root@f21-mail-thegummbear:~# apt install dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  dovecot-core libbxttextcat-2.0-0 libbxttextcat-data liblua5.3-0 ssl-cert
Suggested packages:
  dovecot-gssapi dovecot-ldap dovecot-lmtpd dovecot-lucene
dovecot-managesieve dovecot-mysql dovecot-pgsql dovecot-pop3d dovecot-sieve
dovecot-solr dovecot-sqlite dovecot-submissiond ntp openssl-blacklist
The following NEW packages will be installed:
  dovecot-core dovecot-imapd libbxttextcat-2.0-0 libbxttextcat-data
liblua5.3-0 ssl-cert
0 upgraded, 6 newly installed, 0 to remove and 93 not upgraded.
Need to get 3386 kB of archives.
After this operation, 11.9 MB of additional disk space will be used.
Do you want to continue? [Y/n]
ls -l

total 32
-rw-r--r-- 1 root dovecot 1507 Aug  6 2019 dovecot-dict-auth.conf
-rw-r--r-- 1 root dovecot 852 Aug  6 2019 dovecot-dict-sql.conf
-rw-r--r-- 1 root dovecot 5824 Aug  6 2019 dovecot-sql.conf
-rw-r--r-- 1 root root 4401 Jun 16 13:12 dovecot.conf
drwx------ 2 root root  4096 Sep  27 11:57 private
root@f21-mail-thegummibear:/etc/dovecot# echo "We need to generate a public/private key for secure transmission"
We need to generate a public/private key for secure transmission
root@f21-mail-thegummibear:/etc/dovecot#
root@f21-mail-thegummbear:/etc/dovecot# echo "I will try and use a signed keypair and cert"
I will try and use a signed keypair and cert
root@f21-mail-thegummbear:/etc/dovecot#
root@f21-mail-thegummibear:/etc/dovecot# apt install letsencrypt
root@f21-mail-thegummibear:/etc/dovecot# sudo certbot certonly --standalone -d mail.thegummibear.com
root@f21-mail-thegummibear:/etc/dovecot# sudo certbot certonly --standalone -d mail.thegummibear.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator standalone, Installer None
Enter email address (used for urgent renewal and security notices) (Enter 'c' to cancel): joe@thegummibear.com


(A)gree/(C)ancel: A
root@f21/mail-thegummibear:~/etc/dovecot# sudo certbot certonly --standalone -d mail.thegeumibear.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator standalone, Installer None
Enter email address (used for urgent renewal and security notices) (Enter 'c' to cancel): joe@thegeumibear.com


(Agree/(C)ancel): A

Would you be willing to share your email address with the Electronic Frontier Foundation, a founding partner of the Let's Encrypt project and the non-profit organization that develops Certbot? We'd like to send you email about our work encrypting the web, EFF news, campaigns, and ways to support digital freedom.

(Y)es/(N)o: N
http-01 challenge for mail.thegummibear.com
Waiting for verification...
Cleaning up challenges

**IMPORTANT NOTES:**
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/mail.thegummibear.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/mail.thegummibear.com/privkey.pem

  Your cert will expire on 2021-12-26. To obtain a new or tweaked version of this certificate in the future, simply run certbot again. To non-interactively renew *all* of your certificates, run "certbot renew"

- Your account credentials have been saved in your Certbot configuration directory at /etc/letsencrypt. You should make a secure backup of this folder now. This configuration directory will also contain certificates and private keys obtained by Certbot so making regular backups of this folder is ideal.
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt:  https://letsencrypt.org/donate
  Donating to EFF:  https://eff.org/donate-le

root@f21-mail-thegummibear:/etc/dovecot#
## SSL settings

SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>

ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
#
# Edit these two lines to point to the new letscrypt files
ssl_cert = /etc/letsencrypt/live/mail.the gummbiear.com/fullchain.pem
ssl_key = /etc/letsencrypt/live/mail.the gummbiear.com/privkey.pem

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path>
#ssl_key_password = "conf.d/18-ssl.conf" 82L, 3294C
vi conf.d/10-ssl.conf

Stopped

fg

vi conf.d/10-ssl.conf

service dovecot restart
root@f21-mail-thegummibear:~/etc/dovecot# service dovecot status

● dovecot.service - Dovecot IMAP/POP3 email server
  Loaded: loaded (/lib/systemd/system/dovecot.service; enabled; vendor provided)
  Active: active (running) since Mon 2021-09-27 12:07:11 UTC; 7s ago
  Docs: man:dovecot(1)
        http://wiki2.dovecot.org/
  Main PID: 1262145 (dovecot)
  Tasks: 4 (limit: 470)
  Memory: 3.2M
  CGroup: /system.slice/dovecot.service
        └─1262146 /usr/sbin/dovecot -F

Sep 27 12:07:11 f21-mail-thegummibear systemd[1]: Started Dovecot IMAP/POP3 email relay service.
Sep 27 12:07:11 f21-mail-thegummibear dovecot[1262145]: master: Dovecot v2.3.7.
root@f21-mail-therummibear:/etc/dovecot# netstat -atup
root@f21-mail-thegummibear:/etc/dovecot# echo "We dont want imap 2, it is insecure"
We dont want imap 2, it is insecureoot@f21-mail-thegummibear:/etc/dovecot#
root@f21-mail-thegummibear:/etc/dovecot# vi conf.d/10-master.conf
# Default VSZ (virtual memory size) limit for service processes. This is mainly
# intended to catch and kill processes that leak memory before they eat up
# everything.
#default_vsiz_limit = 256M

# Login user is internally used by login processes. This is the most untrusted
# user in Dovecot system. It shouldn't have access to anything at all.
#default_login_user = dovenull

# Internal user is used by unprivileged processes. It should be separate from
# login user, so that login processes can't disturb other processes.
#default_internal_user = dovecot

service imap-login {
  inet_listener imap {
    #port = 143
    #disable insecure port
    port = 143
  }
  inet_listener imaps {
    #port = 993
    #ssl = yes
  }
}
root@f21-mail-thegummbear:/etc/dovecot# service dovecot restart
root@f21-mail-thegummbear:/etc/dovecot# netstat -atup
root@f21-mail-thegummbear:/etc/dovecot# echo "Make sure imap2 isn't listed"
Make sure imap2 isn't listed
root@f21-mail-thegummbear:/etc/dovecot#
joe@f21-mail-thegummibear:~$ echo "Configure exim to send from remote clients, if authenticated"
Configure exim to send from remote clients, if authenticated
joe@f21-mail-thegummibear:~$
joe@f21-mail-thegummibear:~$ sudo apt install exim4-daemon-heavy
joe@f21-mail-thegummibear:~$ echo "install secure authentication service"
ninstall secure authentication service
joe@f21-mail-thegummibear:~$ sudo apt install sasl2-bin
joe@f21-mail-thegummitbear:~$ sudo vi /etc/default/saslauthd
# Settings for saslauthd daemon
# Please read /usr/share/doc/sasl2-bin/README.Debian for details.
#
# Should saslauthd run automatically on startup? (default: no)
START=yes

# Description of this saslauthd instance. Recommended.
# (suggestion: SASL Authentication Daemon)
DESC="SASL Authentication Daemon"

# Short name of this saslauthd instance. Strongly recommended.
# (suggestion: saslauthd)
NAME="saslauthd"

# Which authentication mechanisms should saslauthd use? (default: pam)
#
# Available options in this Debian package:
# getpwnent -- use the getpwnent() library function
# kerberos5 -- use Kerberos 5
# pam -- use PAM
# rmap -- use a remote IMAP server
"/etc/default/saslauthd" 62L, 2315C written

7,9
joe@f21-mail-thegummibear:~$ ps aux | grep sasl
root  1263525  0.0  0.6 21656  2960 ?   Ss   12:16   0:00 /usr/sbin/saslauthd
lauthd -a pam -c -m /var/run/saslauthd -n 5
root  1263526  0.0  0.2 21656 1064 ?   S   12:16   0:00 /usr/sbin/saslauthd
lauthd -a pam -c -m /var/run/saslauthd -n 5
root  1263527  0.0  0.2 21656 1064 ?   S   12:16   0:00 /usr/sbin/saslauthd
lauthd -a pam -c -m /var/run/saslauthd -n 5
root  1263528  0.0  0.2 21656 1064 ?   S   12:16   0:00 /usr/sbin/saslauthd
lauthd -a pam -c -m /var/run/saslauthd -n 5
root  1263529  0.0  0.2 21656 1064 ?   S   12:16   0:00 /usr/sbin/saslauthd
lauthd -a pam -c -m /var/run/saslauthd -n 5
joe  1263531  0.0  0.1 5192   664 pts/0  S+   12:16   0:00 grep --color=auto sasl
joe@f21-mail-thegummibear:~$
joe@f21-mail-thegummibear:$ echo "now some detailed edits"
joe@f21-mail-thegummibear:~$ sudo vi /etc/exim4/exim4.conf.template
### main/03_exim4-config_tlsoptions

# Locate this section of the file
# ADDED BY JOE TO ENABLE TLS AUTH
MAIN_TLS_ENABLE = yes
#ENABLE STANDARD TLS PORTS
demon_smtp_ports = 25 : 465 : 587
tls_on_connect_ports = 465

#FORCE ENCRYPTION BEFORE AUTH
auth_advertise_hosts = $if eq($tls_cipher){}{}(*)
# END OF JOES ADDITION

# TLS/SSL configuration for exim as an SMTP server.
# See /usr/share/doc/exim4-base/README.Debian.gz for explanations.
Here is an example of CRAM-MD5 authentication against PostgreSQL:

# psqldb_auth_server:
#   driver = cram_md5
#   public_name = CRAM-MD5
#   server_secret = ${lookup pgsql(SELECT pw FROM users WHERE username = '${quote e_psql:$auth1}')}$value
#   server_set_id = $auth1

# Authenticate against local passwords using sasl2-bin
# Requires exim_uid to be a member of sasl group, see README.Debian.gz

# FIND THE FOLLOWING LINES AND UNCOMMENT

# plain_saslauthd_server:
#   driver = plaintext
#   public_name = PLAIN
#   server_condition = ${if saslauthd({$auth2}{$auth3}{1}{0})}
#   server_set_id = $auth2
#   server_prompts = :
#   ifndef AUTH_SERVER_ALLOW_NTLS_PASSWORDS
#     server_advertise_condition = ${if eq($tls_in_cipher}){1}{0})
#   endif

<exim4/exim4.conf.template> 2153L, 80256C written 1967,40 91%
# server_secret = $(lookup pgsql(SELECT pw FROM users WHERE username = '$(quote e_pgsql:$auth1)'){$value}fail)
# server_set_id = $auth1

# Authenticate against local passwords using sasl2-bin
# Requires exim_uid to be a member of sasl group, see README.Debian.gz
#
# FIND THE FOLLOWING LINES AND UNCOMMENT
#
plain_saslauthd_server:
    driver = plaintext
    public_name = PLAIN
    server_condition = $(if saslauthd{$auth2}{$auth3}{1}{0})
    server_set_id = $auth2
    server_prompts = :
    .ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
    server_advertise_condition = $(if eq{$tls_in_cipher}{}{1}{0})
    .endif
#
# login_saslauthd_server:
#    driver = plaintext
#    public_name = LOGIN
#    server_prompts = "Username:: : Password::"
joe@f21-mail-thegummibear:~$ echo "Now to allow exim to use the sasl service"
Now to allow exim to use the sasl service
joe@f21-mail-thegummibear:~$
joe@f21-mail-thegummibear:~$ echo "Now to allow exim to use the sasl service"
Now to allow exim to use the sasl service
joe@f21-mail-thegummibear:~$ sudo adduser Debian-exim sasl
Adding user 'Debian-exim' to group 'sasl' ...
Adding user Debian-exim to group sasl
Done.
joe@f21-mail-thegummibear:~$
joe@f21-mail-thegummibear:~$ echo "Apply the template changes to the action configuration files"
Apply the template changes to the action configuration files
joe@f21-mail-thegummibear:~$
$ echo "Apply the template changes to the action configuration files"
Apply the template changes to the action configuration files
$ sudo update-exim4.conf
joe@f21-mail-thegummibear:$ echo "Restart MTA to use these settings"
Restart MTA to use these settings
joe@f21-mail-thegummibear:$ sudo service exim4 restart
joe@f21-mail-thegummibear:$
<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>144.38.199.52:25</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:25</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:999</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>144.38.199.52:587</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:587</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>144.38.199.52:465</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:465</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.53:53</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:22</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>::1:25</td>
<td>:::*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>::993</td>
<td>:::*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>::1:587</td>
<td>:::*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>::1:465</td>
<td>:::*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>::22</td>
<td>:::*</td>
<td>LISTEN</td>
</tr>
</tbody>
</table>

```bash
joe@mail-thegummibear:~$ netstat -nt1
Active Internet connections (only servers)
```
root@F21-mail-thegumibear:/etc/exim4# ls
conf.d exim.crt exim.key exim4.conf.template passed.client update-exim4.conf.conf
root@F21-mail-thegumibear:/etc/exim4# echo "if you haven't already copied your certbot key and cert into this file, do so now"
if you haven't already copied your certbot key and cert into this file, do so now
root@F21-mail-thegumibear:/etc/exim4#
root@F21-mail-thegumibear:/etc/exim4# cp /etc/letsencrypt/live/mail.thegumibear.com/cert.pem exim.crt
root@F21-mail-thegumibear:/etc/exim4# cp /etc/letsencrypt/live/mail.thegumibear.com/privkey.pem exim.key
root@F21-mall-thequemibear:/etc/xim4# echo "restart services and check open ports"

restart services and check open ports

root@F21-mall-thequemibear:/etc/xim4#
root@F21-mall-thequemibear:/etc/exim4# ls -l

total 180
-rw-r-x  1 root  root   4096 Sep 11 17:59 conf.d
-rw-r--  1 root  root  1858 Sep 27 12:37 exim.crt
-rw-r--  1 root  root  1794 Sep 27 12:37 exim.key
-rw-r--  1 root  root  88249 Sep 27 12:21 exim4.conf.template
-rw-r--  1 root  root  284 Apr 28 12:39 passed.client
-rw-r--  1 root  root  1180 Sep 11 18:04 update-exim4.conf.conf

root@F21-mall-thequemibear:/etc/exim4# echo "Check that your permissions on key and crt match mine above"
root@F21-mail-thequmibear#: /etc/exim4# echo "Now test with a client"