Mail Server Configuration

Stefan Hornburg (Racke)

Contents

List of requirements

- Mailserver needs an MX record
- Reverse DNS record (PTR) which is not a boilerplate one
- Domain name resolves to mail server's IP
- HELO needs sane hostname too
- SPF for all domains and subdomains
- DKIM for all domains and subdomains

Test emails

Validators and Checks

- mail-tester SPAM testing
- DKIM, SPF, SpamAssassin Email Validator

Check DKIM and SPF: `https://www.mail-tester.com/spf-dkim-check`
Check SPF with lots of extra information: `https://www.spf-record.com/spf-lookup`

Commandline

Swaks is a nice tool to send test emails, e.g.

```
swaks --from="racke@linuxia.de" --to="racke@nite.si" --header="Subject: Hello world!" --server=local
```

`--tls` enables STARTTLS.

Exim

A specific from address for a local accounts can be configured in `/etc/email-addresses`:

```
stefan: racke@linuxia.de
```

TLS

Enable TLS in a local macro file, e.g. `/etc/exim4/conf.d/main/00_local_macros`:

```
MAIN_TLS_ENABLE = yes
```

Rewriting

In order to prevent emails going out from a development system to real users you can force all outgoing emails to a specific account:

```
*@* test@example.com Tt
```

Check expected mail delivery

```
$ sudo exim4 -bt test@example.de
R: dnslookup for test@example.de
test@example.de
  router = dnslookup, transport = remote_smtp
  host mx01.ionos.de [217.72.192.67] MX=10
  host mx00.ionos.de [212.227.15.41] MX=10

*** Display configuration information

{{{
~# exim -bP '+local_domains'
domainlist local_domains = @:localhost:linuxia.de:icdev.de
```

Queue

List emails in the queue:

```
~# exim -bp
```

Number of emails in the queue:

```
~# exim -bpc
815
```

Thaw all frozen emails:

```
# exiqgrep -z -i | xargs exim -Mt
Message 1kne6n-0003fU-A5 is no longer frozen
Message 1kneBc-0003w9-7A is no longer frozen
Message 1kneFz-0004BK-NF is no longer frozen
```

Remove **all** emails:

```
$  exiqgrep -i | xargs exim -Mrm
Message 1lj449-0002VX-8z has been removed
Message 1ljEag-0004uV-4h has been removed
Message 1ljKxR-0007JM-L7 has been removed
```

TLS

Security test

Use testssl.sh for this:

```
$ testssl.sh -t smtp smtp.example.com:25
```

```
$ testssl.sh -t imap imap.example.com:143
```

Debian and Ubuntu provide a testssl.sh package including a `testssl` binary.
Test a specific IP (e.g. for a set of loadbalancers):

```
$ testssl.sh -t smtp --ip=10.11.12.13 smtp.example.com:25
```

STARTTLS

```
$ openssl s_client -connect smtp.example.com:25 -starttls smtp
```

Certificates

Display certificate for IMAPS:

```
openssl s_client -connect mail.linuxia.de:993 -showcerts | openssl x509 -text
```

Postfix

Configuration

You can test the Postfix configuration with `postfix check`.
Shows all settings from `main.cf` in alphabetic order which differ from the default value:

```
~# postconf -n
```

List of default values for `main.cf`:

```
~# postconf -d
2bounce_notice_recipient = postmaster
access_map_defer_code = 450
access_map_reject_code = 554
address_verify_cache_cleanup_interval = 12h
address_verify_default_transport = $default_transport
address_verify_local_transport = $local_transport
...
```

TLS Settings

Our recommended TLS settings are:

```
tls_high_cipherlist=!aNULL:!eNULL:!CAMELLIA:HIGH:@STRENGTH
tls_preempt_cipherlist = yes
tls_ssl_options = 0x40000000

smtpd_tls_mandatory_protocols = !SSLv2,!SSLv3,!TLSv1,!TLSv1.1
smtpd_tls_protocols = !SSLv2,!SSLv3,!TLSv1,!TLSv1.1
smtpd_tls_mandatory_cipher = high
smtpd_tls_exclude_ciphers = eNULL, aNULL, LOW, EXP, MEDIUM, ADH, AECDH, MD5, DSS, ECDSA, CAMELLIA128

smtpd_use_tls=yes
smtpd_tls_ciphers=high

smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtpd_tls_loglevel = 1

smtp_use_tls=yes
smtp_tls_ciphers=high

smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

Queue

List emails in the queue:

```
~ postqueue -p
```

Flush (aka retry) all emails in the queue:

```
~ postqueue -f
```

Delete **all** emails from the queue:

```
~ postsuper -d ALL
postsuper: Deleted: 46 messages
```

Canonical maps

It is recommended to prevent email to real persons leaking from your laptop or a development server. You still want to check these emails on a personal email account.

You can achieve that with canonical maps for recipients.

Create a file `canonical_redirect` in your Postfix configuration directory (usually `/etc/postfix`) with the following contents:

```
/^.*$/ test@example.com
```

To deliver to local domains but still capture all outgoing emails use a reverse regular expression with your domain name, e.g. *mylocal.com*:

```
! /^.*@mylocal\.com$/ test.example.com
```

Prepare the file for postfix with *postmap*:

```
postmap canonical_redirect
```

Add the following line to your `main.cf` and restart postfix:

```
recipient_canonical_maps = regexp:/etc/postfix/canonical-redirect
```

Blocked by other servers

Microsoft

This applies to the following mail services:

Hotmail hotmail.*

Live live.*

Outlook outlook.*

Unblock requests

Unblock requests

Smart Network Data Service

SNDS

SPF / DKIM

Testing records:
Mail tester

SPF

The mail server needs a SPF record in DNS, e.g. for `example.com` it could look like that:

```
v=spf1 a mx ip4:93.184.216.34 ~all
```

You can lookup the SPF record from the commandline with:

```
~ dig +short -t TXT linuxia.de
"v=spf1 a mx ip4:95.216.116.54 ip4:62.192.27.135 ip4:146.0.35.17 ~all"
```

DKIM

DKIM on multiple domains with Exim4
Notes:
Rather than modifying a configuration file registered with the package system, I would create a new file for local macros, e.g. `/etc/exim4/conf.d/main/00_local_macros`.
After adding resp. updating this file, update the Exim configuration with:
`update-exim4.conf`
and restart exim:
`systemctl restart exim4`
Script for creating keys:

```
#! /bin/bash -e
#
# Copyright 2015-2021 by Stefan Hornburg (Racke) <racke@linuxia.de>
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
# License along with this program; if not, write to the Free
```

```
# Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston,
# MA 02110-1301, USA.

DKIMDIR=/etc/exim4/dkim
EXIMUSER=Debian-exim
EXIMGROUP=Debian-exim

umask o-rwx

if [ ! -d $DKIMDIR ]; then
    mkdir $DKIMDIR
    chown $EXIMUSER:$EXIMGROUP $DKIMDIR
fi

pubkey_slurp () {
    local buf
    while read line; do
        [[ $line =~ PUBLIC ]] || buf="$buf$line"
    done < $1
    pubkey=$buf
}

cd $DKIMDIR

# generate private and public key for each domain
# supplied on the command line
for domain do
    echo "Domain $domain"

    if [ -f $domain-private.pem ]; then
        echo "Private key for $domain exists!" >&2
    else
        openssl genrsa -out $domain-private.pem 2048
        chown $EXIMUSER:$EXIMGROUP $domain-private.pem
    fi

    if [ ! -f $domain.pub ]; then
        openssl rsa -in $domain-private.pem -pubout > $domain.pub
        chown $EXIMUSER:$EXIMGROUP $domain.pub
    fi

    # post DNS entry
    echo "DNS entry: "
    pubkey_slurp $domain.pub
    echo 'v=DKIM1; p='$pubkey
done
```

Creating DKIM key

```
$ openssl genrsa -out dkim_private.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................................................
.............+++++
e is 65537 (0x010001)
```

Some DNS providers don't provide enough space for DKIM records produced with key of 2048 bits. In this case you have to use 1024 bits.

Resources

DKIM for subdomains
Check new and published DNS records

Spamassassin

You need to install the Mail::DKIM Perl module in order to verify DKIM signatures:

```
apt-get install libmail-dkim-perl
```

Otherwise *all* emails will be flagged with `T_DKIM_INVALID`.

DKIM scores

`DKIM_SIGNED` signed with DKIM, not necessarily valid (default score 0.1)

`DKIM_VALID` signed with DKIM, valid (default score -0.1)

`DKIM_VALID_AU` signed with DKIM, valid, matches author's domain (default score 0.1)

So all your email should show `DKIM_VALID_AU`.

Domain names including the IP

E.g. `ds10-11-12-13.dedicated.hosteurope.de`

`HELO_DYNAMIC_IPADDR` high negative score

Testing email files

You can get a SPAM report from a EML file with spamc:

```
spamc -R < organic-spam.eml
```

This requires that the Spamassassin server is running on the same host.

Miscellaneous

Keep your mail server from blacklists.

Spamhaus is used by a lot of email providers, e.g. GMX and Yahoo, to refuse incoming emails from IPs listed there.

You can check the Spamhaus blacklists (SBL,PBL, XBL) at http://www.spamhaus.org/query/bl?ip=*IP*.

Instructions for avoiding the CBL are here.

The answer to the HELO should be fully qualified domain name (e.g. ”mail.linuxia.de”), with correct reverse DNS lookup.

ClamAV

Enable logging of found virus/malware:
`LogVerbose true` in `/etc/clamav/clamd.conf`.

Unoffical signatures for ClamAV

Debian provides *clamav-unofficial-sigs* package with a script that adds and updates really useful third party signatures for ClamAV.

We recommend the following adjustment to the configuration.
`/etc/clamav-unofficial-sigs.conf.d/50-local.conf` should read:

```
# http://lists.clamav.net/pipermail/clamav-users/2015-April/001459.html
# SecuriteInfo Databases as not operating anymore and spams the logs
si_dbs=""
ss_dbs="$ss_dbs foxhole_generic.cdb
   foxhole_filename.cdb
   foxhole_js.cdb
"
```

Which removes the securiteinfo and adds foxhole low and mid.

Blocking incoming email

Some SPAM attacks are send from IPs from all over the world, but they provide the same hostname as *HELO*.

In Exim you can deny or drop them as follows with the following ACL rule:

```
drop
     condition = ${lookup{$sender_helo_name}lsearch{/etc/exim4/deny_helos}{yes}{no}}
     log_message = HELO on black list
```

The file `/etc/exim4/deny_helos` contains the *HELO* host names which should be blocked.

```
~# cat /etc/exim4/deny_helos
ymlf-pc
kontrollprozesse.contabo.host
```

Outlook

Convert .msg files

These can be converted with msgconvert to a EML file with is human readable and can be opened with thunderbird.

msgconvert can be installed on Debian/Ubuntu:

```
$ apt install libemail-outlook-message-perl
```

Monitoring with check_mk

We add the following services to `/etc/check_mk/mrpe.cfg`:

```
Eximailqueue /usr/lib/nagios/plugins/check_eximailqueue -w 600 -c 800
LocalSMTP /usr/lib/nagios/plugins/check_smtp -H localhost
Spamd /usr/bin/sa-check_spamd --socketpath=/var/run/spamd.sock
```

Run a service discovery for this host to get the new services added.

Logs

It is often useful to include the email subject into the logs for Exim, so add it to the `log_selector`:

```
log_selector = +subject
```

Or to the `MAIN_LOG_SELECTOR` variable in a Debian setup:

```
MAIN_LOG_SELECTOR = +tls_peerdn +subject
```

Linuxia Wiki

Stefan Hornburg (Racke)
Mail Server Configuration

wiki.linuxia.de