# 邮件服务器文档

## 安装前准备

### 配置源

https://mirrors.tuna.tsinghua.edu.cn/help/centos/

### 外部软件源

yum install vim wget

wget http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm

wget http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

rpm -ivh mysql-community-release-el7-5.noarch.rpm

rpm -ivh epel-release-latest-7.noarch.rpm

### 停用selinux

setenforce 0

vim /etc/sysconfig/selinux

SELINUX=enforcing修改为SELINUX=disabled

### 停用firewalld

systemctl stop firewalld

### 配置网卡

**网卡1：**

vim /etc/sysconfig/network-scripts/ifcfg-ens192

TYPE=Ethernet

BOOTPROTO=static

NAME=ens192

DEVICE=ens192

ONBOOT=yes

IPADDR=192.168.241.224

NETMASK=255.255.255.0

GATEWAY=192.168.241.254

**网卡2：**

vim /etc/sysconfig/network-scripts/ifcfg-ens224

TYPE=Ethernet

BOOTPROTO=static

NAME=ens224

DEVICE=ens224

ONBOOT=yes

IPADDR=192.168.241.226

NETMASK=255.255.255.0

GATEWAY=192.168.241.254

### 配置主机名

vim /etc/hostname

mailcentermaster

配完重启

### 配置hosts文件

#HK Relay

203.174.112.106 mailcenter3.quanshi.com

### 更新软件

yum update

yum makecache

yum install epel-release

### 同步服务器时间

cat << EOF >/etc/cron.daily/ntp.sh

#!/bin/sh

ntpdate ntp.gnetis.com >/var/log/messages

EOF

chmod +x /etc/cron.daily/ntp.sh

ntpdate ntp.gnetis.com

## 安装所有软件包

### postfix

yum install postfix\*

### dovecot

yum install dovecot\*

### openldap

yum -y install openldap\* db4 db4-devel

### phpldapadmin

yum -y install httpd php php-ldap php-fpm php-gd php-mbstring php-mysql phpldapadmin

### perl

yum -y install perl-GD perl-DBD-MySQL perl-GD perl-CPAN perl-CGI perl-CGI-Session perl

### pamldap

yum -y install pam\_ldap nss-pam-ldapd compat-openldap

### mysql

yum -y install mysql-community-server mysql-community-client mysql-community-devel

### 编译压缩包

yum -y install gcc\* \*c++\* zilb\* bzip\* make fetchmail fetch-crl re2c

### sals认证

yum -y install cyrus-sasl cyrus-sasl-lib cyrus-sasl-plain cyrus-sasl-devel

yum -y install cyrus-sasl-ldap cyrus-sasl-ntlm cyrus-sasl-gssapi cyrus-sasl-md5

### 其他工具

yum -y install openssl\* telnet ntpdate

## 配置openLDAP

### DB配置

cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

chown ldap:ldap /var/lib/ldap/DB\_CONFIG

### 配置alias.schema

**vim /etc/openldap/schema/alias.schema**

****

### 配置mail.schema

**vim /etc/openldap/schema/mail.schema**



### 配置ldap管理密码

slappasswd

将管理密码写入slapd.conf文件的rootpw

### 配置slapd.conf

**vim /etc/openldap/slapd.conf**

#

# See slapd.conf(5) for details on configuration options.

# This file should NOT be world readable.

#

include /etc/openldap/schema/core.schema

include /etc/openldap/schema/cosine.schema

include /etc/openldap/schema/inetorgperson.schema

include /etc/openldap/schema/nis.schema

include /etc/openldap/schema/mail.schema

include /etc/openldap/schema/alias.schema

# Allow LDAPv2 client connections. This is NOT the default.

allow bind\_v2

# Do not enable referrals until AFTER you have a working directory

# service AND an understanding of referrals.

#referral ldap://root.openldap.org

pidfile /var/run/openldap/slapd.pid

argsfile /var/run/openldap/slapd.args

# Load dynamic backend modules:

# modulepath /usr/lib64/openldap

#cache

#cachesize 50000000

#idlcachesize 15000000

#checkpoint 1024 5

# Modules available in openldap-servers-overlays RPM package

# Module syncprov.la is now statically linked with slapd and there

# is no need to load it here

# moduleload accesslog.la

# moduleload auditlog.la

# moduleload denyop.la

# moduleload dyngroup.la

# moduleload dynlist.la

# moduleload lastmod.la

# moduleload pcache.la

# moduleload ppolicy.la

# moduleload refint.la

# moduleload retcode.la

# moduleload rwm.la

# moduleload smbk5pwd.la

# moduleload translucent.la

# moduleload unique.la

# moduleload valsort.la

# modules available in openldap-servers-sql RPM package:

# moduleload back\_sql.la

# The next three lines allow use of TLS for encrypting connections using a

# dummy test certificate which you can generate by changing to

# /etc/pki/tls/certs, running "make slapd.pem", and fixing permissions on

# slapd.pem so that the ldap user or group can read it. Your client software

# may balk at self-signed certificates, however.

# TLSCACertificateFile /etc/pki/tls/certs/ca-bundle.crt

# TLSCertificateFile /etc/pki/tls/certs/slapd.pem

# TLSCertificateKeyFile /etc/pki/tls/certs/slapd.pem

# Sample security restrictions

# Require integrity protection (prevent hijacking)

# Require 112-bit (3DES or better) encryption for updates

# Require 63-bit encryption for simple bind

# security ssf=1 update\_ssf=112 simple\_bind=64

# Sample access control policy:

# Root DSE: allow anyone to read it

# Subschema (sub)entry DSE: allow anyone to read it

# Other DSEs:

# Allow self write access

# Allow authenticated users read access

# Allow anonymous users to authenticate

# Directives needed to implement policy:

# access to dn.base="" by \* read

# access to dn.base="cn=Subschema" by \* read

# access to \*

# by self write

# by users read

# by anonymous auth

#

access to \*

by dn="cn=Manager,dc=gnetis,dc=com" write

by dn="cn=admin,dc=gnetis,dc=com" write

by self write

by \* read

# if no access controls are present, the default policy

# allows anyone and everyone to read anything but restricts

# updates to rootdn. (e.g., "access to \* by \* read")

#

# rootdn can always read and write EVERYTHING!

#######################################################################

# ldbm and/or bdb database definitions

#######################################################################

database bdb

suffix "dc=gnetis,dc=com"

rootdn "cn=Manager,dc=gnetis,dc=com"

# Cleartext passwords, especially for the rootdn, should

# be avoided. See slappasswd(8) and slapd.conf(5) for details.

# Use of strong authentication encouraged.

# rootpw secret

#rootpw g@net-

rootpw {SSHA}Vb50gTCafI66f2vt+SZp+dY3TDw9ClG4

# rootpw {crypt}ijFYNcSNctBYg

# The database directory MUST exist prior to running slapd AND

# should only be accessible by the slapd and slap tools.

# Mode 700 recommended.

directory /var/lib/ldap

#ldap log

loglevel 256

# Indices to maintain for this database

index objectClass eq,pres

index ou,cn,mail,surname,givenname eq,pres,sub

index uidNumber,gidNumber,loginShell eq,pres

index uid,memberUid eq,pres,sub

index nisMapName,nisMapEntry eq,pres,sub

index mailaliasname,uniqueMember eq,pres

# Replicas of this database

#replogfile /var/lib/ldap/openldap-master-replog

#replica host=ldap-1.example.com:389 starttls=critical

# bindmethod=sasl saslmech=GSSAPI

# authcId=host/ldap-master.example.com@EXAMPLE.COM

# tongbu ldap server

updatedn "cn=Manager,dc=gnetis,dc=com"

updateref ldap://ldapgl.gnetis.com

### 主ldap修改slapd.conf

replica host=192.168.241.224:389 binddn="cn=Manager,dc=gnetis,dc=com" bindmethod=simple credentials=g@net-

### 启用ldap日志

vim /etc/rsyslog.conf

local4.\* /var/log/ldap.log

systemctl restart rsyslog

### gnetis.ldif内容

dn: dc=gnetis,dc=com

structuralObjectClass: domain

entryUUID: e1a2eb02-9d08-1029-8e7d-f5655630c077

creatorsName: cn=Manager,dc=gnetis,dc=com

createTimestamp: 20050809100539Z

objectClass: top

objectClass: domain

objectClass: dcObject

dc: gnetis

entryCSN: 20050828164353Z#000001#00#000000

modifiersName: cn=Manager,dc=gnetis,dc=com

modifyTimestamp: 20050828164353Z

dn: cn=admin,dc=gnetis,dc=com

cn: admin

objectClass: person

objectClass: top

objectClass: uidObject

sn: admin

structuralObjectClass: person

entryUUID: 13f7fa36-49af-102a-92e1-f9abd90c6185

creatorsName: cn=Manager,dc=gnetis,dc=com

createTimestamp: 20060317030839Z

uid: admin

userPassword:: e0NSWVBUfSQxJDhYb2hEcTFmJEQuaUVwOS52NmFWVWguc1F6RDN0NjE=

entryCSN: 20090922102808Z#000000#00#000000

modifiersName: cn=Manager,dc=gnetis,dc=com

modifyTimestamp: 20090922102808Z

dn: cn=Manager,dc=gnetis,dc=com

cn: Manager

objectClass: person

objectClass: top

sn: Manager

structuralObjectClass: person

entryUUID: 1452f602-49af-102a-9331-f9abd90c6185

creatorsName: cn=Manager,dc=gnetis,dc=com

createTimestamp: 20060317030840Z

userPassword:: e0NSWVBUfSQxJGFMOU1tcEE5JGhQejVPVmtJaFdRdlJuN0NVUTZGNi4=

entryCSN: 20160105050943Z#000000#00#000000

modifiersName: cn=admin,dc=gnetis,dc=com

modifyTimestamp: 20160105050943Z

### 导入用户数据

备份slapd.d目录

cp -ra slapd.d dlapd.dbak

删除slapd.d文件里面的内容

rm -rf slapd.d/\*

slapadd -l gnetis.ldif

### 生成slapd.d目录

slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d

chown -R ldap:ldap /etc/openldap/slapd.d

chown -R ldap:ldap /var/lib/ldap/\*

**重启**

systemctl restart slapd

### 配置ldap客户端

命令：setup

第一步：选择Authentication configuration

第二步：选择Use LDAP ，Use MD5 Passwords，Use Shadow Passwords，Use LDAP Authentication，Local authorization is sufficient

第三步：Server: ldap://127.0.0.1/

Base DN: dc=gnetis,dc=com

保存退出。

### 开机自启动

systemctl enable slapd

### 配置phpldapadmin

**修改登录配置**

**vim /etc/phpldapadmin/config.php**

$servers->setValue('server','host','127.0.0.1');

$servers->setValue('login','auth\_type','cookie');

$servers->setValue('login','bind\_id','cn=Manager,dc=gnetis,dc=com');

$servers->setValue('login','attr','dn');

### 添加访问权限

**vim /etc/httpd/conf.d/phpldapadmin.conf**

Require all granted

systemctl restart httpd

### 附文件：/etc/openldap/



### 附文件：/etc/openldap/schema



## 配置saslauthd认证

**vim /etc/saslauthd.conf**

ldap\_servers: ldap://127.0.0.1

ldap\_bind\_dn: cn=Manager,dc=gnetis,dc=com

ldap\_bind\_pw: g@net-

ldap\_search\_base: dc=users,dc=gnetis,dc=com

ldap\_version: 3

ldap\_auth\_method: bind

ldap\_filter: (&(uid=%u))

### 配置机制为ldap

**vim /etc/sysconfig/saslauthd**

MECH=ldap

**vim /etc/sasl2/smtpd.conf**

pwcheck\_method: saslauthd

mech\_list: plain login

## 安装postfix

cd /etc/postfix

### 配置main.cf

cp main.cf main.cfdefault

postconf -n > main1.cf

**vim main.cf**

alias\_database = hash:/etc/aliases

alias\_maps = hash:/etc/aliases

command\_directory = /usr/sbin

config\_directory = /etc/postfix

daemon\_directory = /usr/libexec/postfix

debug\_peer\_level = 2

html\_directory = no

inet\_interfaces = localhost

mail\_owner = postfix

mailq\_path = /usr/bin/mailq.postfix

manpage\_directory = /usr/share/man

#mydestination = $myhostname, localhost.$mydomain, localhost

newaliases\_path = /usr/bin/newaliases.postfix

queue\_directory = /var/spool/postfix

readme\_directory = /usr/share/doc/postfix-2.3.3/README\_FILES

sample\_directory = /usr/share/doc/postfix-2.3.3/samples

sendmail\_path = /usr/sbin/sendmail.postfix

setgid\_group = postdrop

unknown\_local\_recipient\_reject\_code = 550

#mailgroup

home\_mailbox = Maildir/

inet\_interfaces = all

mydestination = $myhostname, $mydomain, localhost, gnetis.com, seegle.com

smtp\_helo\_name = $myhostname

mydomain = quanshi.com

myhostname = mailcenter.quanshi.com

mynetworks = $config\_directory/mynetworks

myorigin = $mydomain

relay\_domains = $mydestination

message\_size\_limit = 41457280

#sasl

smtpd\_sasl\_auth\_enable = yes

broken\_sasl\_auth\_clients = yes

smtpd\_sasl\_local\_domain = $mydomain

smtpd\_sender\_login\_maps = ldap:/etc/postfix/ldap-user.cf,ldap:/etc/postfix/ldap-mailbox.cf,ldap:/etc/postfix/ldap-mailgroup.cf

smtpd\_reject\_unlisted\_sender = yes

smtpd\_helo\_required = yes

smtpd\_delay\_reject = yes

smtpd\_client\_restrictions =

check\_client\_access hash:/etc/postfix/access

permit\_mynetworks,

permit\_sasl\_authenticated,

permit\_tls\_all\_clientcerts,

permit\_tls\_clientcerts,

reject\_rbl\_client zen.spamhaus.org,

reject\_multi\_recipient\_bounce,

reject\_unauth\_pipelining,

reject\_invalid\_hostname,

reject\_non\_fqdn\_hostname,

#reject\_unknown\_hostname,

#reject\_unknown\_client

smtpd\_sender\_restrictions =

# check\_sender\_access regexp:/etc/postfix/sender.re,

permit\_mynetworks,

check\_policy\_service unix:private/policy-spf,

permit\_sasl\_authenticated,

check\_sender\_access hash:/etc/postfix/sender\_access,

reject\_sender\_login\_mismatch,

reject\_unlisted\_sender,

reject\_non\_fqdn\_recipient,

reject\_non\_fqdn\_sender,

reject\_unknown\_sender\_domain

smtpd\_recipient\_restrictions =

permit\_mynetworks,

permit\_sasl\_authenticated,

permit\_auth\_destination,

permit\_mx\_backup,

check\_recipient\_maps

reject\_unverified\_recipient,

# reject\_rbl\_client cblless.anti-spam.org.cn,bl.spamcop.net,zen.spamhaus.org,

reject\_non\_fqdn\_recipient,

reject\_unknown\_recipient\_domain,

permit\_sasl\_authenticated,

reject\_unauth\_destination

smtpd\_sasl\_security\_options = noanonymous

#mail alias

virtual\_alias\_maps = ldap:/etc/postfix/ldap\_alias, ldap:/etc/postfix/ldap\_aliasgroup

virtual\_alias\_expansion\_limit = 3000

#qu chong

enable\_original\_recipient = no

#enable\_original\_recipient = yes

#yu ming wei zhuang

smtp\_generic\_maps = hash:/etc/postfix/my\_generic\_maps

#ssl

smtp\_use\_tls = yes

smtpd\_use\_tls = yes

smtp\_tls\_note\_starttls\_offer = yes

smtpd\_tls\_key\_file = /etc/postfix/ssl/smtpd.pem

smtpd\_tls\_cert\_file = /etc/postfix/ssl/cert.pem

smtpd\_tls\_loglevel = 1

smtpd\_tls\_received\_header = yes

smtpd\_tls\_session\_cache\_timeout = 3600s

#bcc

recipient\_bcc\_maps = hash:/etc/postfix/recipient\_bcc

#amavis+clamav

content\_filter = amavis:127.0.0.1:10024

#limit

default\_process\_limit = 400

#anvil\_rate\_time\_unit = 120s

#smtpd\_client\_connection\_rate\_limit=5

#transport

transport\_maps = hash:/etc/postfix/transport

#

non\_fqdn\_reject\_code = 450

unknown\_local\_recipient\_reject\_code = 450

unknown\_virtual\_alias\_reject\_code = 450

unknown\_virtual\_mailbox\_reject\_code = 450

maps\_rbl\_reject\_code = 450

#

smtpd\_error\_sleep\_time = 1s

smtpd\_soft\_error\_limit = 10

smtpd\_hard\_error\_limit = 20

#

anvil\_rate\_time\_unit = 60s

smtpd\_client\_connection\_rate\_limit = 60

smtpd\_client\_message\_rate\_limit = 60

smtpd\_client\_recipient\_rate\_limit = 60

smtpd\_client\_event\_limit\_exceptions = ${smtpd\_client\_connection\_limit\_exceptions:$mynetworks}

#spf header check

header\_checks = pcre:/etc/postfix/header\_checks

body\_checks = pcre:/etc/postfix/body\_checks

### 配置master.cf

**vim master.cf**

#

# Postfix master process configuration file. For details on the format

# of the file, see the master(5) manual page (command: "man 5 master").

#

# ==========================================================================

# service type private unpriv chroot wakeup maxproc command + args

# (yes) (yes) (yes) (never) (100)

# ==========================================================================

smtp inet n - n - 400 smtpd

#submission inet n - n - - smtpd

# -o smtpd\_enforce\_tls=yes

# -o smtpd\_sasl\_auth\_enable=yes

# -o smtpd\_client\_restrictions=permit\_sasl\_authenticated,reject

#smtps inet n - n - - smtpd

# -o smtpd\_tls\_wrappermode=yes

# -o smtpd\_sasl\_auth\_enable=yes

# -o smtpd\_client\_restrictions=permit\_sasl\_authenticated,reject

smtps inet n - n - 600 smtpd

-o smtpd\_tls\_wrappermode=yes

-o smtpd\_sasl\_auth\_enable=yes

-o smtpd\_client\_restrictions=permit\_sasl\_authenticated,reject

amavis unix - - n - 200 smtp

-o smtp\_data\_done\_timeout=1200

-o smtp\_send\_xforward\_command=yes

-o disable\_dns\_lookups=yes

127.0.0.1:10025 inet n - n - 200 smtpd

-o content\_filter=

-o local\_recipient\_maps=

-o relay\_recipient\_maps=

-o smtpd\_delay\_reject=no

-o mynetworks=127.0.0.0/8,192.168.11.0/24

-o smtpd\_helo\_restrictions=

-o smtpd\_client\_restrictions=permit\_mynetworks,reject

-o smtpd\_sender\_restrictions=

-o smtpd\_recipient\_restrictions=permit\_mynetworks,reject

-o smtpd\_restriction\_classes=

-o smtpd\_data\_restrictions=reject\_unauth\_pipelining

-o smtpd\_end\_of\_data\_restrictions=

-o strict\_rfc821\_envelopes=yes

-o smtpd\_error\_sleep\_time=0

-o smtpd\_soft\_error\_limit=1001

-o smtpd\_hard\_error\_limit=1000

-o smtpd\_client\_connection\_count\_limit=0

-o smtpd\_client\_connection\_rate\_limit=0

-o local\_header\_rewrite\_clients=

-o receive\_override\_options=no\_header\_body\_checks,no\_unknown\_recipient\_checks

#628 inet n - n - - qmqpd

pickup fifo n - n 60 1 pickup

cleanup unix n - n - 0 cleanup

qmgr fifo n - n 300 1 qmgr

#qmgr fifo n - n 300 1 oqmgr

tlsmgr unix - - n 1000? 1 tlsmgr

rewrite unix - - n - - trivial-rewrite

bounce unix - - n - 0 bounce

defer unix - - n - 0 bounce

trace unix - - n - 0 bounce

verify unix - - n - 1 verify

flush unix n - n 1000? 0 flush

proxymap unix - - n - - proxymap

smtp unix - - n - - smtp

# When relaying mail as backup MX, disable fallback\_relay to avoid MX loops

relay unix - - n - - smtp

-o fallback\_relay=

# -o smtp\_helo\_timeout=5 -o smtp\_connect\_timeout=5

showq unix n - n - - showq

error unix - - n - - error

discard unix - - n - - discard

local unix - n n - - local

virtual unix - n n - - virtual

lmtp unix - - n - - lmtp

anvil unix - - n - 1 anvil

scache unix - - n - 1 scache

#

# ====================================================================

# Interfaces to non-Postfix software. Be sure to examine the manual

# pages of the non-Postfix software to find out what options it wants.

#

# Many of the following services use the Postfix pipe(8) delivery

# agent. See the pipe(8) man page for information about ${recipient}

# and other message envelope options.

# ====================================================================

#

# maildrop. See the Postfix MAILDROP\_README file for details.

# Also specify in main.cf: maildrop\_destination\_recipient\_limit=1

#

maildrop unix - n n - - pipe

flags=DRhu user=vmail argv=/usr/local/bin/maildrop -d ${recipient}

#

# The Cyrus deliver program has changed incompatibly, multiple times.

#

old-cyrus unix - n n - - pipe

flags=R user=cyrus argv=/usr/lib/cyrus-imapd/deliver -e -m ${extension} ${user}

# Cyrus 2.1.5 (Amos Gouaux)

# Also specify in main.cf: cyrus\_destination\_recipient\_limit=1

cyrus unix - n n - - pipe

user=cyrus argv=/usr/lib/cyrus-imapd/deliver -e -r ${sender} -m ${extension} ${user}

#

# See the Postfix UUCP\_README file for configuration details.

#

uucp unix - n n - - pipe

flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)

#

# Other external delivery methods.

#

ifmail unix - n n - - pipe

flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)

bsmtp unix - n n - - pipe

flags=Fq. user=foo argv=/usr/local/sbin/bsmtp -f $sender $nexthop $recipient

policy-spf unix - n n - - spawn

user=nobody argv=/usr/bin/perl /usr/libexec/postfix/policyd-spf-perl

### 配置postfix的ldap验证

vim ldap\_alias

server\_host = 127.0.0.1

search\_base = dc=users,dc=gnetis,dc=com

ldapaliases\_scope = one

query\_filter = (&(mailaliasname=%s))

result\_attribute = uid

vim ldap\_aliasgroup

server\_host = 127.0.0.1

search\_base = ou=MailGroup,dc=gnetis,dc=com

ldapaliases\_scope = one

query\_filter = (&(mailaliasname=%s))

result\_attribute = mail

vim ldap-mailbox.cf

server\_host = 127.0.0.1

search\_base = dc=users,dc=gnetis,dc=com

ldapaliases\_scope = one

query\_filter = (&(homeDirectory=%s))

result\_attribute = uid

vim ldap-mailgroup.cf

server\_host = 127.0.0.1

search\_base = ou=MailGroup,dc=gnetis,dc=com

ldapaliases\_scope = one

query\_filter = (&(mailaliasname=%s))

result\_attribute = mail

vim ldap-user.cf

server\_host = 127.0.0.1

search\_base = dc=users,dc=gnetis,dc=com

ldapaliases\_scope = one

query\_filter = (&(uid=%s))

result\_attribute = uid

### 重启postfix

systemctl restart postfix

### 设置开机启动

systemctl enable postfix

vim /etc/postfix/recipient\_bcc

### 

### 附文件：/etc/postfix/



### 附文件：/etc/postfix/ssl/



## 安装Perl模块

#### 下载软件

新版的不支持只能下旧版本了

wget https://launchpad.net/postfix-policyd-spf-perl/trunk/2.009/+download/postfix-policyd-spf-perl-2.009.tar.gz

#### 安装模块

perl -MCPAN -e 'install version'

perl -MCPAN -e 'install NetAddr::IP'

perl -MCPAN -e 'install Mail::SPF'

perl -MCPAN -e 'install Sys::Hostname::Long'

#### 解压软件

tar zxf postfix-policyd-spf-perl-2.011.tar.gz

cd postfix-policyd-spf-perl

cp postfix-policyd-spf-perl /usr/libexec/postfix/policyd-spf-perl

## 2、配置命令

1)配置postfix使postfix调用policy-spf程序

vim /etc/postfix/master.cf

#spf check

Policy-spf unix - n n - - spawn

User=nobody argv=/usr/bin/perl /usr/libexec/postfix/policyd-spf-perl

2)配置postfix主配置文件，将检查spf选项添加到permit\_mynetworks之后，使内网中的网段不受spf的影响

vim /etc/postfix/main.cf

smtpd\_sender\_restrictions =

permit\_mynetworks,

check\_policy\_service unix:private/policy-spf,

header\_checks = pcre:/etc/postfix/header\_checks

3)spf产生的三种状态pass，softfail，none 将后两种状态的邮件视为垃圾邮件拒绝掉

vim /etc/postfix/header\_checks

#/Received-SPF: none/ REJECT

/Received-SPF\:\ softfail REJECT

4)执行postmap生成header\_checks.db文件，重启postfix使之生效

postmap /etc/postfix/header\_checks

/etc/init.d/postfix restart

## 3、测试查看日志

查看spf状态为none



## 安装dovecot

### 配置主配置文件

**vim /etc/dovecot/dovecot.conf**

protocols = imap pop3 lmtp

listen = \*, ::

### 进入功能配置文件目录

**cd /etc/dovecot/conf.d/**

### 配置认证：

**vim 10-auth.conf**

disable\_plaintext\_auth = no

### 配置log文件：

**vim 10-logging.conf**

log\_path = /var/log/dovecot.log

info\_log\_path = /var/log/dovecot\_info.log

log\_timestamp = "%b %d %H:%M:%S "

### 配置mail收件目录：

**vim 10-mail.conf**

mail\_location = maildir:~/Maildir

### ldap验证配置：

**vim auth-ldap.conf.ext**

passdb {

driver = ldap

args = /etc/dovecot/dovecot-ldap.conf

}

userdb {

driver = ldap

args = /etc/dovecot/dovecot-ldap.conf

}

**vim /etc/dovecot/dovecot-ldap.conf**

hosts=127.0.0.1

dn = cn=Manager,dc=gnetis,dc=com

dnpass = g@net-

auth\_bind = yes

base = dc=gnetis,dc=com

deref = never

scope = subtree

user\_attrs = homeDirectory=home,uidNumber=uid,gidNumber=gid

user\_filter = (&(objectClass=posixAccount)(uid=%u))

pass\_attrs = uid=user,userPassword={md5}password,homeDirectory=userdb\_home,uidNumber=userdb\_uid,gidNumber=userdb\_gid

pass\_filter = (&(objectClass=posixAccount)(uid=%u))

default\_pass\_scheme = CRYPT

### 重启dovecot

systemctl restart dovecot

### 设置开机启动

systemctl enable dovecot

### 附文件:/etc/dovecot/



### 附文件:/etc/dovecot/conf.d



## 安装配置clamav

wget https://www.ijs.si/software/amavisd/amavisd-new-2.11.1.tar.bz2

groupadd amavis

groupadd clamav

useradd -g amavis -s /bin/false -d /dev/null amavis

useradd -g amavis -s /bin/false -d /dev/null clamav

tar zxvf clamav-0.101.0.tar.gz

./configure --prefix=/usr/local/clamav --with-dbdir=/usr/local/share/clamav

make

make check

make install

**cp /usr/local/clamav/etc/clamd.conf /usr/local/clamav/etc/clamd.conf.bak**

#Example

User amavis

LogFile /var/log/clamav/clamd.log

LogSyslog yes

LogFacility LOG\_MAIL

LogVerbose yes

PidFile /var/run/clamav/clamd.pid

DatabaseDirectory /usr/local/share/clamav

LocalSocket /var/run/clamav/clamd.sock

TCPSocket 3310

StreamMaxLength 10M

ScanELF yes

ScanMail yes

ScanArchive yes

**vim /usr/local/clamav/etc/freshclam.conf**

#Example

DatabaseDirectory /usr/local/share/clamav

UpdateLogFile /var/log/clamav/freshclam.log

LogVerbose yes

LogSyslog yes

LogFacility LOG\_MAIL

PidFile /var/run/clamav/freshclam.pid

DatabaseOwner amavis

DatabaseMirror db.CN.clamav.net

Checks 12

NotifyClamd /usr/local/clamav/etc/clamd.conf

### 授权目录

mkdir /var/log/clamav

chown -R amavis:amavis /var/log/clamav

chmod -R 744 /var/log/clamav

mkdir /usr/local/share/clamav

chown -R amavis:amavis /usr/local/share/clamav

mkdir /var/run/clamav

chown -R amavis.amavis /var/run/clamav

chmod 700 /var/run/clamav

### 病毒库更新

/usr/local/clamav/bin/freshclam

### 设置自动每天自动更新

vim /etc/cron.daily/amavis.sh

#!/bin/sh

/usr/local/clamav/bin/freshclam --quiet -l /var/log/clamav/clamd.log

### 设置开机启动

systemctl enable clamav-daemon

systemctl enable clamav-freshclam

## 安装配置spamassassin

### 安装perl模块

perl -MCPAN -e 'install Mail::SpamAssassin'

perl -MCPAN -e 'install Net::Server'

perl -MCPAN -e 'install Digest::SHA'

perl -MCPAN -e 'install Net::DNS'

perl -MCPAN -e 'install NetAddr::IP'

perl -MCPAN -e 'install Archive::Tar'

perl -MCPAN -e 'install Digest::SHA1'

perl -MCPAN -e 'install Mail::SPF'

perl -MCPAN -e 'install IP::Country'

perl -MCPAN -e 'install Razor2::Syslog'

perl -MCPAN -e 'install Net::Ident'

perl -MCPAN -e 'install IO::Socket::INET6'

perl -MCPAN -e 'install ExtUtils::MakeMaker'

perl -MCPAN -e 'IO::Socket::SSL'

perl -MCPAN -e 'Mail::DKIM'

perl -MCPAN -e 'Encode::Detect'

perl -MCPAN -e 'install IO::Stringy'

perl -MCPAN -e 'install MIME::Words'

perl -MCPAN -e 'install Convert::BinHex'

perl -MCPAN -e 'install Archive::Zip'

perl -MCPAN -e 'install Convert::UUlib'

perl -MCPAN -e 'install HTML::Parser'

perl -MCPAN -e 'install Convert::TNEF'

perl -MCPAN -e 'install Unix::Syslog'

perl -MCPAN -e 'install Net::Server'

perl -MCPAN -e 'install Net::Server::PreFork'

perl -MCPAN -e 'install BerkeleyDB'

perl -MCPAN -e 'install Crypt::OpenSSL::RSA'

perl -MCPAN -e 'install Mail::DKIM::Verifier'

perl -MCPAN -e 'install Convert::TNEF'

perl -MCPAN -e 'install Convert::UUlib'

perl -MCPAN -e 'install Archive::Zip'

perl -MCPAN -e 'install Mail::Mime'

perl -MCPAN -e 'install Geo::IP'

perl -MCPAN -e 'install Net::CIDR::Lite'

perl -MCPAN -e 'install Encode::Detect::Detector'

perl -MCPAN -e 'install Net::Patricia'

perl -MCPAN -e 'install BSD::Resource'

perl -MCPAN -e 'install File::Fetch'

### 安装spamassassin

wget http://mirrors.hust.edu.cn/apache//spamassassin/source/Mail-SpamAssassin-3.4.2.tar.gz

tar xf Mail-SpamAssassin-3.4.2.tar.gz

cd Mail-SpamAssassin-3.4.2

perl Makefile.PL

如提示有没有装的perl模块，可以照上面的安装一下

make

make install

cd Mail-SpamAssassin-3.4.2/spamd

cp redhat-rc-script.sh /etc/init.d/spamd

chmod +x /etc/init.d/spamd

### 配置spamassassin

**vim /etc/mail/spamassassin/local.cf**

# This is the right place to customize your installation of SpamAssassin.

#

# See 'perldoc Mail::SpamAssassin::Conf' for details of what can be

# tweaked.

#

# Only a small subset of options are listed below

#

###########################################################################

# Add \*\*\*\*\*SPAM\*\*\*\*\* to the Subject header of spam e-mails

#

rewrite\_header Subject \*\*\*\*\*SPAM\*\*\*\*\*

# Save spam messages as a message/rfc822 MIME attachment instead of

# modifying the original message (0: off, 2: use text/plain instead)

#

report\_safe 0

# Set which networks or hosts are considered 'trusted' by your mail

# server (i.e. not spammers)

#

# trusted\_networks 212.17.35.

# Set file-locking method (flock is not safe over NFS, but is faster)

#

# lock\_method flock

# Set the threshold at which a message is considered spam (default: 5.0)

#

required\_score 5.0

# Use Bayesian classifier (default: 1)

#

use\_bayes 1

# Bayesian classifier auto-learning (default: 1)

#

bayes\_auto\_learn 1

# Set headers which may provide inappropriate cues to the Bayesian

# classifier

bayes\_min\_ham\_num 2500

bayes\_min\_spam\_num 2500

bayes\_auto\_learn\_threshold\_nonspam 15

bayes\_path /var/amavis/.spamassassin/bayes

bayes\_file\_mode 0770

score BAYES\_00 -13

score BAYES\_05 -11.5

score BAYES\_20 -9.5

score BAYES\_40 -8.5

score BAYES\_50 -4

score BAYES\_60 4.5

score BAYES\_80 6

score BAYES\_95 8

score BAYES\_99 13

score BAYES\_999 15

skip\_rbl\_checks 0

use\_razor2 1

use\_pyzor 1

dns\_available yes

header LOCAL\_RCVD Received =~ /.\*\(\S+\.quanshi\.com\s+\[.\*\]\)/

describe LOCAL\_RCVD Received from local machine

score LOCAL\_RCVD -50

score DCC\_CHECK 4.000

score SPF\_FAIL 10.000

score SPF\_HELO\_FAIL 10.000

score RAZOR2\_CHECK 2.500

score HEAD\_ILLEGAL\_CHARS 0

score UPPERCASE\_25\_50 0

score X\_MSMAIL\_PRIORITY\_HIGH 0

score X\_PRIORITY\_HIGH 0

score TO\_TXT 100

score RATWARE\_HASH\_2 100

score RATWARE\_HASH\_2\_V2 100

score FROM\_ILLEGAL\_CHARS 0.1

score MIME\_BASE64\_TEXT 0.1

score NO\_RDNS\_DOTCOM\_HELO 0.1

score CHINA\_HEADER 0.1

score NO\_REAL\_NAME 0.2

score HTML\_MESSAGE 0.2

score MIME\_HTML\_ONLY 0.2

score MIME\_HTML\_ONLY\_MULTI 0.2

score FORGED\_MUA\_OUTLOOK 0.2

score FORGED\_HOTMAIL\_RCVD 0.2

score FORGED\_OUTLOOK\_TAGS 0.2

score MAILTO\_TO\_SPAM\_ADDR 0.2

header RCVD\_IN\_CASA\_CBL eval:check\_rbl('CBL','cbl.anti-spam.org.cn.','127.0.8.2')

describe RCVD\_IN\_CASA\_CBL Relay has be listed in CASA CBL, http://anti-spam.org.cn/

tflags RCVD\_IN\_CASA\_CBL net

header RCVD\_IN\_CASA\_CDL eval:check\_rbl('CDL','cdl.anti-spam.org.cn.','127.0.8.4')

describe RCVD\_IN\_CASA\_CDL Relay has be listed in CASA CDL, http://anti-spam.org.cn/

tflags RCVD\_IN\_CASA\_CDL net

header RCVD\_IN\_CASA\_CBLPLUS eval:check\_rbl('CBLPLUS','cblplus.anti-spam.org.cn.','127.0.8.6')

describe RCVD\_IN\_CASA\_CBLPLUS Relay has be listed in CASA CBL+, http://anti-spam.org.cn/

tflags RCVD\_IN\_CASA\_CBLPLUS net

header RCVD\_IN\_CASA\_CBLLESS eval:check\_rbl('CBLLESS','cblless.anti-spam.org.cn.','127.0.8.5')

describe RCVD\_IN\_CASA\_CBLLESS Relay has be listed in CASA CBL-, http://anti-spam.org.cn/

tflags RCVD\_IN\_CASA\_CBLLESS net

header RCVD\_IN\_CASA\_CML eval:check\_rbl('CML','cml.anti-spam.org.cn.','127.0.8.1')

describe RCVD\_IN\_CASA\_CML Relay has be listed in CASA CML (whitelist), http://anti-spam.org.cn/

tflags RCVD\_IN\_CASA\_CML net nice

#

score RCVD\_IN\_SORBS\_BLOCK 4.0

score RCVD\_IN\_SORBS\_DUL 3.0

score RCVD\_IN\_SORBS\_HTTP 6.0

score RCVD\_IN\_SORBS\_MISC 4.0

score RCVD\_IN\_SORBS\_SMTP 4.0

score RCVD\_IN\_SORBS\_SPAM 6.0

score RCVD\_IN\_SORBS\_SOCKS 6.0

score RCVD\_IN\_SORBS\_WEB 3.0

score RCVD\_IN\_SORBS\_ZOMBIE 1.0

score RCVD\_IN\_SBL 6.0

score RCVD\_IN\_XBL 14.0

score RCVD\_IN\_PBL 6.0

score RCVD\_IN\_SBL\_CSS 6.0

score RCVD\_IN\_BL\_SPAMCOP\_NET 6.0

score RCVD\_IN\_MAPS\_RBL 4.0

score RCVD\_IN\_MAPS\_DUL 4.0

score RCVD\_IN\_MAPS\_RSS 4.0

score RCVD\_IN\_MAPS\_OPS 4.0

score RCVD\_IN\_MAPS\_NML -4.0

score RCVD\_IN\_IADB\_VOUCHED -4.0

score RCVD\_IN\_IADB\_DOPTIN -9.0

score RCVD\_IN\_IADB\_ML\_DOPTIN -12

score RCVD\_IN\_RP\_RNBL 4.0

score RCVD\_IN\_RP\_CERTIFIED -8.0

score RCVD\_IN\_RP\_SAFE -9.0

score RCVD\_IN\_CASA\_CBL 9.0

score RCVD\_IN\_CASA\_CDL 9.0

score RCVD\_IN\_CASA\_CBLPLUS 9.0

score RCVD\_IN\_CASA\_CBLLESS 9.0

score RCVD\_IN\_CASA\_CML -10.0

score DKIMDOMAIN\_IN\_DWL -10.0

score DKIMDOMAIN\_IN\_DWL\_UNKNOWN -2.0

#

# bayes\_ignore\_header X-Bogosity

# bayes\_ignore\_header X-Spam-Flag

# bayes\_ignore\_header X-Spam-Status

# Some shortcircuiting, if the plugin is enabled

#

ifplugin Mail::SpamAssassin::Plugin::Shortcircuit

#

# default: strongly-whitelisted mails are \*really\* whitelisted now, if the

# shortcircuiting plugin is active, causing early exit to save CPU load.

# Uncomment to turn this on

#

# shortcircuit USER\_IN\_WHITELIST on

# shortcircuit USER\_IN\_DEF\_WHITELIST on

# shortcircuit USER\_IN\_ALL\_SPAM\_TO on

# shortcircuit SUBJECT\_IN\_WHITELIST on

# the opposite; blacklisted mails can also save CPU

#

# shortcircuit USER\_IN\_BLACKLIST on

# shortcircuit USER\_IN\_BLACKLIST\_TO on

# shortcircuit SUBJECT\_IN\_BLACKLIST on

# if you have taken the time to correctly specify your "trusted\_networks",

# this is another good way to save CPU

#

# shortcircuit ALL\_TRUSTED on

# and a well-trained bayes DB can save running rules, too

#

# shortcircuit BAYES\_99 spam

# shortcircuit BAYES\_00 ham

endif # Mail::SpamAssassin::Plugin::Shortcircuit

### 配置规则黑白名单

注意此文件必须符合ISO-8859标准，否则不生效，执行如下命令查看：

**file Chinese\_rules\_GB2312.cf**

输出Chinese\_rules\_GB2312.cf: ISO-8859 English text

可以将文件用notepad++保存为utf8 Unicode格式

file 文件名 查看文件类型

测试：垃圾邮件过滤

病毒邮件过滤

黑白名单过滤功能



**mkdir sa-update-keys**



### 开启bayes学习功能

sa-update

service spamd start

### 设置开机启动

chkconfig spamd on

## 安装配置amavis

mkdir -p /var/amavis /var/amavis/tmp /var/amavis/var /var/amavis/db

chown -R amavis:amavis /var/amavis

chmod -R 777 /var/amavis

cd amavisd-new-2.11.1

cp amavisd /usr/local/sbin/

cp amavisd.conf /etc/

chown root:amavis /etc/amavisd.conf

chmod 640 /etc/amavisd.conf

mkdir /var/virusmails

chown amavis:amavis /var/virusmails

chmod 777 /var/virusmails

cp amavisd\_init.sh /etc/init.d/amavisd

ln -s /usr/local/sbin/amavisd /usr/sbin/amavisd

chkconfig amavisd on

### 配置amavis

检查修改下方内容：

vim /etc/amavisd.conf

$max\_servers = 200; # num of pre-forked children (2..30 is common), -m

$daemon\_user = 'amavis'; # (no default; customary: vscan or amavis), -u

$daemon\_group = 'amavis'; # (no default; customary: vscan or amavis), -g

$mydomain = 'quanshi.com'; # a convenient default for other settings

$MYHOME = '/var/amavis'; # a convenient default for other settings, -H

$TEMPBASE = "$MYHOME/tmp"; # working directory, needs to exist, -T

$ENV{TMPDIR} = $TEMPBASE; # environment variable TMPDIR, used by SA, etc.

$QUARANTINEDIR = '/var/virusmails'; # -Q

@mynetworks = qw( 127.0.0.0/8 [::1] [FE80::]/10 [FEC0::]/10

10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 203.174.107.0/24 203.174.98.0/24 172.31.64.0/24 220.181.97.0/24 14.215.129.0/24 119.147.82.72 203.174.112.106);

#$inet\_socket\_port = 10024; # listen on this local TCP port(s)

$inet\_socket\_port = [10024,10026]; # listen on multiple TCP ports

virus\_admin\_maps => ["yufei.chen\@$mydomain"],

spam\_admin\_maps => ["yufei.chen\@$mydomain"],

forward\_method => 'smtp:[127.0.0.1]:10027',

$sa\_tag\_level\_deflt = 14; # add spam info headers if at, or above that level

$sa\_tag2\_level\_deflt = 14; # add 'spam detected' headers at that level

$sa\_kill\_level\_deflt = 14.7; # triggers spam evasive actions (e.g. blocks mail)

$sa\_dsn\_cutoff\_level = 14; # spam level beyond which a DSN is not sent

$sa\_crediblefrom\_dsn\_cutoff\_level = 13; # likewise, but for a likely valid From

# $sa\_quarantine\_cutoff\_level = 25; # spam level beyond which quarantine is off

$penpals\_bonus\_score = 8; # (no effect without a @storage\_sql\_dsn database)

$penpals\_threshold\_high = $sa\_kill\_level\_deflt; # don't waste time on hi spam

$bounce\_killer\_score = 50; # spam score points to add for joe-jobbed bounces

$sa\_mail\_body\_size\_limit = 400\*1024; # don't waste time on SA if mail is larger

$sa\_local\_tests\_only = 0; # only tests which do not require internet access?

$virus\_admin = "yufei.chen\@$mydomain"; # notifications recip.

$mailfrom\_notify\_admin = "yufei.chen\@$mydomain"; # notifications sender

$mailfrom\_notify\_recip = "yufei.chen\@$mydomain"; # notifications sender

$mailfrom\_notify\_spamadmin = "spam.police\@$mydomain"; # notifications sender

@addr\_extension\_virus\_maps = ('virus');

@addr\_extension\_banned\_maps = ('banned');

@addr\_extension\_spam\_maps = ('spam');

@addr\_extension\_bad\_header\_maps = ('badh');

$MAXLEVELS = 14;

$MAXFILES = 3000;

$MIN\_EXPANSION\_QUOTA = 100\*1024; # bytes (default undef, not enforced)

$MAX\_EXPANSION\_QUOTA = 500\*1024\*1024; # bytes (default undef, not enforced)

$sa\_spam\_subject\_tag = '\*\*\*Spam\*\*\* ';

$defang\_virus = 1; # MIME-wrap passed infected mail

$defang\_banned = 1; # MIME-wrap passed mail containing banned name

# for defanging bad headers only turn on certain minor contents categories:

$defang\_by\_ccat{CC\_BADH.",3"} = 0; # NUL or CR character in header

$defang\_by\_ccat{CC\_BADH.",5"} = 1; # header line longer than 998 characters

$defang\_by\_ccat{CC\_BADH.",6"} = 1; # header field syntax error

$myhostname = 'mailcentermaster.quanshi.com'; # must be a fully-qualified domain name!

$notify\_method = 'smtp:[127.0.0.1]:10025';

$forward\_method = 'smtp:[127.0.0.1]:10025'; # set to undef with milter!

$final\_virus\_destiny = D\_REJECT;

$final\_banned\_destiny = D\_REJECT;

$final\_spam\_destiny = D\_DISCARD; #!!! D\_DISCARD / D\_REJECT

$final\_bad\_header\_destiny = D\_PASS;

qr'.\.(exe|vbs|pif|scr|cpl|bat|cmd|com)$'i, # banned extension - basic+cmd

@av\_scanners = (

['ClamAV-clamd',

\&ask\_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.sock"],

qr/\bOK$/m, qr/\bFOUND$/m,

qr/^.\*?: (?!Infected Archive)(.\*) FOUND$/m ],

### 测试amavis

/usr/local/sbin/amavisd debug

### 开机自启动

chkconfig amavisd on

### 添加bcc用户用于邮件备份

useradd bcc

## 邮件系统调优

### 调节amavisd进程数和邮件处理速度

**vim /etc/amavisd**

$max\_servers = 200; # num of pre-forked children (2..30 is common),-m

**vim /etc/postfix/master.cf**

amavis unix - - n - 200 smtp

### 调节ldapDB配置

**vim /var/lib/ldap/DB\_CONFIG**

set\_cachesize 1 536870912 1

set\_lk\_max\_lockers 6000

set\_lk\_max\_locks 6000

set\_lk\_max\_objects 6000

set\_lg\_max 604857600

set\_lg\_bsize 60971520

set\_flags DB\_LOG\_AUTOREMOVE

### 设置postfix的并发量

**vim /etc/postfix/main.cf**

default\_process\_limit = 400

**vim /etc/postfix/master.cf**

smtp inet n - n - 400 smtpd

### 配置防火墙

在ens192上配置防火墙

firewall-cmd --permanent --add-service smtp

firewall-cmd --permanent --add-service pop3

firewall-cmd --permanent --add-service ftp

firewall-cmd --permanent --add-service imap

firewall-cmd --permanent --add-service http

firewall-cmd --permanent --add-port=25/tcp

firewall-cmd --permanent --add-port=110/tcp

firewall-cmd --permanent --add-port=465/tcp

firewall-cmd --permanent --add-port=995/tcp

systemctl enable firewalld

systemctl restart firewalld

### 防火墙的替代方法

原理：根据postfix的main.cf里检查access文件，将验证失败次数超过50次的ip加入拒绝列表

**vim authfailed-joinaccess.sh**

cat /root/maillog| grep SASL\ LOGIN\ authentication\ failed | awk -F '[' '{print $3}' | awk -F ']' '{print $1}' | grep -v "^$" | sort | uniq -c | awk '$1>=50 {print $2}' > authfailedleg50ip

for authfailedip in `cat authfailedleg50ip`

do

failedip=`grep $authfailedip /etc/postfix/access`

if [ $? == 1 ]

then

echo $authfailedip reject >> /etc/postfix/access

fi

done

添加计划任务

vim /etc/crontab

\*/5 \* \* \* \* /root/script/authfailed-joinaccess.sh

0 10 \* \* \* postmap /etc/postfix/access

## 安装roundcubemail

### 下载完整版

wget https://github.com/roundcube/roundcubemail/releases/download/1.3.8/roundcubemail-1.3.8-complete.tar.gz

tar xf roundcubemail-1.3.8-complete.tar.gz

cp roundcubemail-1.3.8 /var/www/html/roundcubemail

### 创建数据库

CREATE DATABASE roundcubemail CHARACTER SET utf8 COLLATE utf8\_general\_ci;

### 授权

GRANT ALL PRIVILEGES ON roundcubemail.\* TO roundcube@localhost IDENTIFIED BY 'password';

### 初始化数据库

cd /var/www/html/roundcubemail/

mysql -uroot -p roundcubemail < SQL/mysql.initial.sql

### 配置文件

cd /var/www/html/roundcubemail/config

vim config.inc.php

修改MySQL连接

$config['db\_dsnw'] = 'mysql://roundcube:password@localhost/roundcubemail';

配置主机

$config['default\_host'] = 'mailcentermaster.quanshi.com';

$config['smtp\_server'] = 'mailcentermaster.quanshi.com';

配置默认主题（可以不改）

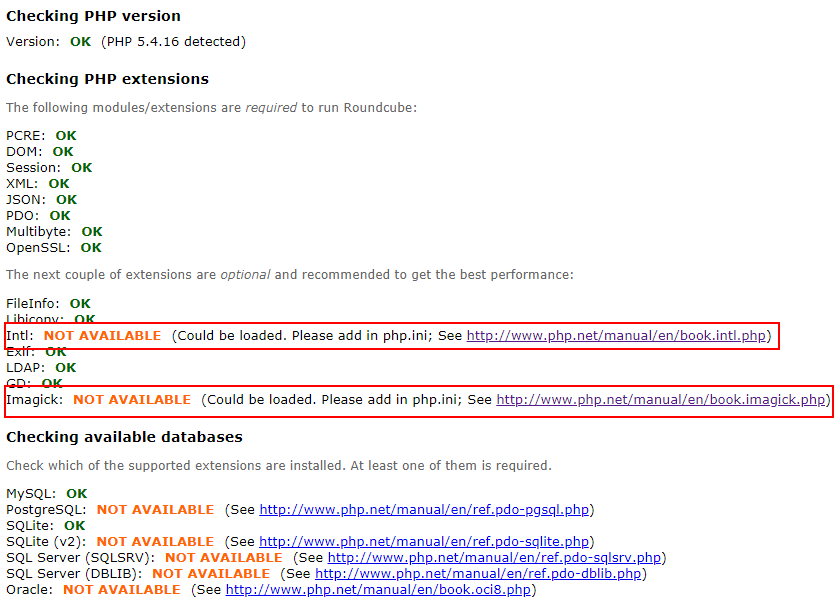
$config['skin'] = 'classic';

配置启用安装

$config['enable\_installer'] = true;

### 访问网址安装

http://192.168.241.224/roundcubemail/installer/index.php



### 修改php.ini时区

vim /etc/php.ini

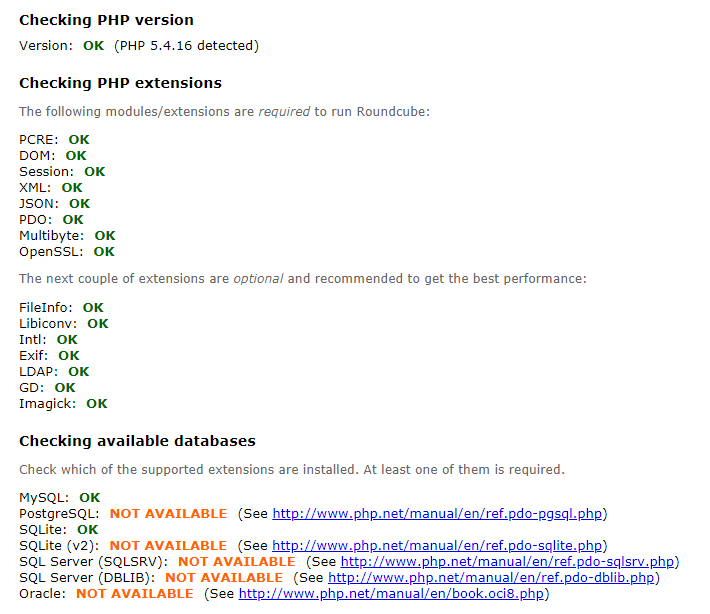
date.timezone = Asia/Shanghai

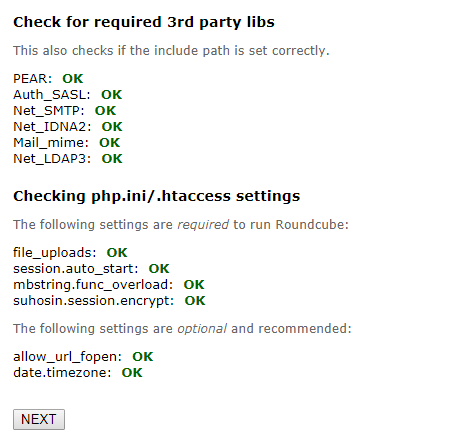
### 安装PHP模块

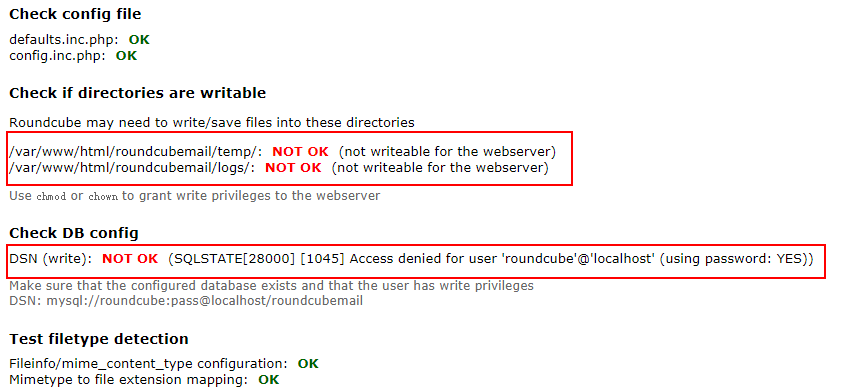
yum install php-pecl-imagick php-intl

systemctl restart httpd

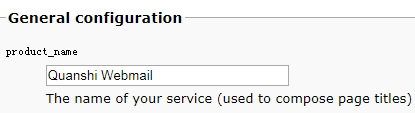
以下状态即完成检查

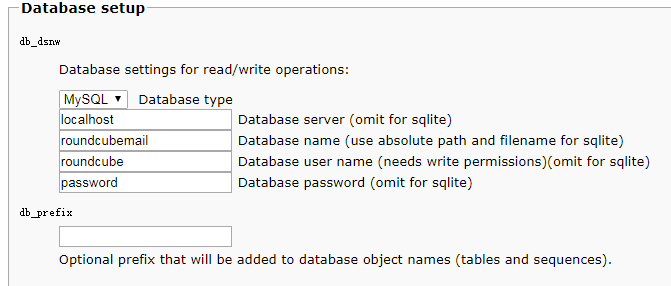


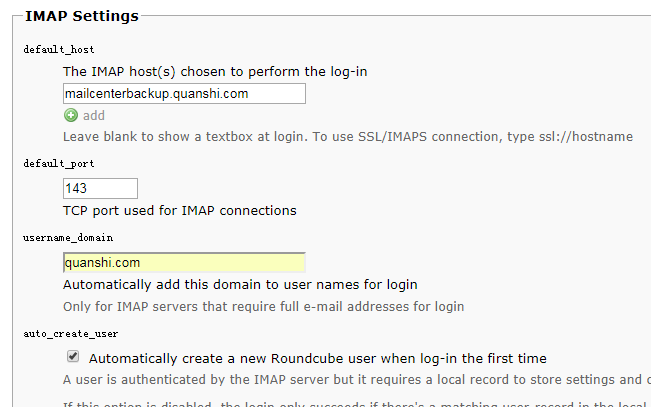


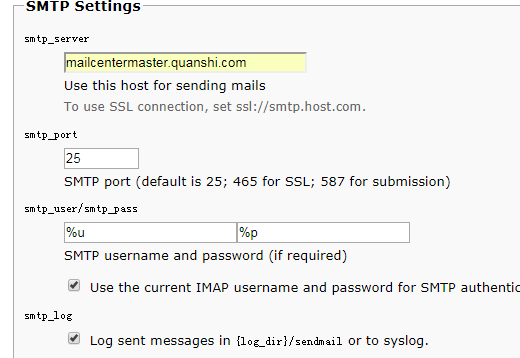


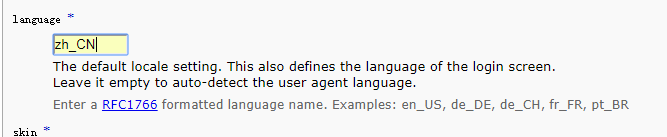
### 点击网页上2.创建配置文件











### 安装完成移除安装文件

mv /var/www/html/roundcubemail/installer /var/www/html/roundcubemail/installerremove

vim /var/www/hmtl/roundcubemail/config/config.inc.php

$config['enable\_installer'] = false;

### 配置自定义图片

/var/www/html/roundcubemail/skins/larry/images/watermark.jpg





/var/www/html/roundcubemail/skins/larry/images/roundcube\_logo.png



C:\Users\yufei.chen\Desktop\bak\roundcube_logo.png

## 同步home文件夹到备份服务器

### 在备服务器安装rsync-server服务

yum install rsync-server

systemctl enable rsyncd

### 配置rsync的用户密码

**vim /etc/rsync.pass**

rsync:rsync@123

### 配置rsync目录

**vim /etc/rsync.conf**

pid file = /var/run/rsyncd.pid

port = 873

address = 192.168.241.224

uid = root

gid = root

read only = no

#limit access to private LANs

hosts allow=192.168.241.0/24

hosts deny=\*

max connections = 10

[home]

path = /home

list=yes

#ignore errors

auth users=rsync

secrets file = /etc/rsync.pass

comment = This is mail data

[postfix]

path = /etc/postfix

list=yes

#ignore errors

auth users=rsync

secrets file = /etc/rsync.pass

comment = This is postfix conf

[spam]

path = /etc/mail/spamassassin

list=yes

#ignore errors

auth users=rsync

secrets file = /etc/rsync.pass

comment = This is spam conf

[maillog]

path = /var/log

list=yes

#ignore errors

auth users=rsync

secrets file = /var/log/maillog

comment = This is maillog

### 在主服务器安装rsync客户端

yum install rsync

### 在主服务器上安装sersync

下载wget https://github.com/wsgzao/sersync/archive/master.zip

解压unzip master.zip

**进入目录**

cd sersync-master

解压sersync2.5.4\_64bit\_binary\_stable\_final.tar.gz

mv GNU-Linux-x86 /use/local/sersync

**链接执行文件**

ln -s /usr/local/sersync/sersync2 /usr/bin/sersync2

**创建密码文件**

echo "rsync@123" > /usr/local/sersync/user.pass

**配置sersync找到以下标签修改**

vim /usr/local/sersync/confxml.xml

<localpath watch="/home/"> 本地要同步到备的目录

<remote ip="192.168.21.193" name="home"/> 备服务器ip和rsync模块

<commonParams params="-artu"/> rsync选项

<auth start="true" users="rsync" passwordfile="/usr/local/sersync/user.pass"/> rsync密码

<failLog path="/var/log/rsync\_fail\_log.sh" timeToExecute="60"/> 错误日志

### 配置定期同步文件

## 定期删除病毒邮件

vim /etc/crontab

0 22 \*/14 \* \* /script/spamdel.sh >/etc/null 2>&1

vim /root/script/spamdel.sh

#!/bin/sh

find /var/virusmails/ -type f -atime +7 | xargs rm