On the mail server. We are going to install Dovecot which will provide a secure IMAP service.

```
joe@mail-thegummibear:~$ echo "On the mail server. We are going to install Dovecot which will provide a secure IMAP service"
joe@mail-thegummibear:~$ sudo apt-get install dovecot-imapd
```
We need to generate a public/private key pair for secure transmission.
joe@mail-thegummibear:/etc/dovecot$ cd /usr/share/dovecot/
joe@mail-thegummibear:/usr/share/dovecot$ ls
conf.d
dovecot.conf
dovecot-dict-auth.conf.ext
dovecot-dict-sql.conf.ext
dovecot-openssl.cnf
dovecot-openssl.cnf

joe@mail-thegummibear:/usr/share/dovecot$
joe@mail-thegummibear:~/usr/share/dovecot$ sudo vi dovecot-openssl.cnf
SSLeay configuration file for Dovecot.

RANDFILE = /dev/urandom

[ req ]
default_bits = 2048
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
prompt = no
policy = policy_anything
req_extensions = v3_req
x509_extensions = v3_req

[ req_distinguished_name ]
organizationName = The Gummi Bear
organizationalUnitName = CIT
commonName = mail.thegummibear.com
emailAddress = joe@thegummibear.com

[ v3_req ]
basicConstraints = CA:FALSE
"dovecot-openssl.cnf" 23L, 543C

1,1 All
joe@mail-thegummibear:/usr/share/dovecot$ ls
conf.d     dovecot-dict-sql.conf.ext  mkcert.sh
dovecot.conf  dovecot-openssl.cnf  protocols.d
dovecot-dict-auth.conf.ext dovecot-sql.conf.ext  stopwords
joe@mail-thegummibear:/usr/share/dovecot$ sudo ./mkcert.sh
root@mail-thegummibear:/etc/dovecot$ sudo bash
root@mail-thegummibear:/etc/dovecot# ls
conf.d  dovecot-dict-auth.conf.ext  dovecot.pem  private
dovecot.conf  dovecot-dict-sql.conf.ext  dovecot-sql.conf.ext  README
root@mail-thegummibear:/etc/dovecot# ls private/
dovecot.pem
root@mail-thegummibear:/etc/dovecot# echo "here is my private key"
here is my private key
root@mail-thegummibear:/etc/dovecot#
root@mail-thegummibear: /etc/dovecot

root@mail-thegummibear: /etc/dovecot# vi conf.d/10-ssl.conf
## 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

ssl_cert = `/etc/dovecot/private/dovecot.pem`
ssl_key = `/etc/dovecot/private/dovecot.key`

# 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 =

# PEM encoded trusted certificate authority. Set this only if you intend to use
# ssl_verify_client_cert=yes. The file should contain the CA certificate(s)
# followed by the matching CRL(s). (e.g. ssl_ca = `/etc/ssl/certs/ca.pem`

"/etc/dovecot/conf.d/10-ssl.conf" 63L, 2329C
root@mail-thegummibear:/etc/dovecot# service dovecot restart
root@mail-thegummibear:/etc/dovecot#
### Active Internet connections (servers and established)

<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><em>:</em>:imap2</td>
<td><em>::</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>28699/dovecot</td>
<td>0</td>
<td>0</td>
<td><em>:</em>:ssh</td>
<td><em>::</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>2158/sshd</td>
<td>0</td>
<td>0</td>
<td>mail.thegummibear.c:smtp</td>
<td><em>::</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>2532/exim4</td>
<td>0</td>
<td>0</td>
<td>localhost:smtp</td>
<td><em>::</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td><em>:</em>:imaps</td>
<td><em>::</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>28699/dovecot</td>
<td>0</td>
<td>0</td>
<td>296 mail.thegummibear.c:ssh yavin.cs.dixie.ed:56790</td>
<td>ESTABLISHED</td>
<td></td>
</tr>
<tr>
<td>28272/sshd: joe</td>
<td>pr</td>
<td>tcp6</td>
<td>0 [::]:imap2</td>
<td>[::]:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>[::]:ssh</td>
<td>[::]:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>localhost:smtp</td>
<td>[::]:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>[::]:imaps</td>
<td>[::]:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>[::]:imap2</td>
<td>[::]:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>28699/dovecot</td>
<td>0</td>
<td>0</td>
<td>[::]:ssh</td>
<td>[::]:*</td>
<td>LISTEN</td>
</tr>
</tbody>
</table>
we don't want the imap2 port. It is insecure
root@mail-thegummibear:/etc/dovecot

root@mail-thegummibear:/etc/dovecot# vi conf.d/10-master.conf
#default_process_limit = 100
#default_client_limit = 1000

# 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_vsz_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 plain text logins
    port = 0
}
inet_listener imaps {
"conf.d/10-master.conf" 121L, 3427C written
root@mail-thegummibear: /etc/dovecot# service dovecot restart
<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>PID/Program name</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>*:ssh</td>
<td><em>:</em></td>
<td>2158/sshd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>mail.thegummibear::smtp</td>
<td><em>:</em></td>
<td>2532/exim4</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>localhost:smtp</td>
<td><em>:</em></td>
<td>2532/exim4</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>*:imaps</td>
<td><em>:</em></td>
<td>28723/dovecot</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>296 mail.thegummibear.c::ssh</td>
<td>yavin.cs.dixie.ed:56790</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>[::]:ssh</td>
<td>[::]:*</td>
<td>2158/sshd</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>localhost:smtp</td>
<td>[::]:*</td>
<td>2532/exim4</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>[::]:imaps</td>
<td>[::]:*</td>
<td>28723/dovecot</td>
</tr>
</tbody>
</table>