iRedMail 安装完成之后收邮件很慢的问题解决。

昨天，安装了iRedmail,版本号为：9.0.4。

安装完成后各个功能正常，给QQ邮箱发邮件，立马收到了，这速度，真快。可是，收邮件的时候却非常非常慢。如果有人收不到邮件，看看是不是你的端口映射有问题。好了，下面总结下安装按成后需要做的工作，这些东西都是在官方文档里找到的答案。对于邮箱服务器，最重要的还是DNS解析把，别让人家把你当成垃圾邮件给阻挡了。其实，有时候，你的邮件能躺在人家的垃圾邮箱里也是种幸福，毕竟你是小众群体。

DNS的配置，官方的说法：

A record for server hostname

What is an A recordrecords map a FQDN (fully qualified domain name) to an IP
address. This is usually the most often used record type in any
DNS system. This is the DNS record you should add if you want
to point a domain name to a web server.

添加方法：在A记录里面增加一个mail 然后指向邮件服务器的IP。比如：

A mail.abc.com ---->12.12.12.1 TTL 和优先级默认。abc.com 视为你的域名。

---------------------------分割线----------------------------

Reverse PTR record for server
IP address
What is a reverse PTR record
PTR record or more appropriately a reverse PTR record is a
process of resolving an IP address to its associated hostname.
This is the exact opposite of the process of resolving a hostname
to an IP address (A record). Example, when you ping a name

mail.mydomain.com it will get resolved to the ip address using the DNS to something like 192.168.1.5 . Reverse PTR record does the opposite; it looks up the hostname for the given IP address. In the example above the PTR record for IP address 192.168.1.5 will get resolved to mail.mydomain.com .

第二步：增加PTR

方法：增加一个MX记录，解析值为:mail.abc.com.   <---com后面有个.有的DNS厂家会自动给你补上，有的不会。

NAME	PRIORITY	TYPE	DATA
mydomain.com.	10	mx	mail.abc.com.

-----------------------分割线-------------------------

SPF record for your mail domain name
What is a SPF record SPF is a spam and phishing scam fighting method which uses
DNS SPF-records to define which hosts are permitted to send e-mails for a domain. For details on SPF, please see
http://www.openspf.org/
This works by defining a DNS SPF-record for the e-mail domain name specifying which hosts (e-mail servers) are permitted to send e-mail from the domain name.

Other e-mail servers can lookup this record when receiving an e-mail from this domain name to verify that sending e-mail server is connecting from a permitted IP address.

第三步：增加SPF解析

方法：

```
@    TXT "v=spf1 mx mx:mydomain.com  -all"

@    TXT "v=spf1 ip4:192.168.1.100 -all"
```

在根域名下增加一个TXT解析，上面两种方法都可以，我都加上去了。

--------------------分割线-----------------------

DKIM record for your mail domain name
What is a DKIM recordDKIM allows an organization to take responsibility for amessage in a way that can be verified by a recipient. The organization can be a direct handler of the message, such as the author's, the originating sending site's, or an intermediary's along the transit path. However, it can also be an indirect handler, such as an independent service that is providing assistance to a direct handler. DKIM defines a domain-level digital signature authentication framework for email through the use of public-key cryptography and using the domain name service as its key server technology (RFC4871). It permits verification of the signer of a message, as well as the integrity of its contents. DKIM will also provide a mechanism that permits potential email signers to publish information about their email signing practices; this will permit email receivers to make additional assessments of unsigned messages. DKIM's authentication of email identity can assist in the global control of "spam" and "phishing".
A person or organization has an "identity" -- that is, a constellation of characteristics that distinguish them from any other identity. Associated with this abstraction can be a label used as a reference, or "identifier". This is the distinction between a thing and the name of the thing. DKIM uses a domain name as an identifier, to refer to the identity of a responsible person or organization. In DKIM, this identifier is called the Signing Domain IDentifier (SDID) and is contained in the DKIM-Signature header fields d= tag. Note that the same identity can have multiple identifiers.

好长啊，我都没看。

第四部：增加DKIM解析

方法：增加一个TXT记录，二级域名填dkim._domainkey.mydomain.com. 改成你的域名。

txt值为：v=DKIM1; p=××××××××××××××××××××××××

那一串××××怎么来的?

#amavisd -c /etc/amavisd/amavisd.conf showkeys 运行此命令得来的。

另外安装完成的时候，在当前目录里面有个pis文件。里面有详细的参数，要啥有啥。种类齐全。

-------------------------分割线--------------------

DNS搞定之后，就是端口映射了，这个不想在这里说了。我就说说浪费我一下午的时间来搞接受邮件慢的问题。

贴上错误日志:tail -20 /var/log/maillog

```
May  4 09:32:50 mx postfix/smtpd[6996]: NOQUEUE: reject: RCPT from smtpbg329.qq.com[14.17.43.214]: 451 4.7.1 <**@wode.com>: Recipient address rejected: Intentional policy rejection, please try again later; from=<k*(**@foxmail.com> to=<**@wode.com> proto=ESMTP helo=<smtpbg329.qq.com>
```

基本有用的信息就这些。

一看就是被规则阻止掉了，在百度上搜了下这个错误，查出来了个“呵呵”。结果去Bing查询，查处不少有用的东西，有个帖子的链接把我引导了iRedMail的官网，我也想在官网查，可是官网没有论坛，哎。

链接：http://www.iredmail.com/docs/manage.iredapd.html

里面先是说了白名单，黑名单种种，我傻乎乎的跟着配，结果，人家是@anyone ->@anyone

跟空的iptables一样。

最后几行小字看到了想要的东西：

It queries SPF and MX records of specified mail domain names, then store all converted IP addresses/networks defined in SPF/MX records in SQL table`iredapd.greylisting_whitelists`.

To whitelist IP addresses/networks of some mail domain, for example,`outlook.com`, `microsoft.com`, please run command like below:

```
# cd /opt/iredapd/tools/
# python spf_to_greylist_whitelists.py outlook.com microsoft.com
```

If you want to whitelist more mail domains, just run the command with the domain names like above sample.

Since iRedAPD-1.8.0, we have SQL table `iredapd.greylisting_whitelist_domains`to store these mail domain names. if you run `spf_to_greylist_whitelists.py`without any argument, it will fetch all mail domains stored in sql table `greylisting_whitelist_domains` instead of fetching from command line arguments.

```
# python spf_to_greylist_whitelists.py
```

You should setup a cron job to run this script, so that it can keep the IP addresses/networks up to date. iRedMail sets up the cron job to run every 10 minutes, like below:

```
*/10   *    *    *    *    /usr/bin/python /opt/iredapd/tools/spf_to_greylist_w
```

进入tools文件夹，执行命令：

```
python spf_to_greylist_whitelists.py outlook.com microsoft.com 126.com 163.
```

卧槽，终于解决了。