**邮件服务安装步骤**

**说明：**此文档主要是快速安装文档，详细说明请查看详细部署文档，主要是基本postfix+ldap+dovecot+amavis+clamav+spam等完整邮件系统。

1. **安装服务系统：**

**请参考安装centos6.4 x86\_64 系统文档。**

1. **停用iptables**

/etc/init.d/iptables stop

/etc/init.d/ip6tables stop

chkconfig iptables off

1. **停用selinux**

setenforce 0

vi /etc/sysconfig/selinux

SELINUX=enforcing

改为

SELINUX=disabled

1. **绑定服务器ip地址**

vim /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=em1

HWADDR=14:FE:B5:D9:10:F4

TYPE=Ethernet

UUID=d6766c6a-6504-406c-883d-9c143e696087

ONBOOT=yes

NM\_CONTROLLED=yes

BOOTPROTO=none

IPADDR=192.168.11.1

NETMASK=255.255.255.0

GATEWAY=192.168.11.254

DNS1=192.168.240.217

IPV4\_FAILURE\_FATAL=yes

IPV6INIT=no

1. **设置代理**

export http\_proxy=http://192.168.21.248:3128

1. **安装yum源**

设置yum源，此版本因官方源提供支持且速度较快，建议不需要更改yum源文件。

缓存yum源到本地

yum makecache

更新目前服务器的文件包

yum update

1. **更改主机名**

vi /etc/sysconfig/network

NETWORKING=yes

NETWORKING\_IPV6=no

HOSTNAME=mailcenter.quanshi.com

1. **本地dns解析**

vi /etc/hosts

192.168.240.216 mailcenter.quanshi.com quanshi.com

#HK Relay

203.174.112.106 mailcenter3.quanshi.com

1. **dns文件配置**

vi /etc/resolv.conf

search quanshi.com

nameserver 192.168.240.217

nameserver 192.168.240.236

1. **同步服务器时间**

写入时间同步脚本

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

#!/bin/sh

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

EOF

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

1. **安装服务器基本操作辅助工具**

因centos 6.4 是最小化安装，所以多个工具并没有随系统安装而安装。

yum -y install vim

yum -y install wget

yum -y install ntpdate

yum -y install bind-utils

yum -y install telnet

yum -y install openssh-clients

yum -y install setuptool

yum -y install nss-pam-ldapd

yum -y install httpd\*

yum -y install php-\*

yum -y install gcc\*

1. **安装并配置postfix**

yum -y install postfix\*

**配置postfix**

cp -r /etc/postfix/main.cf /etc/postfix/main.cf.bak

cd /etc/postfix/

postconf -n >main1.cf

mv main1.cf main.cf

vi /etc/postfix/main.cf

添加postfix域名环境

将系统中默认mydestination注销掉

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

#mailgroup

home\_mailbox = Maildir/

inet\_interfaces = all

mydomain = quanshi.com

myhostname = mailcenter.quanshi.com

mydestination = $myhostname, localhost,$mydomain, localhost

mynetworks = 127.0.0.0/8

myorigin = $mydomain

relay\_domains = $mydestination

message\_size\_limit = 22485760

**启动并设置开机启动**

/etc/init.d/postfix restart

chkconfig postfix on

1. **安装并配置dovecot**

yum -y install dovecot\*

由于dovecot 2.0以上版本目录结构发送了改变。所以我们在不同的配置文件中配置不同的功能。

进入dovecot 目录

cd /etc/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

**启动并设置开机启动**

/etc/init.d/dovecot restart

chkconfig dovecot on

1. **安装并配置ldap**

yum -y install openldap\*

因ldap新版本的目录结构改变，默认没有slapd.conf文件

从安装包中将slapd.conf复制到ldap目录

cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf

从安装包中将DB文件复制到ldap数据库目录

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

备份slapd.conf 文件

cp /etc/openldap/slapd.conf{,.bak}

将主服务器217的ldap数据复制到此服务器上

scp -r [root@192.168.240.217:/backup/ldap/gnetis.ldif ./](mailto:root@192.168.240.217:/backup/ldap/gnetis.ldif%20./)

生成mail.schema文件和alias.schema文件

vim /etc/openldap/schema/alias.schema

attributetype ( 1.33.6.1.4.1.6333.333.33.3

NAME 'mailaliasname'

SUP name )

objectclass ( 1.33.6.1.4.1.6111.111.11.1

NAME 'mailaliasuser'

SUP inetOrgPerson

STRUCTURAL

MAY mailaliasname )

objectclass (1.33.6.1.4.1.6222.222.22.2

NAME 'aliasgroup'

SUP top

STRUCTURAL

MUST ( mail $ mailaliasname ) )

配置ldap配置文件做如下更改：（注意格式）

vim /etc/openldap/slapd.conf

include /etc/openldap/schema/alias.schema

#database config

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

#database monitor

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

database bdb

suffix "dc=gnetis,dc=com"

checkpoint 1024 15

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

rootpw \*\*\*\*\*\*

directory /var/lib/ldap

loglevel 256

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

updateref ldap://ldap1.gnetis.com

注意此处为从服务器，请在主服务器217上确认添加了如下内容：

replica host=192.168.240.216:389 binddn="cn=Manager,dc=gnetis,dc=com" bindmethod=simple credentials=\*\*\*\*\*\*

**启用ldap日志功能**

vim /etc/rsyslog.conf

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

/etc/init.d/rsyslog restart

**清空缓存文件中的默认文件**

rm -rf slapd.d/\*

**导入ldap数据**

slapadd -l gnetis.ldif

指定当前slapd.conf配置文件写入到缓存文件中

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/\*

**启动并设置开机启动服务**

/etc/init.d/slapd restart

chkconfig slapd on

1. **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。

1. **整合ldap和dovecot**

配置ldap主配置文件

cd /etc/dovecot/conf.d

vim auth-ldap.conf.ext

passdb {

driver = ldap

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

}

userdb {

driver = ldap

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

}

配置生成dovecot-ldap.conf文件

vi /etc/dovecot/dovecot-ldap.conf

hosts = localhost

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

dnpass = \*\*\*\*\*\* (以实际密码为主)

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

**重启服务**

/etc/init.d/dovecot restart

设置帐号读写权限

chmod 777 /home

做简单的账户邮件收发测试

telnet mailcenter.quanshi.com 25

Trying 192.168.240.215...

Connected to mailcenter.quanshi.com(192.168.240.215).

Escape character is '^]'.

220 mailcenter.gnetis.comESMTP Postfix

helo mailcenter.quanshi.com

250 mailcenter.quanshi.com

mail from: qiang.wang@quanshi.com

250 2.1.0 Ok

rcpt to: shuaishuai.zhang@quanshi.com

250 2.1.5 Ok

data

354 End data with <CR><LF>.<CR><LF>

subject:a test mail

helo!

this is test mail

250 2.0.0 Ok: queued as B5BBA241E52

quit

221 2.0.0 Bye

Connection closed by foreign host

查看邮件

telnet mailcenter.quanshi.com 110

Trying 192.168.240.214...

Connected to mailcenter.quanshi.com (192.168.240.214).

Escape character is '^]'.

+OK Dovecot ready.

user shuaishuai.zhang

+OK

pass 123456

+OK Logged in.

list

+OK 1 messages:

1 459

quit

+OK Logging out.

Connection closed by foreign host.

1. **安装并配置sasl**

yum -y install cyrus-sasl cyrus-sasl-devel cyrus-sasl-lib cyrus-sasl-md5 cyrus-sasl-plain cyrus-sasl-ldap cyrus-sasl-ntlm cyrus-sasl-gssapi

配置机制为ldap

vi /etc/sysconfig/saslauthd

MECH=ldap

认证模式（一般默认就是saslauthd模式，为不出错误最好做一下检查）

vi /etc/sasl2/smtpd.conf

pwcheck\_method: saslauthd

mech\_list: plain login

创建sasl绑定认证文件

vi /etc/saslauthd.conf

ldap\_servers: ldap://127.0.0.1

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

ldap\_bind\_pw: \*\*\*\*\*\*(以实际密码为主)

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

ldap\_version: 3

ldap\_auth\_method: bind

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

**启动并设置开机启动**

/etc/init.d/saslauthd restart

chkconfig saslauthd on

配置postfix启用sasl认证

vi /etc/postfix/main.cf

#sasl

smtpd\_sasl\_auth\_enable = yes

broken\_sasl\_auth\_clients = yes

smtpd\_sasl\_local\_domain = $mydomain

smtpd\_reject\_unlisted\_sender = yes

smtpd\_helo\_required = yes

smtpd\_delay\_reject = yes

smtpd\_client\_restrictions =

permit\_mynetworks,

permit\_sasl\_authenticated,

permit\_tls\_all\_clientcerts,

permit\_tls\_clientcerts,

reject\_multi\_recipient\_bounce,

reject\_unauth\_pipelining,

reject\_invalid\_hostname,

reject\_non\_fqdn\_hostname,

# reject\_unknown\_hostname

smtpd\_sender\_restrictions =

permit\_mynetworks,

permit\_sasl\_authenticated,

reject\_sender\_login\_mismatch,

reject\_unlisted\_sender,

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\_non\_fqdn\_recipient,

reject\_unknown\_recipient\_domain,

permit\_sasl\_authenticated,

reject\_unauth\_destination

smtpd\_sasl\_security\_options = noanonymous

**配置完成重启服务**

/etc/init.d/postfix restart

**测试sasl认证**

**测试telnet是否可以通过冒充帐号登录或者发送邮件**

**测试outlook客户端是否不加允许smtp认证可以通过**

1. **设置Postfix别名和别名组**

vi /etc/postfix/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

vi /etc/postfix/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

生成postmap文件

postmap /etc/postfix/ldap\_alias

postmap /etc/postfix/ldap\_aliasgroup

**将别名添加到main.cf文件中**(注意：将原有的别名指定文件注销掉)

vi /etc/postfix/main.cf

#mail alias

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

**别名组，别名发邮件测试**

**测试发送邮件到别名是否正常。**

**测试发送邮件到别名组是否正常。**

1. **邮件去重**

vim /etc/postfix/main.cf

#qu chong

enable\_original\_recipient = no

1. **邮件别名伪装**

vim /etc/postfix/main.cf

#yu ming wei zhuang

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

将后缀名为gnetis.com的邮件地址改写为quanshi.com

vim /etc/postfix/my\_generic\_maps

@gnetis.com @quanshi.com

生成数据库文件

postmap /etc/postfix/my\_generic\_maps

1. **安装并设置ssl认证**

安装ssl包

yum -y install openssl\*

将源服务器上的证书下载到本地

创建本地ssl存放目录

mkdir /etc/postfix/ssl

scp -r root@192.168.240.216:/etc/postfix/ssl/smtpd.pem /etc/postfix/ssl/

scp -r root@192.168.240.216:/etc/postfix/ssl/cert.pem /etc/postfix/ssl/

配置postfix使用ssl证书

vi /etc/postfix/main.cf

#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/smtpd.pem

smtpd\_tls\_loglevel = 1

smtpd\_tls\_received\_header = yes

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

vi /etc/postfix/master.cf (注意格式)

smtps inet n - n - - smtpd

-o smtpd\_tls\_wrappermode=yes

-o smtpd\_sasl\_auth\_enable=yes

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

**dovecot支持ssl认证**

vim /etc/dovecot/conf.d/10-ssl.conf

ssl\_disable = no

ssl\_cert = </etc/pki/dovecot/certs/dovecot.pem

ssl\_key = </etc/pki/dovecot/private/dovecot.pem

ssl\_cipher\_list = ALL:!LOW:!SSLv2:!EXP:!aNULL

**重起服务**

/etc/init.d/postfix restart

/etc/init.d/dovecot restart

1. **启用imap日志跟踪**

vim /etc/dovecot/conf.d/20-imap.conf

protocol imap {

mail\_plugins = mail\_log

}

vim /etc/dovecot/conf.d/10-logging.conf

plugin {

# Events to log. Also available: flag\_change append

mail\_log\_events = delete undelete expunge copy mailbox\_delete mailbox\_rename

# Group events within a transaction to one line.

mail\_log\_group\_events = no

# Available fields: uid, box, msgid, from, subject, size, vsize, flags

# size and vsize are available only for expunge and copy events.

mail\_log\_fields = uid box msgid size

}

**重启dovecot服务**

/etc/init.d/dovecot restart

测试使用outlook帐号以imap的方式登录，查看/var/log/dovecot\_info.log记录

1. **安装Webmail Extmail**

**下载并解压extmail包**

**因官网不支持直接下载软件包方式，此处只提供下载页面**

[**http://www.extmail.org/download**](http://www.extmail.org/download)

**解压下载完成文件**

tar zxvf extmail-1.2.tar.gz

mv extmail-1.2 /var/www/html/extmail

**配置安装httpd服务**

vim /etc/httpd/conf/httpd.conf

<VirtualHost \*:80>

ServerAdmin qiang.wang@quanshi.com

DocumentRoot /var/www/html/extmail/

ScriptAlias /extmail/cgi /var/www/html/extmail/cgi

Alias /extmail /var/www/html/extmail/html

ServerName extmail.quanshi.com

</VirtualHost>

**配置Extmail服务文件**

**进入Extmail目录并复制生成配置文件**

cd /var/www/html/extmail/

cp webmail.cf.default webmail.cf

赋予相关httpd读写权限

chown -R apache:apache /var/www/html/extmail

编辑配置文件

vim /var/www/html/extmail/webmail.cf

SYS\_CONFIG = /var/www/html/extmail/

SYS\_LANGDIR = /var/www/html/extmail/lang

SYS\_TEMPLDIR = /var/www/html/extmail/html

SYS\_HTTP\_CACHE = 0

SYS\_SMTP\_HOST = 127.0.0.1

SYS\_SMTP\_PORT = 25

SYS\_SMTP\_TIMEOUT = 5

SYS\_SPAM\_REPORT\_ON = 0

SYS\_SPAM\_REPORT\_TYPE = dspam

SYS\_SHOW\_WARN = 0

SYS\_IP\_SECURITY\_ON = 1

SYS\_PERMIT\_NOQUOTA = 1

SYS\_SESS\_DIR = /tmp

SYS\_UPLOAD\_TMPDIR = /tmp

SYS\_LOG\_ON = 1

SYS\_LOG\_TYPE = syslog

SYS\_LOG\_FILE = /var/log/extmail.log

SYS\_SESS\_TIMEOUT = 0

SYS\_SESS\_COOKIE\_ONLY = 1

SYS\_USER\_PSIZE = 10

SYS\_USER\_SCREEN = auto

SYS\_USER\_LANG = zh\_CN

SYS\_APP\_TYPE = WebMail

SYS\_USER\_TEMPLATE = default

SYS\_USER\_CHARSET = utf-8

SYS\_USER\_TRYLOCAL = 1

SYS\_USER\_TIMEZONE = +0800

SYS\_USER\_CCSENT = 1

SYS\_USER\_SHOW\_HTML = 1

SYS\_USER\_COMPOSE\_HTML = 1

SYS\_USER\_CONV\_LINK =1

SYS\_USER\_ADDR2ABOOK = 1

SYS\_MESSAGE\_SIZE\_LIMIT = 15242880

SYS\_MIN\_PASS\_LEN = 2

SYS\_MFILTER\_ON = 1

SYS\_NETDISK\_ON = 0

SYS\_SHOW\_SIGNUP = 1

SYS\_DEBUG\_ON = 1

SYS\_AUTH\_TYPE = ldap

SYS\_AUTH\_SCHEMA = vpopmail1

SYS\_CRYPT\_TYPE = cleartext

SYS\_LDAP\_BASE = dc=users,dc=gnetis,dc=com

SYS\_LDAP\_RDN = cn=Manager,dc=gnetis,dc=com

SYS\_LDAP\_PASS = g@net-

SYS\_LDAP\_HOST = localhost

SYS\_LDAP\_ATTR\_USERNAME = uid

SYS\_LDAP\_ATTR\_DOMAIN = mtsv1.com

SYS\_LDAP\_ATTR\_PASSWD = userPassword

SYS\_LDAP\_ATTR\_CLEARPW = clearPassword

SYS\_LDAP\_ATTR\_HOME = homeDirectory

**安装perl源CPAN包(安装extmail所需的CGI包)**

yum -y install perl-CPAN

**执行cpan安装**

perl -MCPAN -e shell或cpan

提示自动安装写入yes

Would you like me to configure as much as possible automatically? [yes] yes

**安装CGI包**

cpan[1]> install CGI

cpan[2]> install Unix::Syslog

cpan[3]>install Net::LDAP (若安装失败请执行yum –y install perl-LDAP)

cpan[4]> install DBI

cpan[4]> install YAML

**使用pear方式安装以下包**

pear install DB

pear install LOG

pear install Date

pear install Net\_IMAP

pear install File

**启动并设置开机启动httpd**

/etc/init.d/httpd restart

chkconfig httpd on

**开启web端的自动回复功能**

安装休假自动回复软件包

yum -y install gdbm\*

yum -y install gcc\*

mkdir -p /usr/man/man1

wget http://sourceforge.net/projects/vacation/files/latest/download

tar zxvf vacation-1.2.7.1.tar.gz

cd vacation-1.2.7.1

make ; make install

测试：web邮件收发

测试：自动转发

测试：自动回复功能

1. **启动https功能**

安装https支持包mod-ssl

yum -y install mod\_ssl

cp /etc/httpd/conf.d/ssl.conf /etc/httpd/conf.d/ssl.conf.bak

复制原服务器证书

scp root@192.168.240.216:/etc/pki/tls/certs/localhost.crt /etc/pki/tls/certs

scp root@192.168.240.216:/etc/pki/tls/private/localhost.key /etc/pki/tls/private

vim /etc/httpd/conf.d/ssl.conf

SSLCertificateFile /etc/pki/tls/certs/localhost.crt

SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

<VirtualHost \*:443>

DocumentRoot "/var/www/html/horde"

ServerName mailcenter.quanshi.com:443

重新启动httpd服务

/etc/init.d/httpd restart

1. **安装并配置clamav**

yum -y install gcc\* \*c++\* zilb\* bzip\*

wget http://downloads.sourceforge.net/clamav/clamav-0.97.8.tar.gz

groupadd clamav

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

groupadd amavis

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

tar zxvf clamav-0.97.8.tar.gz

cd clamav-0.97.8

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

make

make check

make install

**配置clamav的配置文件**

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

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

#Example

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

User amavis

ScanELF yes

ScanMail yes

ScanArchive yes

**配置病毒库升级文件**

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

给目录相应的权限

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

**启动并设置开机启动**

/usr/local/clamav/sbin/clamd

vim /etc/rc.local

/usr/local/clamav/sbin/clamd start

1. **安装并配置spamd**

使用span方式安装以下内容（必须按照顺序），安装过程有点慢，请耐心等待。

perl -MCPAN -e shell

cpan> install Net::Server

cpan> install Digest::SHA

cpan> install Net::DNS

cpan> install NetAddr::IP

cpan> install Archive::Tar

cpan> install Digest::SHA1

cpan> install Mail::SPF

cpan> install IP::Country

cpan> install Razor2::Syslog

cpan> install Net::Ident

cpan> install IO::Socket::INET6

cpan> install ExtUtils::MakeMaker

cpan> install IO::Socket::SSL

cpan> install Mail::DKIM

cpan> install Encode::Detect

**安装spamassassin**

wget http://mirrors.cnnic.cn/apache//spamassassin/source/Mail-SpamAssassin-3.3.2.tar.gz

tar zxvf Mail-SpamAssassin-3.3.2.tar.gz

cd Mail-SpamAssassin-3.3.2

perl Makefile.PL

make

make install

配置spamassassin

vim /etc/mail/spamassassin/local.cf

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

report\_safe 0

required\_score 5.0

use\_bayes 1

bayes\_auto\_learn 1

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

skip\_rbl\_checks 0

use\_razor2 1

use\_pyzor 1

dns\_available yes

header LOCAL\_RCVD Received =~ /.\*\(\S+\.qs\.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 BAYES\_99 4.300

score BAYES\_90 3.500

score BAYES\_80 3.000

score HEAD\_ILLEGAL\_CHARS 0

score SUBJ\_ILLEGAL\_CHARS 0

score DATE\_IN\_PAST\_03\_06 0

score UPPERCASE\_25\_50 0

score UPPERCASE\_50\_75 0

score UPPERCASE\_75\_100 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 BAYES\_99 0.1

score BAYES\_80 0.1

score BAYES\_60 0.1

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

#The blacklist

blacklist\_from \*@sohu.com \*@mailfb.com \*@163.com

#White list

whitelist\_from \*@quanshi.com \*@qq.com \*@126.com \*@gmail.com

header RCVD\_IN\_CBL eval:check\_rbl('bl', 'bl.anti-spam.org.cn.')

describe RCVD\_IN\_CBL Received via a relay in cbl.anti-spam.org.cn

tflags RCVD\_IN\_CBL net

header RCVD\_IN\_CDL eval:check\_rbl('dl-notfirsthop','dl.anti-spam.org.cn.')

describe RCVD\_IN\_CDL CDL: dialup sender did non-local SMTP

tflags RCVD\_IN\_CDL net

#SCORE

score RCVD\_IN\_CBL 4.0

score RCVD\_IN\_CDL 3.0

ifplugin Mail::SpamAssassin::Plugin::Shortcircuit

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

检测spamassassin是否有问题，开启bayes学习功能

sa-update

设置开机启动

cp /root/Mail-SpamAssassin-3.3.2/spamd/redhat-rc-script.sh /etc/init.d/spamd

chkconfig spamd on

1. **安装amavis框架**

wget http://www.amavis.org/amavisd-new-2.8.1.tar.gz

tar zxvf amavisd-new-2.8.1.tar.gz

创建目录并给予权限

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-2.8.1

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

配置amavis

vim /etc/amavisd.conf

$max\_servers = ***40***;

$daemon\_user =***'amavis'***;

$daemon\_group = ***'amavis'***;

$mydomain = ***'quanshi.com'***;

$inet\_socket\_port = ***10024***;

$sa\_tag\_level\_deflt = 5.0;

$sa\_tag2\_level\_deflt = ***4***;

$sa\_kill\_level\_deflt = ***5.0***;

$sa\_dsn\_cutoff\_level = 9;

virus\_admin\_maps => ["***postmaster***\@$mydomain"],

spam\_admin\_maps => ["***postmaster***\@$mydomain"],

$virus\_admin = "***postmaster***\@$mydomain";

$mailfrom\_notify\_admin = "***postmaster***\@$mydomain";

$mailfrom\_notify\_recip = "***postmaster***\@$mydomain";

$mailfrom\_notify\_spamadmin = "***postmaster***\@$mydomain";

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

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

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

$final\_virus\_destiny = D\_REJECT;

$final\_banned\_destiny = D\_REJECT;

$final\_spam\_destiny = D\_REJECT;

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

['ClamAV-clamd',

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

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

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

['Mail::ClamAV', \&ask\_clamav, "\*", [0], [1], qr/^INFECTED: (.+)/],

**测试amavis**

在测试之前，需要安装以下perl安装包

perl -MCPAN -e shell

cpan>install IO::Stringy

cpan>install MIME::Words

cpan>install Convert::BinHex

cpan>install Convert::BinHex

cpan> install Archive::Zip

cpan> install Archive::Tar

cpan> install Convert::UUlib

cpan> install HTML::Parser

cpan> install Convert::TNEF

执行测试命令

/usr/local/sbin/amavisd debug

设置amavis开机启动

cd amavisd-new-2.8.1

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

chmod +x /etc/init.d/amavisd

vi /etc/init.d/amavisd

prog="/usr/local/sbin/amavisd"

chkconfig amavisd on

运行sa-update命令

sa-update

启动amavis和spamassassin

/etc/init.d/amavisd restart

/etc/init.d/spamd restart

**整合postfix**

vim /etc/postfix/main.cf

#amavis+clamav

content\_filter = amavis:127.0.0.1:10024

vim /etc/postfix/master.cf

amavis unix - - n - 2 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 - - 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

重新启动postfix服务

1. **设置垃圾邮件内容过滤**

请注意以下内容是否和给出的一致，

cat /etc/amavisd.conf

$sa\_tag\_level\_deflt = 6.3;

$sa\_tag2\_level\_deflt = 4;

$sa\_kill\_level\_deflt = 6.3;

$sa\_dsn\_cutoff\_level = 9;

$virus\_admin = "postmaster\@$mydomain";

$mailfrom\_notify\_admin = "postmaster\@$mydomain";

$mailfrom\_notify\_recip = "postmaster\@$mydomain"; $mailfrom\_notify\_spamadmin = "postmaster\@$mydomain"; $mailfrom\_to\_quarantine = '';

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

$defang\_virus = 1;

$defang\_banned = 1;

$final\_virus\_destiny = D\_REJECT;

$final\_banned\_destiny = D\_REJECT;

$final\_spam\_destiny = D\_REJECT;

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

将过滤菜单内容复制到/etc/mail/spamassassin下（此名单在216上有）

cp Chinese\_rules\_GB2312.cf /etc/mail/spamassassin

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

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

若更改内容需要系统支持

以下操作是需要修改Chinese\_rules文件时，需要执行的命令，其它情况下下不需要的，查看系统默认的编码格式

local

更改默认编码格式为GB2312

export LANG="zh\_CN.gb2312"

export LC\_CTYPE="zh\_CN.gb2312"

重启相关服务

/etc/init.d/amavisd restart

/etc/init.d/spamd restart

测试：垃圾邮件过滤

病毒邮件过滤

黑白名单过滤功能

1. **设置内网或指定网段不进行垃圾邮件过滤**

设置amavisd配置文件

vim /etc/amavis.conf

@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 );

以上为默认网段，可自行添加不需要过滤的网段。

同时修改MYNETS策略如下

$policy\_bank{'MYNETS'} = { # mail originating from @mynetworks

originating => 1, # is true in MYNETS by default, but let's make it explicit

os\_fingerprint\_method => undef, # don't query p0f for internal clients

bypass\_spam\_checks\_maps => [1], # don't spam-check internal mail

bypass\_banned\_checks\_maps => [1], # don't banned-check internal mail

bypass\_header\_checks\_maps => [1], # don't header-check internal mail

};

将不需要过滤的域名加入白名单

vi /etc/mail/spamassassin/local.cf

whitelist\_from \*@quanshi.com

重新启动服务

/etc/init.d/spamd restart

/etc/init.d/amavisd restart

1. **邮件系统调优**

调节amavisd进程数和邮件处理速度

vim /etc/amavisd

$max\_servers = 40; # num of pre-forked children (2..30 is common),-m

vim /etc/postfix/master.cf

amavis unix - - n - 40 smtp

提升ldap库文件和多次连接的速度

vim /etc/openldap/slapd.conf

cachesize 50000000

idlcachesize 15000000

checkpoint 1024 5

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

#bing fa

default\_process\_limit = 400

vim /etc/postfix/master.cf

smtp inet n - n - 400 smtpd

1. 重启服务器

reboot