Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > CentOS

Postfix Backup MX eMail Server Anti-Spam Configuration

Posted by Vivek Gite <vivek@nixcraft.com>

According to RFC2821 the lowest-numbered records are the most preferred MX for domain. So I've a target Postfix backup server to keep the messages in a queue waiting for the primary server to become available. This ensures that if my primary MX goes down I do not loss any emails. However, spammers are connecting to my backup MX to avoid anti spam filters that are running on the primary MX server. This also hides their real IP from my primary MX. How do I configure anti-spam for my backup RHEL / CentOS 5.3 based Postfix mx server?

[1]

This is well known issue. Make sure your backup MX runs the same config in terms of spam rejection as your primary server. Try the following to improve backup eMail server anti spam configuration.

If the backup MX acts as a store-and-forward mail server

Consider the following example:

```
nixcraft.com. 86400 IN MX  10 mx01.nixcraft.net.in.
nixcraft.com. 86400 IN  MX  20 mx02.nixcraft.net.in.
```

nixcraft.com email handled by two email servers. mx02.nixcraft.net.in is your backup server. Open main.cf and append the following restrictions on mx02.nixcraft.net.in.

Only allow your own domain to accept email

Use relay_domains to relay email for two domain called nixcraft.com and cyberciti.com. Also, set lookup tables with all valid addresses in the domains that match $relay_domains i.e. only accept email for valid email address.

```
# vi /etc/postfix/main.cf
```

Modify settings as follows:

```
relay_domains = nixcraft.com, cyberciti.com, $mydestination
relay_recipient_maps = hash:/etc/postfix/relay_recipients
```

Create /etc/postfix/relay_recipients to accept email for vivek@nixcraft.com, vivek@cyberciti.com, user3@nixcraft.com and so on..

```
vivek@nixcraft.com   OK
vivek@cyberciti.com   OK
user3@nixcraft.com    OK
```

Save and close the file. Finally, update your db:

```
# postmap hash:/etc/postfix/relay_recipients
```

Anti spam via RBL

Now, add following lines main.cf to check spammer IP address using RBLs [2]. Reject all email if they do not have a valid hostname or proper email address:

```
smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks,
  reject_non_fqdn_hostname,
  reject_non_fqdn_sender,
  reject_non_fqdn_recipient,
  reject_unauth_destination,
  reject_unauth_pipelining,
  reject_invalid_hostname,
  reject_rbl_client zen.spamhaus.org
# helo required
smtpd_helo_required = yes
# disable vrfy command
disable_vrfy_command = yes

smtpd_data_restrictions =
            reject_unauth_pipelining,
            permit
```

Save and close the file. Restart / reload postfix:

```
# service postfix reload
```

There are other anti UCE settings, see Postfix anti UCE [3] cheat sheet for more information.

Nolisting mx A entry

Spammers email software does not retry higher-priority MX records. So all you have to do is create a non-existent primary mail server and a working secondary mail server, attempts to contact the primary mail server will always fail. This technique uses a non-existent primary mail server, which is compatible with all correctly configured mail servers such as Sendmail, MS-Exchange, Postfix, Qmail, Exim etc. Create BIND dns configuration as follows:

```
nixcraft.com. 86400 IN MX  10 mx01.nixcraft.net.in.
nixcraft.com. 86400 IN  MX  20 mx02.nixcraft.net.in.
nixcraft.com. 86400 IN  MX  30 mx03.nixcraft.net.in.
nixcraft.com. 86400 IN  MX  40 mx04.nixcraft.net.in.
```

Where,

- **mx02.nixcraft.net.in** - Runs your actual primary MX with anti spam and anti virus configurations.
- **mx03.nixcraft.net.in** - Your backup mx server with anti spam / virus and act as store and forward server for mx02.nixcraft.net.in.
- **mx01.nixcraft.net.in** and **mx04.nixcraft.net.in** are nolist MX servers. They can either be dead (or point to non existing IP) or you can run SMTP on port 25 that always returns 4xx error so that legitimate MTA to retry on a lower numbered MX server. nolist MX servers can also used to get more information about spammers to blacklist them. Google for "spam filtering services that offer free nolist servers" specifically for botnet data harvesting.

Greylisting Backup MX

Postfix can be configured to temporarily reject any email from a sender it does not recognize. If the mail is legitimate, the originating server will try again and the email is accepted. If the mail is from a spammer it will probably not be retried since a spammer goes through thousands of email addresses and cannot afford the time delay to retry. See how to configure postfix greylist policy server [4].

Spamassassin+Amavis+Clamd For Backup MX Server

Spamassassin is open source mail filter, to identify spam using a wide range of heuristic tests on mail headers and body text. You can install Spamassassin spam checking on your backup server. Emails found to be Spam (with higher spam score) will be drop out before reaching your primary email server. You can also use Clamav / Amavis to scan email and drop or forward infected emails. Install spamassassin, clamd and amavisd-new using yum or apt-get commands (turn on EPEL repo under RHEL / CentOS [5] to install the following packages):

```
# yum install clamav-server amavisd-new spamassassin
```

- **clamav-server** : Clam Antivirus scanner server
- **amavisd-new** : amavisd-new is a high-performance and reliable interface between Postfix and virus scanners, and/or
  Mail::SpamAssassin Perl module.

- **spamassassin** : Spam filter for email which can be invoked from mail delivery agents or in our case via amavisd-new

Once done, add as the following to your **/etc/postfix/main.cf**:

```
content_filter=smtp-amavis:[127.0.0.1]:10024
```

Save and close the file. Open **/etc/postfix/master.cf** and add the following settings:

```
smtp-amavis unix - - n - 2 smtp
  -o smtp_data_done_timeout=2400
  -o smtp_send_xforward_command=yes
  -o disable_dns_lookups=yes
  -o max_use=20
127.0.0.1:10025 inet n - n - - smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_delay_reject=no
  -o smtpd_client_restrictions=permit_mynetworks,reject
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks_style=host
  -o mynetworks=127.0.0.0/8
  -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 receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_address_
```

Save and close the file. Also, update **/etc/amavisd/amavisd.conf** with required settings.

```
$daemon_user  = 'amavis';     # (no default;  customary: vscan or amavis), -u
$daemon_group = 'amavis';     # (no default;  customary: vscan or amavis), -g
$mydomain = 'nixcraft.net.in';   # a convenient default for other settings
$log_level = 1;              # verbosity 0..5, -d
$DO_SYSLOG = 1;              # log via syslogd (preferred
$inet_socket_port = 10024;   # listen on this local TCP port(s) (see $protocol)
$sa_tag_level_deflt  = -999;  # add spam info headers if at, or above that level
$sa_tag2_level_deflt = 6.31; # add 'spam detected' headers at that level
$sa_kill_level_deflt = 6.31; # triggers spam evasive actions
$sa_dsn_cutoff_level = 10;   # spam level beyond which a DSN is not sent
$virus_admin               = 'postmaster\@nixcraft.net.in';                    # notificati
$mailfrom_notify_admin     = 'postmaster\@nixcraft.net.in';                    # notificati
$mailfrom_notify_recip     = 'postmaster\@nixcraft.net.in';                    # notificati
$mailfrom_notify_spamadmin = 'postmaster\@nixcraft.net.in';                    # notificati
$mailfrom_to_quarantine = 'postmaster\@nixcraft.net.in'; # null return path; uses original
$sa_spam_subject_tag = '***SPAM*** ';
$myhostname = 'mx02.nixcraft.net.in';  # 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!
# add your server public ip, private ip,
@inet_acl = qw( 203.1.2.3 127/8  10.10.29.11);
```

Save and close the file. Update spamassassin settings in /var/spool/amavisd/:

```
# usermod -s /bin/bash amavis
# passwd amavis
# su - amavis
$ razor-admin -discover
$ razor-admin -create
$ razor-admin -register -l -user=vivek@nixcraft.co.in -pass=somePassword
$ cd .spamassassin
$ cp /usr/share/spamassassin/user_prefs.template user_prefs
$ exit
# usermod -s /sbin/nologin amavis
```

Update /etc/clamd.d/amavisd.conf as follows:

```
# Use system logger.
LogSyslog yes

# Specify the type of syslog messages - please refer to 'man syslog'
# for facility names.
LogFacility LOG_MAIL

# This option allows you to save a process identifier of the listening
# daemon (main thread).
PidFile /var/run/amavisd/clamd.pid

# Remove stale socket after unclean shutdown.
# Default: disabled
FixStaleSocket yes

# Run as a selected user (clamd must be started by root).
User amavis

# Path to a local socket file the daemon will listen on.
LocalSocket /var/spool/amavisd/clamd.sock
```

Update **/etc/mail/spamassassin/local.cf** as follows:

```
required_hits 6.31
report_safe 1
rewrite_subject         0
# Enable the Bayes system
use_bayes               1
# Enable Bayes auto-learning
auto_learn              1
```

Save and close the file. Finally, restart postfix and other services:

```
# service [6] clamd.amavisd start
# service amavisd start
# service postfix restart
```

Turn services on boot:

```
# chkconfig [7] clamd.amavisd on
# chkconfig [7] amavisd on
# chkconfig [7] postfix on
```

Now, check your /var/log/maillog for any errors or details:

```
# netstat -tulpn -A inet| egrep ':25|:1002?'
# tail -f /var/log/maillog
```

Above configuration will open the following ports on server:

1. 10024 - Amavisd
2. 10025 - Amavisd will communicate back the results to Postfix
3. 25 - SMTP Port

A note about same priority mx servers

You can point the mail servers, all with the same priority. It offers the following benfits:

- Load balancing

- Centralized user mail managment via LDAP or MySQL / PGSQL
- Centralized virus scanning
- Centralized Spam scanning

Sample dns records:

```
nixcraft.com. 86400 IN MX  10 mx01.nixcraft.net.in.
nixcraft.com. 86400 IN  MX  10 mx02.nixcraft.net.in.
nixcraft.com. 86400 IN  MX  10 mx03.nixcraft.net.in.
; imap server
imap  86400 IN  A  202.54.1.2
; pop3 server - can be CNAME too
pop3  86400 IN  A  202.54.1.2
```

You may need additional servers inside your lan:

- MySQL/OpenLDAP (10.24.116.2) - Store user name, email, mailbox and other information.
- Central anti virus server (10.24.116.3) - Used by all your mx servers for scanning using TCP/IP. You can also do the same for spam scanning using TCP/IP.

Each mx server can use centralized anti spam and anti-virus server. Once scanned Postfix can deliver final mail which can be retrieved using POP3 / IMAP server.

Further Readings / References :

This FAQ assumed that you have working Postfix primary and backup server. It only covered anti spam related topics. For further details refer the following urls and respective man pages:

- Postfix [8]
- Spamassassin [9]
- Clamd [10]
- Amavisd [11]
- Bind [12]
- Wikipedia articles about NOListing [13] and MX record [14]

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/postfix-backup-mx-server-anti-spam/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/email-servers/**
[2] address using RBLs: **http://www.cyberciti.biz/tips/postfix-spam-filtering-with-blacklists-howto.html**
[3] anti UCE: **http://jimsun.linxnet.com/misc/postfix-anti-UCE.txt**
[4] postfix greylist policy server: **http://www.postfix.org/SMTPD_POLICY_README.html#greylist**
[5] EPEL repo under RHEL / CentOS: **http://www.cyberciti.biz/faq/rhel-fedora-centos-linux-enable-epel-repo/**
[6] service: **http://www.cyberciti.biz/faq/check-running-services-in-rhel-redhat-fedora-centoslinux/**
[7] chkconfig: **http://www.cyberciti.biz/faq/rhel5-update-rcd-command/**
[8] Postfix: **http://www.postfix.org/documentation.html**
[9] Spamassassin: **http://spamassassin.apache.org/**
[10] Clamd: **http://www.clamav.net/**
[11] Amavisd: **http://www.ijs.si/software/amavisd/**
[12] Bind: **https://www.isc.org/products/BIND**
[13] NOListing: **http://en.wikipedia.org/wiki/Nolisting**
[14] MX record: **http://en.wikipedia.org/wiki/MX_record**