm Beach, FL 33401

然后给他提交上去，继续等待
然后又过了一段时间，回复成功开通



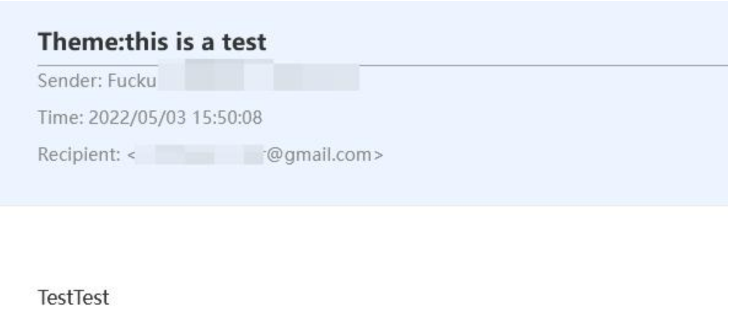
Accounts Team Vultr Staff

Hello,

Thank you for sharing your intentions.

We have removed the default SMTP block on your account.
Please restart any active instances via https://my.vultr.com for the change to take effect (restarting via the server itself _will_not_ work).

然后 restart 服务器，25 端口就可以用了。
发送一封测试邮件给我的 gmail 试一下



Theme:this is a test

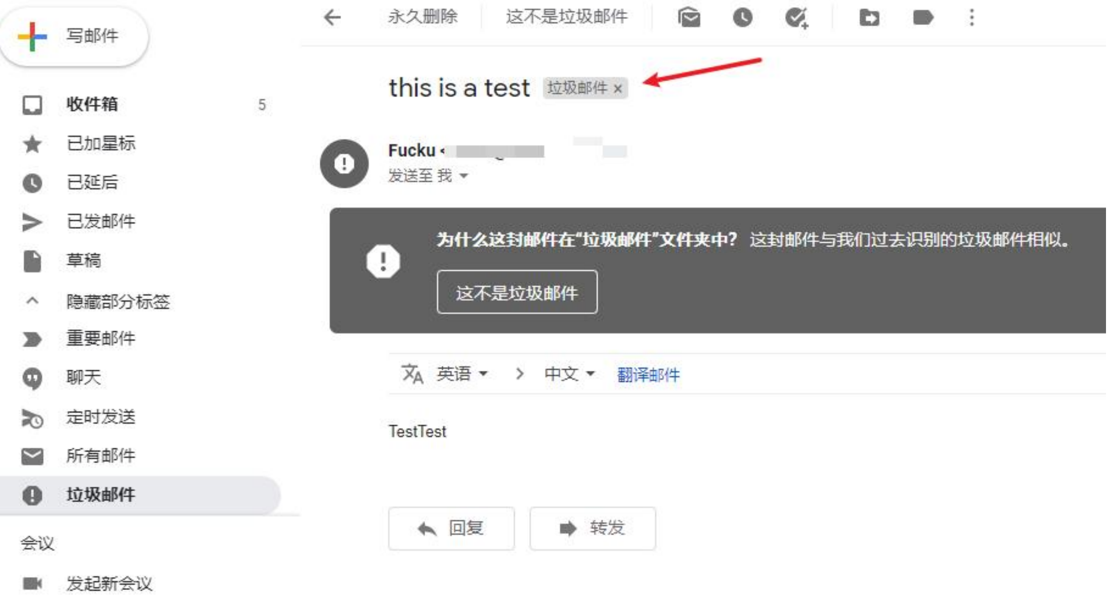
Sender: Fucku[redacted]

Time: 2022/05/03 15:50:08

Recipient: <[redacted]@gmail.com>

TestTest

Gmail 这边查看



this is a test 垃圾邮件 ×

Fucku <[redacted]

发送至 我

为什么这封邮件在"垃圾邮件"文件夹中？ 这封邮件与我们过去识别的垃圾邮件相似。

这不是垃圾邮件

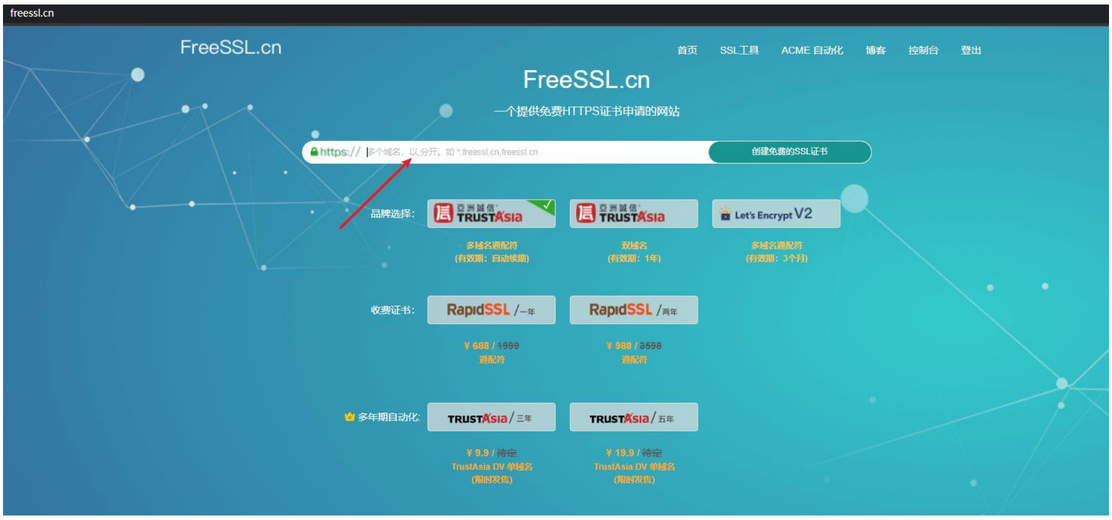
TestTest

成功发入垃圾箱

接下来需要继续操作，让邮件不发入垃圾箱

首先需要添加证书

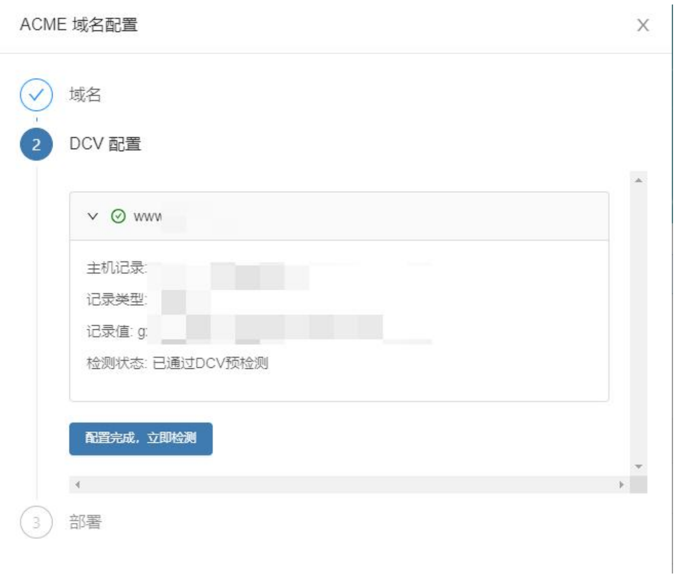
证书有免费申请的地方，在 freessl



这里填写注册的域名点击申请

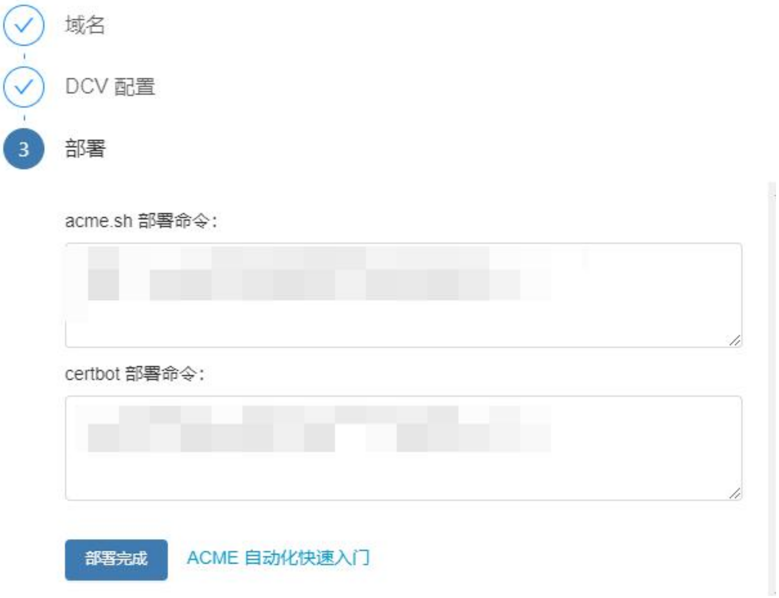
申请完毕之后进入到配置页面

这里先配两个 cname



主机记录: [redacted]
记录类型: [redacted]
记录值: g[redacted]
检测状态: 已通过DCV预检测

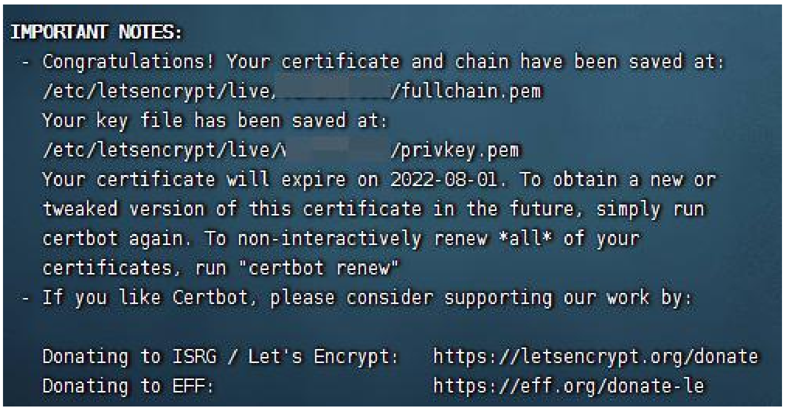
配置完毕之后点击检测
检测通过之后，在 vps 上开始部署



acme.sh 部署命令：[redacted]

certbot 部署命令：[redacted]

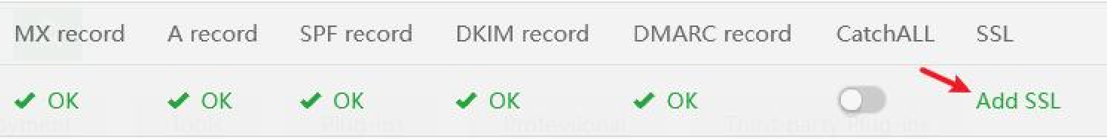
直接把命令复制粘贴过去就行。
这里部署成功



```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/[redacted]/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/[redacted]/privkey.pem
   Your certificate will expire on 2022-08-01. To obtain a new or
   tweaked version of this certificate in the future, simply run
   certbot again. To non-interactively renew *all* of your
   certificates, run "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

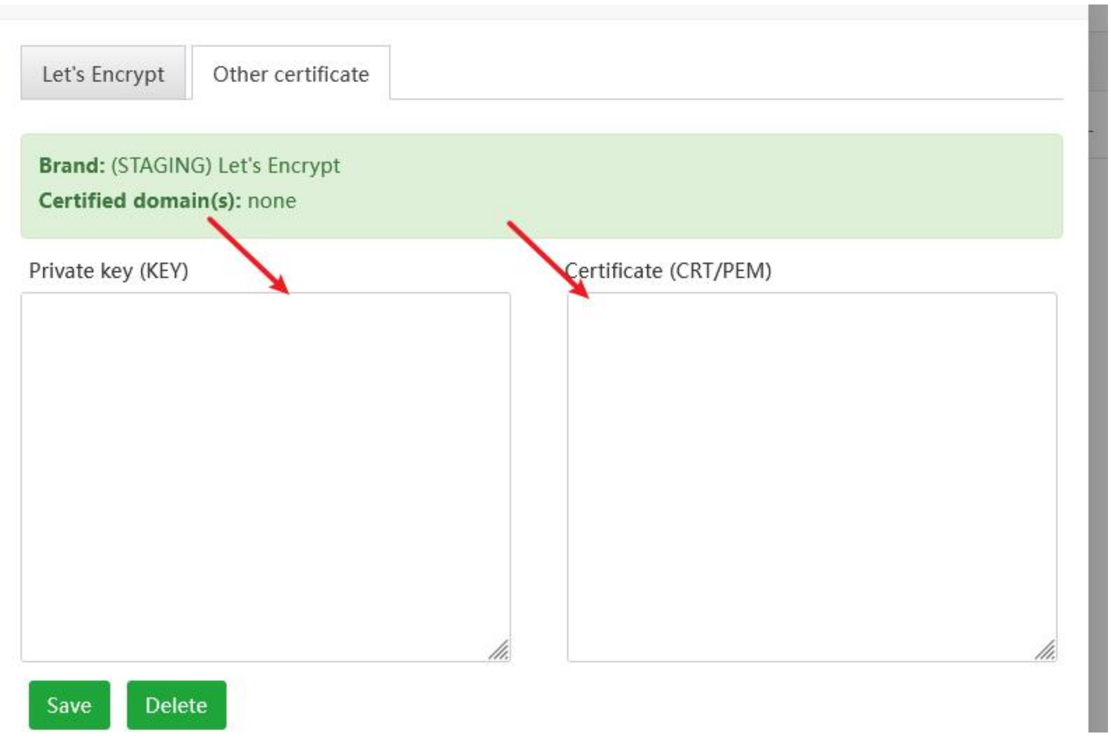
其实 cs 的证书申请也是一回事，也在这里申请

点击宝塔邮局的 ssl 选项



MX record	A record	SPF record	DKIM record	DMARC record	CatchALL	SSL
✓ OK	✓ OK	✓ OK	✓ OK	✓ OK	○	Add SSL

把 key 和 pem 证书复制到这个位置



Brand: (STAGING) Let's Encrypt
Certified domain(s): none

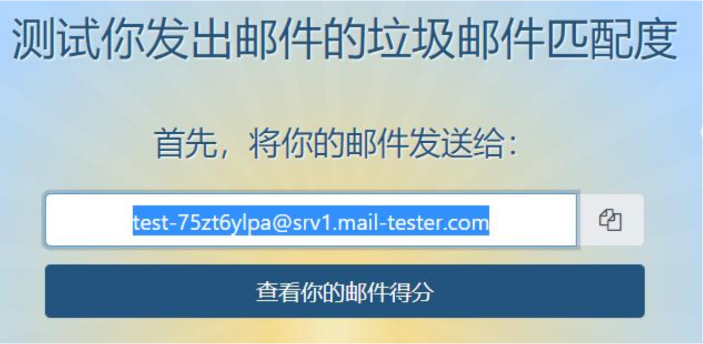
Private key (KEY)

Certificate (CRT/PEM)

复制完毕之后 save

添加完毕之后，发送给测试站邮件

//mail-tester.com

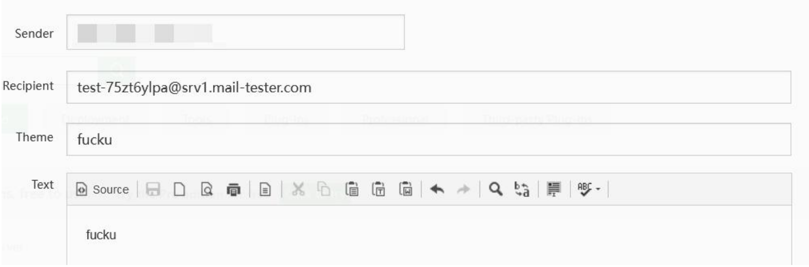


测试你发出邮件的垃圾邮件匹配度

首先，将你的邮件发送给：

test-75zt6ylpa@srv1.mail-tester.com

这里编辑一封邮件发送



Sender [redacted]

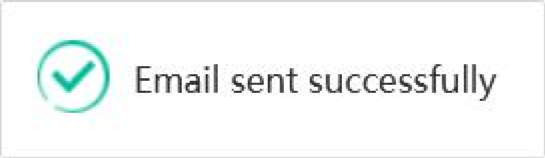
Recipient test-75zt6ylpa@srv1.mail-tester.com

Theme fucku

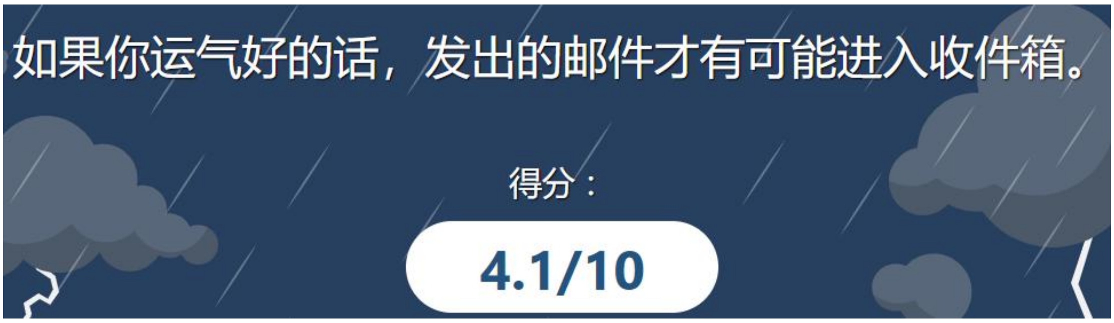
Text

fucku

发送成功


Email sent successfully

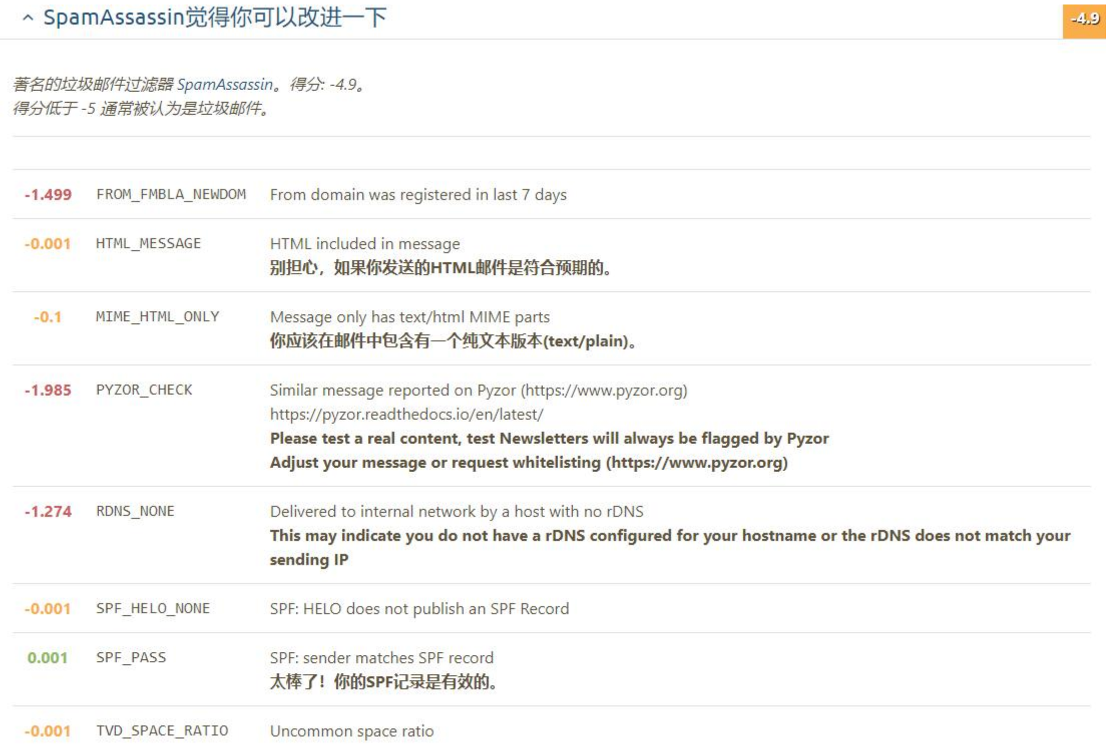
这里显示了得分


如果你运气好的话，发出的邮件才有可能进入收件箱。

得分：

4.1/10

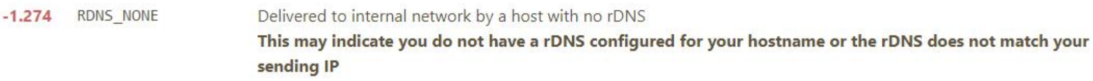
以及可以改进的项目


^ SpamAssassin觉得你可以改进一下 -4.9

著名的垃圾邮件过滤器 SpamAssassin。得分: -4.9。
得分低于 -5 通常被认为是垃圾邮件。

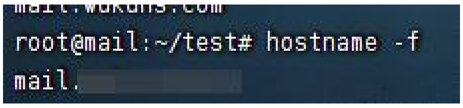
-1.499	FROM_FMBLA_NEWDOM	From domain was registered in last 7 days
-0.001	HTML_MESSAGE	HTML included in message **别担心，如果你发送的HTML邮件是符合预期的。**
-0.1	MIME_HTML_ONLY	Message only has text/html MIME parts **你应该在邮件中包含有一个纯文本版本(text/plain)。**
-1.985	PYZOR_CHECK	Similar message reported on Pyzor (https://www.pyzor.org) https://pyzor.readthedocs.io/en/latest/ **Please test a real content, test Newsletters will always be flagged by Pyzor** **Adjust your message or request whitelisting (https://www.pyzor.org)**
-1.274	RDNS_NONE	Delivered to internal network by a host with no rDNS **This may indicate you do not have a rDNS configured for your hostname or the rDNS does not match your sending IP**
-0.001	SPF_HELO_NONE	SPF: HELO does not publish an SPF Record
0.001	SPF_PASS	SPF: sender matches SPF record **太棒了！你的SPF记录是有效的。**
-0.001	TVD_SPACE_RATIO	Uncommon space ratio

针对这条



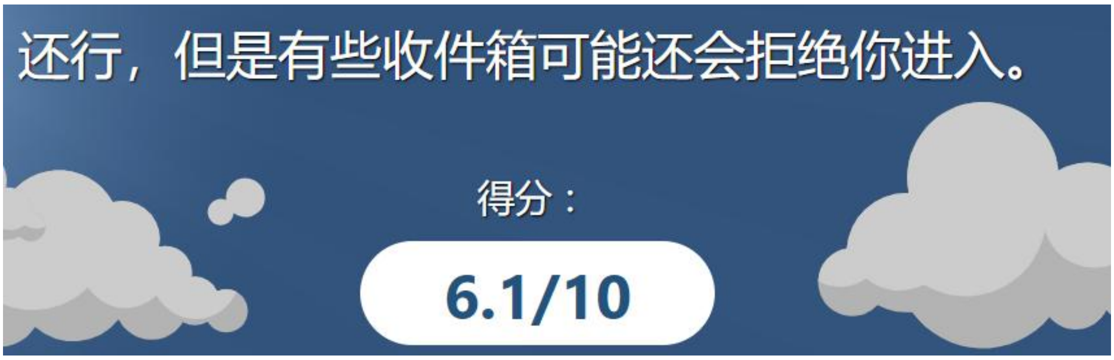
-1.274	RDNS_NONE	Delivered to internal network by a host with no rDNS **This may indicate you do not have a rDNS configured for your hostname or the rDNS does not match your sending IP**

修改主机名和域名相同



```
root@mail:~/test# hostname -f
mail.[redacted]
```

然后换一封邮件发送，发送一封内容多一点的真实邮件：



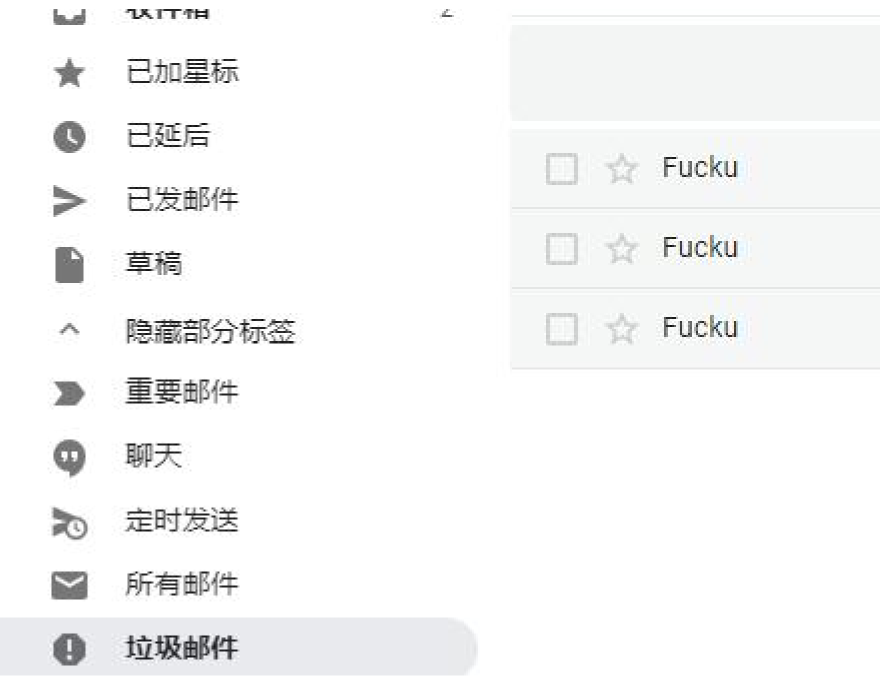
还行，但是有些收件箱可能还会拒绝你进入。

得分：

6.1/10

这里可以看到评分升高了

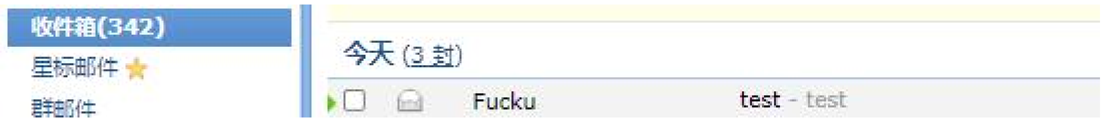
拿同样的邮件再测试一下 gmail



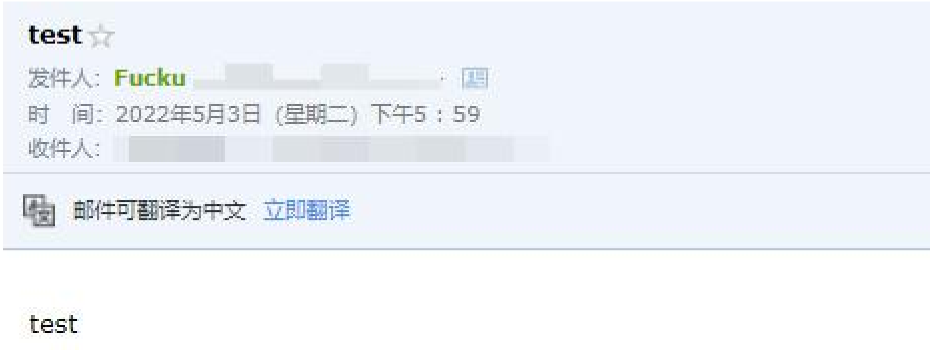
依然在垃圾箱里面，还需要再提升邮箱的可信度才能过 gmail。

发送给 qq 邮箱试一下:

成功在收件箱中收到



内容直白



test

发件人：Fucku [redacted]

时　间：2022年5月3日（星期二）下午5：59

收件人：[redacted]

test

以上，基础邮箱搭建完成，进阶的办法可以在前面加前置机。
可以参考

BCS（北京网络安全大会）2019 红队行动会议重点内容
//https://github.com/Mel0day/RedTeam-BCS

Done