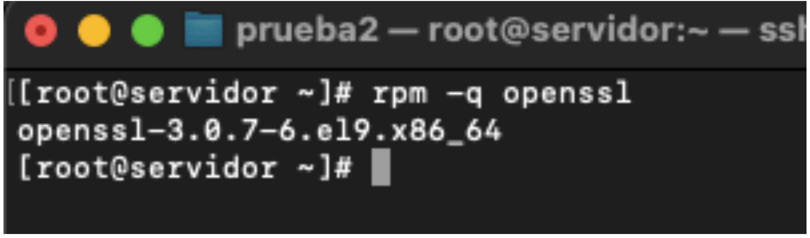
Verificamos si SSL están instalado:

```
rpm –q openssl
```



```
[[root@servidor ~]# rpm -q openssl
openssl-3.0.7-6.el9.x86_64
[root@servidor ~]#
```

Ya lo tengo instalado, en caso no tenerlo instalado se procede a instalar con:

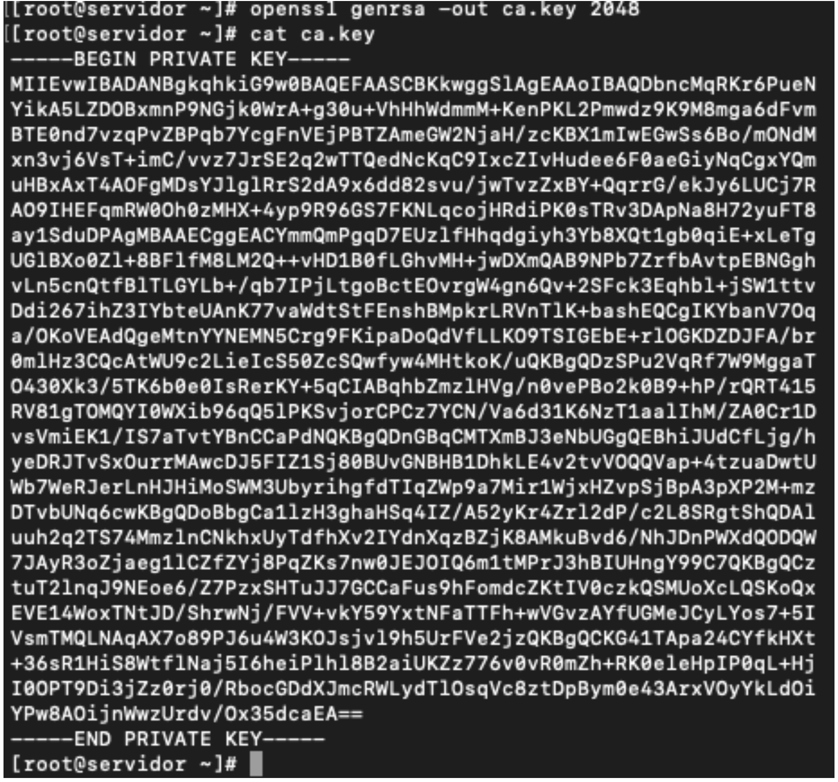
```
yum install openssl
```

Creación de los certificados y las claves

1.Generación de la clave privada

Generamos la clave de RSA:

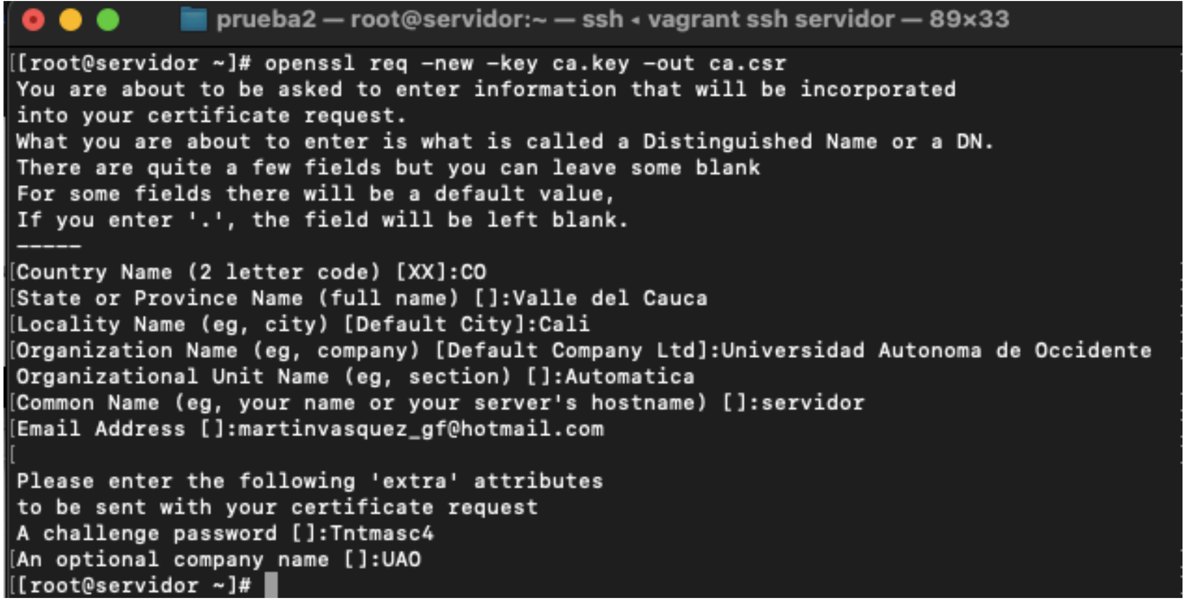
```
openssl genrsa –out ca.key 2048
La verificamos:
cat ca.key
```



```
[[root@servidor ~]# openssl genrsa -out ca.key 2048
[[root@servidor ~]# cat ca.key
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDbncMqRKr6PueN
YikA5LZDOBxmnP9NGjk0WrA+g30u+VhHhWdmmM+KenPKL2Pmwdz9K9M8mga6dFvm
BTE0nd7vzqPvZBPqb7YcgFnVEjPBTZAmeGW2NjaH/zcKBX1mIwEGwSs6Bo/mONdM
xn3vj6VsT+imC/vvz7JrSE2q2wTTQedNcKqC9IxcZIvHudee6F0aeGiyNqCgxYQm
uHBxAxT4AOFgMDsYJlglRrS2dA9x6dd82svu/jwTvzZxBY+QqrrG/ekJy6LUCj7R
AO9IHEFqmRW0Oh0zMHX+4yp9R96GS7FKNLqcojHRdiPK0sTRv3DApNa8H72yuFT8
ay1SduDPAgMBAAECggEACYmmQmPgqD7EUzlfHhqdgiyh3Yb8XQt1gb0qiE+xLeTg
UGlBXo0Zl+8BFlfM8LM2Q++vHD1B0fLGhvMH+jwDXmQAB9NPb7ZrfbAvtpEBNGgh
vLn5cnQtfBlTLGYLb+/qb7IPjLtgoBctEOvrgW4gn6Qv+2SFck3Eqhbl+jSW1ttv
Ddi267ihZ3IYbteUAnK77vaWdtStFEnshBMpkrLRVnTlK+bashEQCgIKYbanV7Oq
a/OKoVEAdQgeMtnYYNEMN5Crg9FKipaDoQdVfLLKO9TSIGEbE+rlOGKDZDJFA/br
0mlHz3CQcAtWU9c2LieIcS50ZcSQwfyw4MHtkoK/uQKBgQDzSPu2VqRf7W9MggaT
O430Xk3/5TK6b0e0IsRerKY+5qCIABqhbZmzlHVg/n0vePBo2k0B9+hP/rQRT415
RV81gTOMQYI0WXib96qQ5lPKSvjorCPCz7YCN/Va6d31K6NzT1aalIhM/ZA0Cr1D
vsVmiEK1/IS7aTvtYBnCCaPdNQKBgQDnGBqCMTXmBJ3eNbUGgQEBhiJUdCfLjg/h
yeDRJTvSxOurrMAwcDJ5FIZ1Sj80BUvGNBHB1DhkLE4v2tvVOQQVap+4tzuaDwtU
Wb7WeRJerLnHJHiMoSWM3UbyrihgfdTIqZWp9a7Mir1WjxHZvpSjBpA3pXP2M+mz
DTvbUNq6cwKBgQDoBbgCa1lzH3ghaHSq4IZ/A52yKr4Zrl2dP/c2L8SRgtShQDAl
uuh2q2TS74MmzlnCNkhxUyTdfhXv2IYdnXqzBZjK8AMkuBvd6/NhJDnPWXdQODQW
7JAyR3oZjaeg1lCZfZYj8PqZKs7nw0JEJOIQ6m1tMPrJ3hBIUHngY99C7QKBgQCz
tuT2lnqJ9NEoe6/Z7PzxSHTuJJ7GCCaFus9hFomdcZKtIV0czkQSMUoXcLQSKoQx
EVE14WoxTNtJD/ShrwNj/FVV+vkY59YxtNFaTTFh+wVGvzAYfUGMeJCyLYos7+5I
VsmTMQLNAqAX7o89PJ6u4W3KOJsjvl9h5UrFVe2jzQKBgQCKG41TApa24CYfkHXt
+36sR1HiS8WtflNaj5I6heiPlhl8B2aiUKZz776v0vR0mZh+RK0eleHpIP0qL+Hj
I0OPT9Di3jZz0rj0/RbocGDdXJmcRWLydTlOsqVc8ztDpBym0e43ArxVOyYkLdOi
YPw8AOijnWwzUrdv/Ox35dcaEA==
-----END PRIVATE KEY-----
[root@servidor ~]#
```

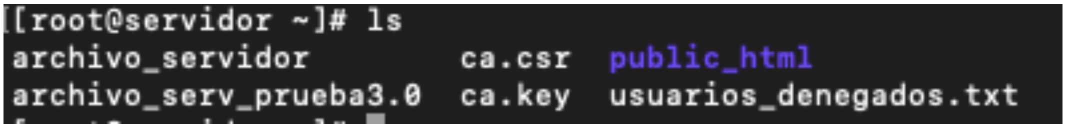
2.Generación de la petición de certificado (Certificate Signing Request = CSR):

```
openssl req -new -key ca.key -out ca.csr
```


prueba2 — root@servidor:~ — ssh ◂ vagrant ssh servidor — 89×33

```
[[root@servidor ~]# openssl req -new -key ca.key -out ca.csr
 You are about to be asked to enter information that will be incorporated
 into your certificate request.
 What you are about to enter is what is called a Distinguished Name or a DN.
 There are quite a few fields but you can leave some blank
 For some fields there will be a default value,
 If you enter '.', the field will be left blank.
 -----
[Country Name (2 letter code) [XX]:CO
[State or Province Name (full name) []:Valle del Cauca
[Locality Name (eg, city) [Default City]:Cali
[Organization Name (eg, company) [Default Company Ltd]:Universidad Autonoma de Occidente
 Organizational Unit Name (eg, section) []:Automatica
[Common Name (eg, your name or your server's hostname) []:servidor
[Email Address []:martinvasquez_gf@hotmail.com
[
 Please enter the following 'extra' attributes
 to be sent with your certificate request
 A challenge password []:Tntmasc4
[An optional company name []:UAO
[[root@servidor ~]#
```

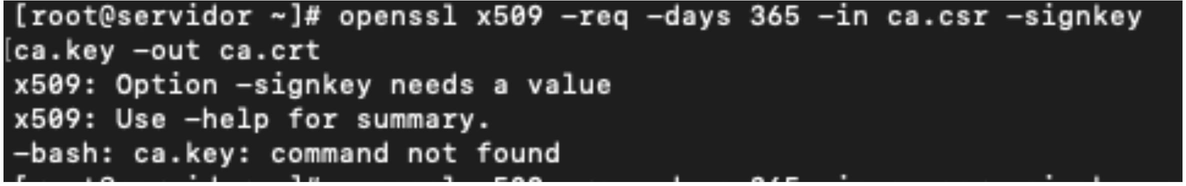
```
ls
```



```
[[root@servidor ~]# ls
 archivo_servidor          ca.csr  public_html
 archivo_serv_prueba3.0    ca.key  usuarios_denegados.txt
```

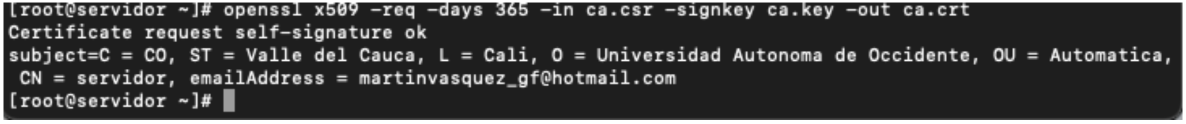
3.Generación del certificado x509:

```
openssl x509 -req -days 365 -in ca.csr -signkey
ca.key -out ca.crt ----Este me dio error
```



```
 [root@servidor ~]# openssl x509 -req -days 365 -in ca.csr -signkey
[ca.key -out ca.crt
 x509: Option -signkey needs a value
 x509: Use -help for summary.
 -bash: ca.key: command not found
```

openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt

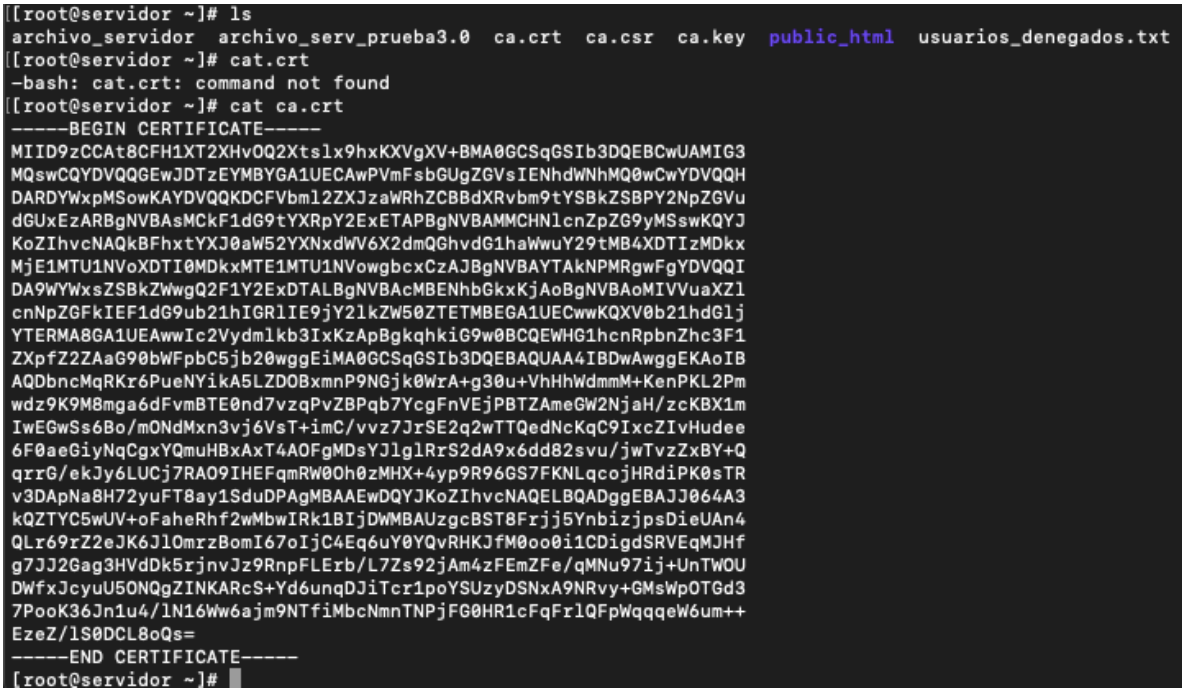


```
[root@servidor ~]# openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
Certificate request self-signature ok
subject=C = CO, ST = Valle del Cauca, L = Cali, O = Universidad Autonoma de Occidente, OU = Automatica,
 CN = servidor, emailAddress = martinvasquez_gf@hotmail.com
[root@servidor ~]#
```

Certificado:

```
ls
```

cat ca.crt



```
[[root@servidor ~]# ls
 archivo_servidor  archivo_serv_prueba3.0  ca.crt  ca.csr  ca.key  public_html  usuarios_denegados.txt
[[root@servidor ~]# cat.crt
 -bash: cat.crt: command not found
[[root@servidor ~]# cat ca.crt
 -----BEGIN CERTIFICATE-----
 MIID9zCCAt8CFH1XT2XHvOQ2Xtslx9hxKXVgXV+BMA0GCSqGSIb3DQEBCwUAMIG3
 MQswCQYDVQQGEwJDTzEYMBYGA1UECAwPVmFsbGUgZGVsIENhdWNhMQ0wCwYDVQQH
 DARDYWxpMSowKAYDVQQKDCFVbml2ZXJzaWRhZCBBdXRvbm9tYSBkZSBPY2NpZGVu
 dGUxEzARBgNVBAsMCkF1dG9tYXRpY2ExETAPBgNVBAMMCHNlcnZpZG9yMSswKQYJ
 KoZIhvcNAQkBFhxtYXJ0aW52YXNxdWV6X2dmQGhvdG1haWwuY29tMB4XDTIzMDkx
 MjE1MTU1NVoXDTI0MDkxMTE1MTU1NVowgbcxCzAJBgNVBAYTAkNPMRgwFgYDVQQI
 DA9WYWxsZSBkZWwgQ2F1Y2ExDTALBgNVBAcMBENhbGkxKjAoBgNVBAoMIVVuaXZl
 cnNpZGFkIEF1dG9ub21hIGRlIE9jY2lkZW50ZTETMBEGA1UECwwKQXV0b21hdGlj
 YTERMA8GA1UEAwwIc2Vydmlkb3IxKzApBgkqhkiG9w0BCQEWHG1hcnRpbnZhc3F1
 ZXpfZ2ZAaG90bWFpbC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
 AQDbncMqRKr6PueNYikA5LZDOBxmnP9NGjk0WrA+g30u+VhHhWdmmM+KenPKL2Pm
 wdz9K9M8mga6dFvmBTE0nd7vzqPvZBPqb7YcgFnVEjPBTZAmeGW2NjaH/zcKBX1m
 IwEGwSs6Bo/mONdMxn3vj6VsT+imC/vvz7JrSE2q2wTTQedNcKqC9IxcZIvHudee
 6F0aeGiyNqCgxYQmuHBxAxT4AOFgMDsYJlglRrS2dA9x6dd82svu/jwTvzZxBY+Q
 qrrG/ekJy6LUCj7RAO9IHEFqmRW0Oh0zMHX+4yp9R96GS7FKNLqcojHRdiPK0sTR
 v3DApNa8H72yuFT8ay1SduDPAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAJJ064A3
 kQZTYC5wUV+oFaheRhf2wMbwIRk1BIjDWMBAUzgcBST8Frjj5YnbizjpsDieUAn4
 QLr69rZ2eJK6JlOmrzBomI67oIjC4Eq6uY0YQvRHKJfM0oo0i1CDigdSRVEqMJHf
 g7JJ2Gag3HVdDk5rjnvJz9RnpFLErb/L7Zs92jAm4zFEmZFe/qMNu97ij+UnTWOU
 DWfxJcyuU5ONQgZINKARcS+Yd6unqDJiTcr1poYSUzyDSNxA9NRvy+GMsWpOTGd3
 7PooK36Jn1u4/lN16Ww6ajm9NTfiMbcNmnTNPjFG0HR1cFqFrlQFpWqqqeW6um++
 EzeZ/lS0DCL8oQs=
 -----END CERTIFICATE-----
[root@servidor ~]#
```

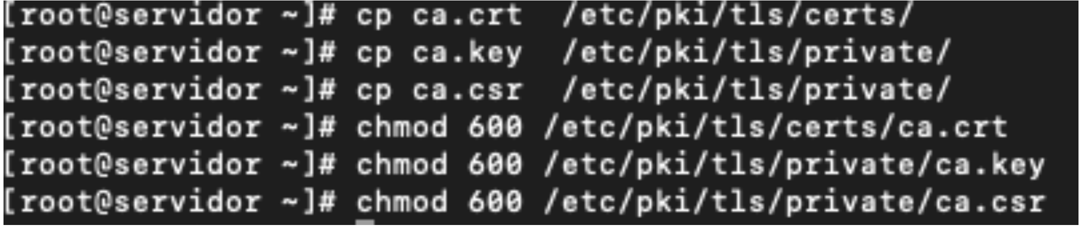
Ubicación de los archivos generados

Los archivos generados (ca.key, ca.csr, ca.crt) se deben copiar en las siguientes ubicaciones:

```
cp ca.crt  /etc/pki/tls/certs/
cp ca.key  /etc/pki/tls/private/
cp ca.csr  /etc/pki/tls/private/
```

Damos permisos de lectura y escritura de estos archivos solo a root

```
chmod 600 /etc/pki/tls/certs/ca.crt
chmod 600 /etc/pki/tls/private/ca.key
```



```
[root@servidor ~]# cp ca.crt  /etc/pki/tls/certs/
[root@servidor ~]# cp ca.key  /etc/pki/tls/private/
[root@servidor ~]# cp ca.csr  /etc/pki/tls/private/
[root@servidor ~]# chmod 600 /etc/pki/tls/certs/ca.crt
[root@servidor ~]# chmod 600 /etc/pki/tls/private/ca.key
[root@servidor ~]# chmod 600 /etc/pki/tls/private/ca.csr
```

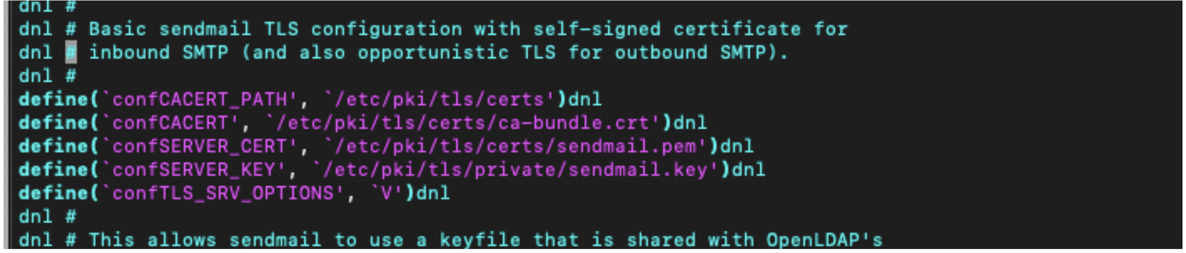
Configuración de sendmail para aceptar los certificados y claves creados

Configurar en sendmail las opciones de SSL. Para esto se debe editar el archivo de configuración:

```
vim /etc/mail/sendmail.mc
```

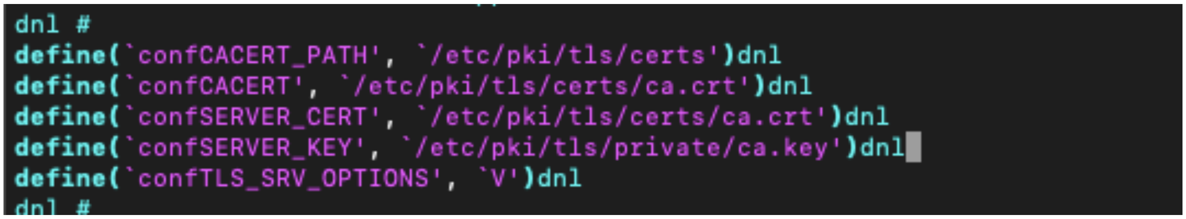
En este archivo se debe indicar donde quedaron almacenados los archivos de certificado y claves. Esto se hace modificando las siguientes directivas (linea 60 aprox., borre el "dnl" que antecede a los comandos de ser necesario):

`Original:` `Linea 60 + –`



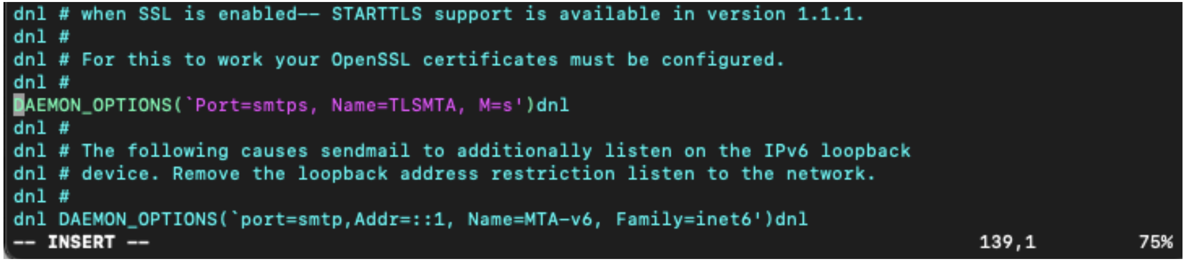
```
dnl #
dnl # Basic sendmail TLS configuration with self-signed certificate for
dnl # inbound SMTP (and also opportunistic TLS for outbound SMTP).
dnl #
define(`confCACERT_PATH', `/etc/pki/tls/certs')dnl
define(`confCACERT', `/etc/pki/tls/certs/ca-bundle.crt')dnl
define(`confSERVER_CERT', `/etc/pki/tls/certs/sendmail.pem')dnl
define(`confSERVER_KEY', `/etc/pki/tls/private/sendmail.key')dnl
define(`confTLS_SRV_OPTIONS', `V')dnl
dnl #
dnl # This allows sendmail to use a keyfile that is shared with OpenLDAP's
```

Cambio:



```
dnl #
define(`confCACERT_PATH', `/etc/pki/tls/certs')dnl
define(`confCACERT', `/etc/pki/tls/certs/ca.crt')dnl
define(`confSERVER_CERT', `/etc/pki/tls/certs/ca.crt')dnl
define(`confSERVER_KEY', `/etc/pki/tls/private/ca.key')dnl
define(`confTLS_SRV_OPTIONS', `V')dnl
dnl #
```

Luego (alrededor de la línea 136) se debe habilitar el puerto que sendmail usará, que por defecto es el 465



```
dnl # when SSL is enabled-- STARTTLS support is available in version 1.1.1.
dnl #
dnl # For this to work your OpenSSL certificates must be configured.
dnl #
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
dnl #
dnl # The following causes sendmail to additionally listen on the IPv6 loopback
dnl # device. Remove the loopback address restriction listen to the network.
dnl #
dnl DAEMON_OPTIONS(`port=smtp,Addr=::1, Name=MTA-v6, Family=inet6')dnl
-- INSERT --                                                     139,1         75%
```

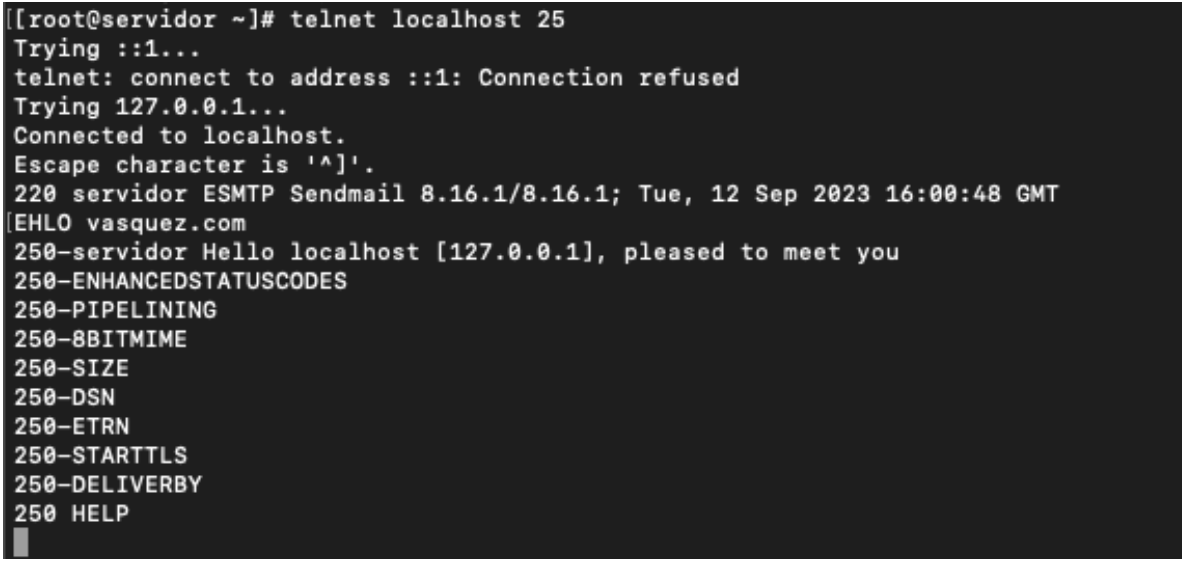
Por último se debe reiniciar el servicio de sendmail, pero antes se debe ejecutar el m4:

```
sudo m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf

service sendmail restart
```

Prueba de sendmail Seguro

Ingresamos al servidor desde una conexión telnet y ejecutamos el comando EHLO al servidor, debe responder de la siguiente manera (La línea 250-STARTTLS debe estar presente)



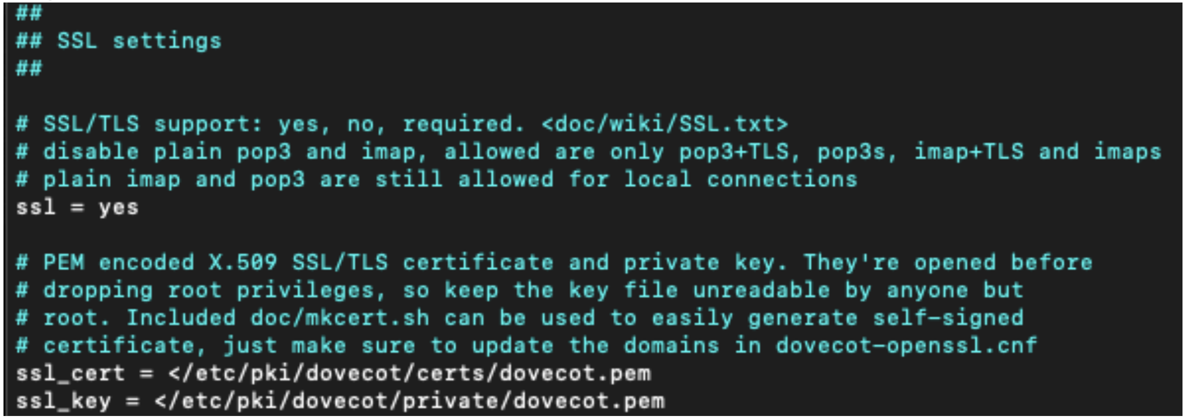
```
[[root@servidor ~]# telnet localhost 25
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 servidor ESMTP Sendmail 8.16.1/8.16.1; Tue, 12 Sep 2023 16:00:48 GMT
[EHLO vasquez.com
250-servidor Hello localhost [127.0.0.1], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-STARTTLS
250-DELIVERBY
250 HELP
```

Configuración de dovecot para aceptar los certificados y las claves

Se procede a activar ssl en dovecot. Para esto se debe editar el archivo de configuración: /etc/dovecot/conf.d/10-ssl.conf. De la siguiente manera:

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

Original:

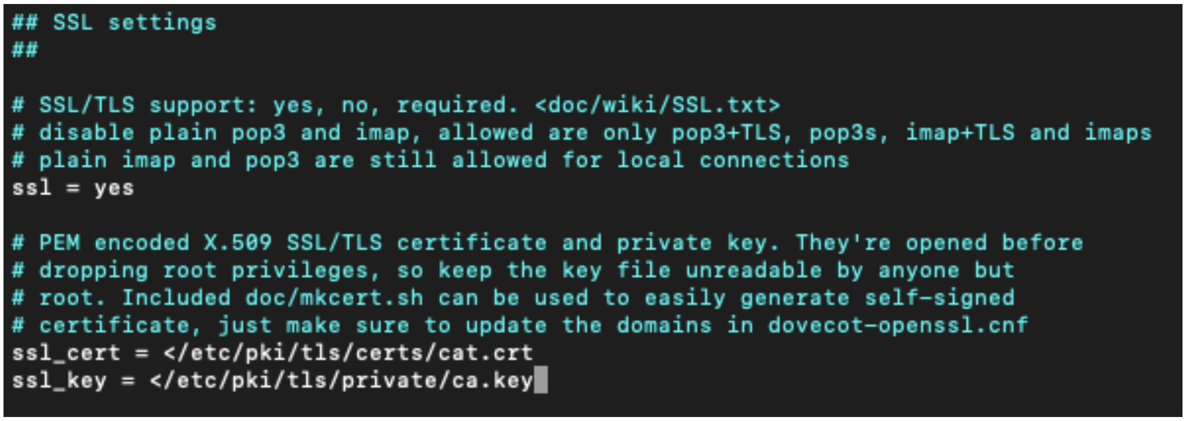


```
##
## SSL settings
##

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
# disable plain pop3 and imap, allowed are only pop3+TLS, pop3s, imap+TLS and imaps
# plain imap and pop3 are still allowed for local connections
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/pki/dovecot/certs/dovecot.pem
ssl_key = </etc/pki/dovecot/private/dovecot.pem
```

Cambio:



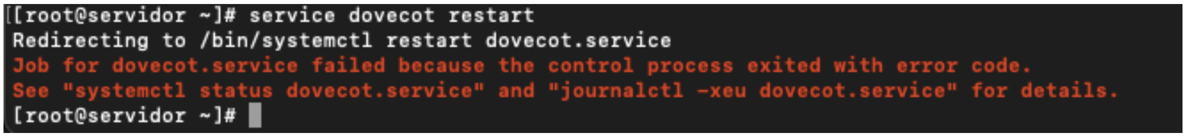
```
## SSL settings
##

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
# disable plain pop3 and imap, allowed are only pop3+TLS, pop3s, imap+TLS and imaps
# plain imap and pop3 are still allowed for local connections
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/pki/tls/certs/cat.crt
ssl_key = </etc/pki/tls/private/ca.key
```

Reiniciamos el servicio dovecot:

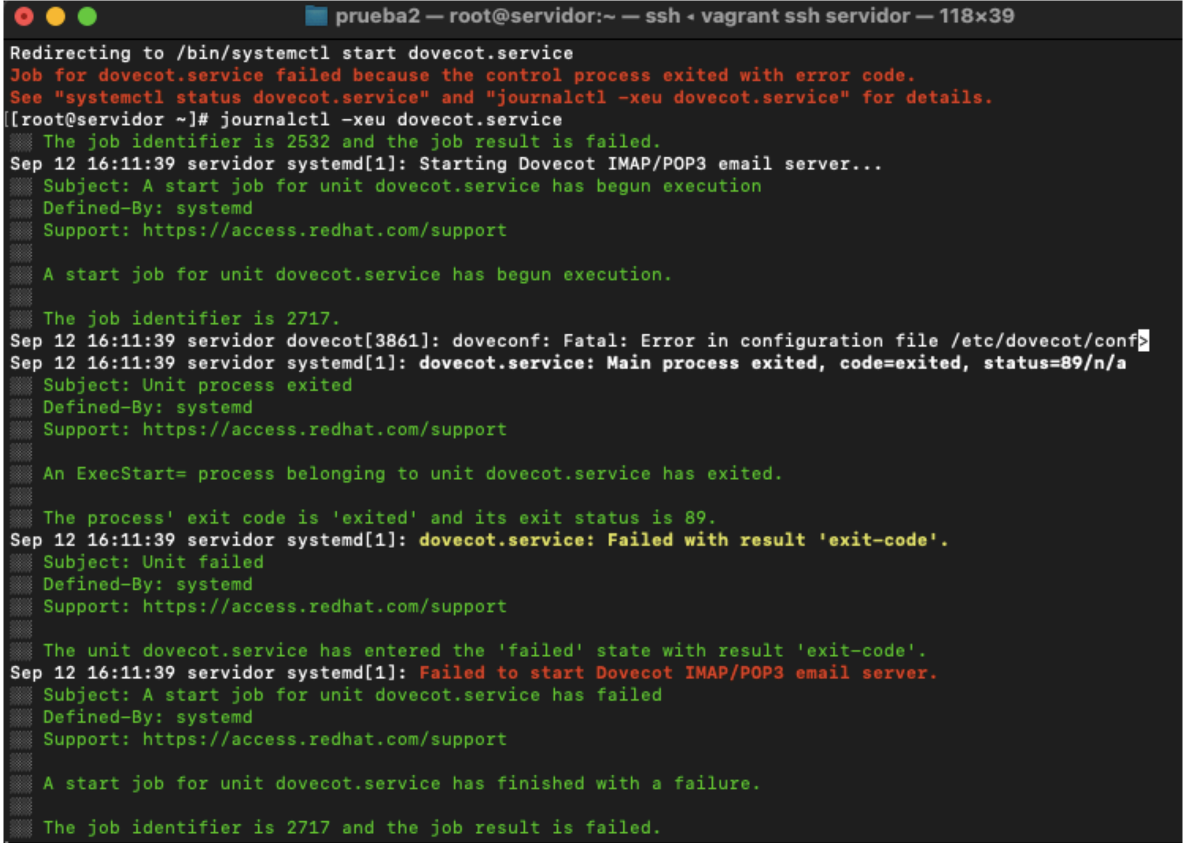
`service dovecot restart` ERROR



```
[[root@servidor ~]# service dovecot restart
Redirecting to /bin/systemctl restart dovecot.service
Job for dovecot.service failed because the control process exited with error code.
See "systemctl status dovecot.service" and "journalctl -xeu dovecot.service" for details.
[root@servidor ~]#
```

Para ver informe del error:

`journalctl -xeu dovecot.service`



prueba2 — root@servidor:~ — ssh ◂ vagrant ssh servidor — 118×39

```
Redirecting to /bin/systemctl start dovecot.service
Job for dovecot.service failed because the control process exited with error code.
See "systemctl status dovecot.service" and "journalctl -xeu dovecot.service" for details.
[[root@servidor ~]# journalctl -xeu dovecot.service
▒▒ The job identifier is 2532 and the job result is failed.
Sep 12 16:11:39 servidor systemd[1]: Starting Dovecot IMAP/POP3 email server...
▒▒ Subject: A start job for unit dovecot.service has begun execution
▒▒ Defined-By: systemd
▒▒ Support: https://access.redhat.com/support
▒▒
▒▒ A start job for unit dovecot.service has begun execution.
▒▒
▒▒ The job identifier is 2717.
Sep 12 16:11:39 servidor dovecot[3861]: doveconf: Fatal: Error in configuration file /etc/dovecot/conf>
Sep 12 16:11:39 servidor systemd[1]: dovecot.service: Main process exited, code=exited, status=89/n/a
▒▒ Subject: Unit process exited
▒▒ Defined-By: systemd
▒▒ Support: https://access.redhat.com/support
▒▒
▒▒ An ExecStart= process belonging to unit dovecot.service has exited.
▒▒
▒▒ The process' exit code is 'exited' and its exit status is 89.
Sep 12 16:11:39 servidor systemd[1]: dovecot.service: Failed with result 'exit-code'.
▒▒ Subject: Unit failed
▒▒ Defined-By: systemd
▒▒ Support: https://access.redhat.com/support
▒▒
▒▒ The unit dovecot.service has entered the 'failed' state with result 'exit-code'.
Sep 12 16:11:39 servidor systemd[1]: Failed to start Dovecot IMAP/POP3 email server.
▒▒ Subject: A start job for unit dovecot.service has failed
▒▒ Defined-By: systemd
▒▒ Support: https://access.redhat.com/support
▒▒
▒▒ A start job for unit dovecot.service has finished with a failure.
▒▒
▒▒ The job identifier is 2717 and the job result is failed.
```