

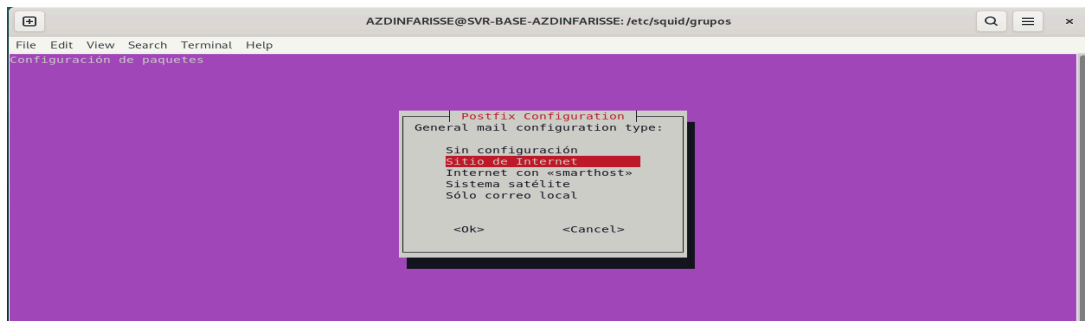
Implementación de un servidor de correo empresarial

1. Instalación y configuración del servidor de correo.

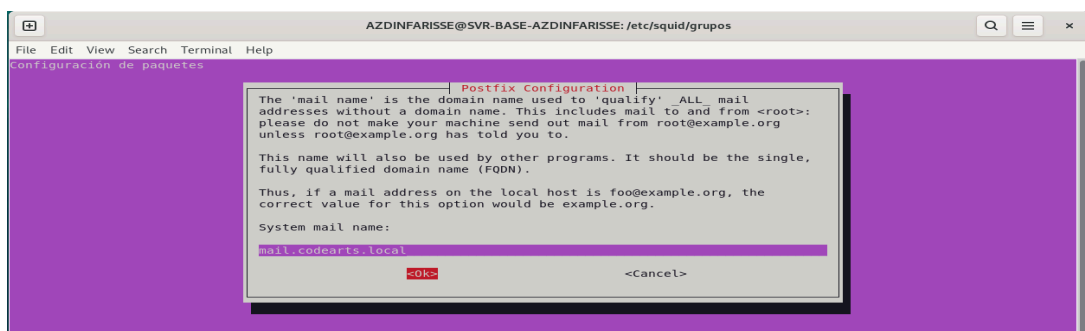
Para instalar Postfix como servidor SMTP para el envío de correos, lo hacemos con el comando:

```
sudo apt update  
sudo apt install postfix
```

A mitad de la instalación del paquete, se nos abre una ventana la cual nos pregunta qué tipo de configuración de mail utilizaremos, y en este caso seleccionamos **Internet site**.



Esto nos lleva a otra pantalla en la que debemos especificar el nombre del dominio, el cual le pondremos: **mail.codearts.local**.



Ahora procedemos a instalar dovecot como servidor IMAP/POP3 para la recepción de correos. Esto lo hacemos con el comando:

```
sudo apt install dovecot-core dovecot-imapd dovecot-pop3d
```

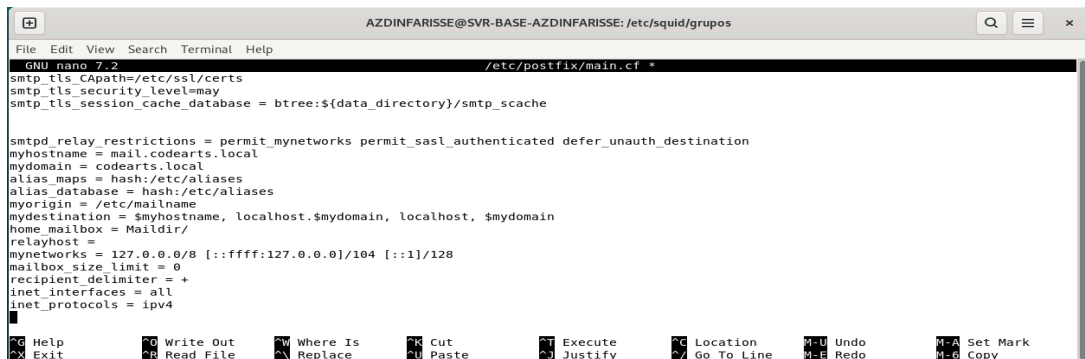
Ahora para configurar el dominio de correo mail.codearts.local hemos de abrir el archivo de configuración **main.cf** y ajustar las líneas para que queden así:

```
myhostname = mail.codearts.local  
mydomain = codearts.local  
myorigin = /etc/mailname  
inet_interfaces = all
```

inet_protocols = ipv4

mydestination = \$myhostname, localhost.\$mydomain, localhost, \$mydomain

home_mailbox = Maildir/



```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: /etc/squid/grupos
GNU nano 7.2 /etc/postfix/main.cf *
smtp_tls_Capath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

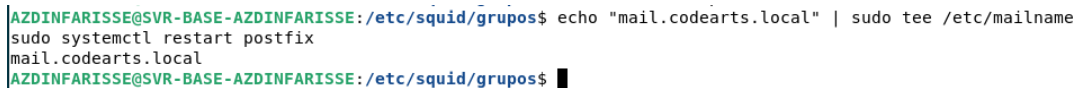
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.codearts.local
mydomain = codearts.local
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
home_mailbox = Maildir/
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^G Location   ^U Undo       ^M Set Mark
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  ^E Redo       ^O Copy
```

Y ahora lo guardamos y reiniciamos con el comando:

echo "mail.codearts.local" | sudo tee /etc/mailname

sudo systemctl restart postfix



```
AZDINFARISSE@SVR-BASE-AZDINFARISSE:/etc/squid/grupos$ echo "mail.codearts.local" | sudo tee /etc/mailname
sudo systemctl restart postfix
mail.codearts.local
AZDINFARISSE@SVR-BASE-AZDINFARISSE:/etc/squid/grupos$
```

Ahora para definir la estructura de buzones en /var/mail/usuarios/, volvemos a abrir el archivo main.cf y cambiamos la línea de **home_mailbox** para que quede así:

home_mailbox = /var/mail/usuarios/



```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: /etc/squid/grupos
GNU nano 7.2 /etc/postfix/main.cf *
myhostname = mail.codearts.local
mydomain = codearts.local
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
home_mailbox = /var/mail/usuarios/
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^G Location   ^U Undo       ^M Set Mark
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  ^E Redo       ^O Copy
```

2. Creación y gestión de cuentas de correo.

Para crear los buzones de correo para estos empleados, hemos de hacerlo primero con estos comandos:

Crear la carpeta si no existe

sudo mkdir -p /var/mail/usuarios

sudo chmod 755 /var/mail/usuarios

Crear empleado1

sudo useradd -M -d /var/mail/usuarios/empleado1 -s /sbin/nologin empleado1

sudo touch /var/mail/usuarios/empleado1

sudo chown empleado1:mail /var/mail/usuarios/empleado1

sudo chmod 660 /var/mail/usuarios/empleado1

Crear empleado2

sudo useradd -M -d /var/mail/usuarios/empleado2 -s /sbin/nologin empleado2

sudo touch /var/mail/usuarios/empleado2

sudo chown empleado2:mail /var/mail/usuarios/empleado2

sudo chmod 660 /var/mail/usuarios/empleado2

Ahora para configurar los alias editamos el archivo **/etc/aliases** y le añadimos las siguientes líneas:

administracion: empleado1

marketing: empleado2

y aplicamos los cambios con:

sudo newaliases

Ahora para el reenvío de correos internos, de empleado1 a empleado2, tenemos que crear el archivo **/etc/postfix/virtual** y añadirle la línea:

empleado1@mail.codearts.local empleado2@mail.codearts.local

Luego creamos el mapa hash y lo activamos con:

sudo postmap /etc/postfix/virtual

Ahora, en **main.cf**, añadimos:

virtual_alias_maps = hash:/etc/postfix/virtual

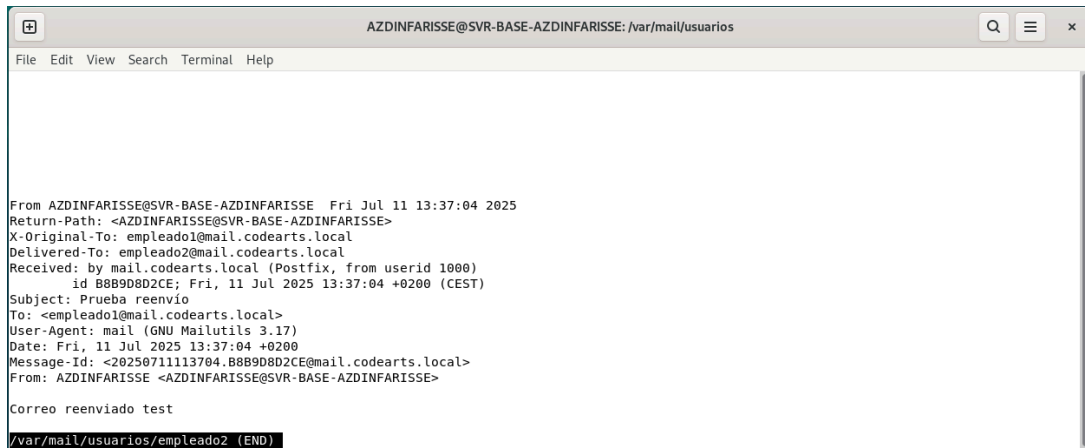
Y por último reiniciamos el postfix y ya tendríamos activo el reenvío de correos internos.

Para probar que se reenvían al empleado2, haremos una prueba enviando un correo al empleado1 y si todo está bien, lo debería de recibir el empleado2. Esto lo hacemos enviando un correo con el comando:

echo "Correo reenviado test" | mail -s "Prueba reenvío" empleado1@mail.codearts.local

Y comprobamos el archivo de empleado2:

sudo less /var/mail/usuarios/empleado2



```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: /var/mail/usuarios
File Edit View Search Terminal Help

From AZDINFARISSE@SVR-BASE-AZDINFARISSE  Fri Jul 11 13:37:04 2025
Return-Path: <AZDINFARISSE@SVR-BASE-AZDINFARISSE>
X-Original-To: empleado1@mail.codearts.local
Delivered-To: empleado2@mail.codearts.local
Received: by mail.codearts.local (Postfix, from userid 1000)
        id B8B9D8D2CE; Fri, 11 Jul 2025 13:37:04 +0200 (CEST)
Subject: Prueba reenvio
To: <empleado1@mail.codearts.local>
User-Agent: mail (GNU Mailutils 3.17)
Date: Fri, 11 Jul 2025 13:37:04 +0200
Message-Id: <2025071113704.B8B9D8D2CE@mail.codearts.local>
From: AZDINFARISSE <AZDINFARISSE@SVR-BASE-AZDINFARISSE>

Correo reenviado test
/var/mail/usuarios/empleado2 (END)
```

Como se puede ver en la foto, el correo ha sido entregado al empleado2 correctamente.

3. Seguridad y autenticación.

Para activar la autenticación de usuarios en el servidor, lo haremos activandola en Postfix añadiendo las siguientes lineas al archivo [main.cf](#):

— SASL —

```
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $mydomain
# Solo aceptar correo de usuarios autenticados por 587/465
smtpd_recipient_restrictions =
    permit_sasl_authenticated,
    permit_mynetworks,
    reject_unauth_destination
```

Lo siguiente es habilitar los puertos submission y SMTPS modificando el archivo [master.cf](#) con las siguientes lineas:

```
submission inet n      -    y    -    -    smtpd
-o syslog_name=postfix/submission
-o smtpd_tls_security_level=encrypt
-o smtpd_sasl_auth_enable=yes

smtps      inet n      -    y    -    -    smtpd
-o syslog_name=postfix/smtps
-o smtpd_tls_wrappermode=yes
-o smtpd_sasl_auth_enable=yes
```

Para probar desde un cliente introducimos el comando:

```
openssl s_client -starttls smtp -connect 192.168.100.1:587
```

```

admin@kali:~$ openssl s_client -connect 192.168.100.1:587
Archive  Máquina  Ver  Entrada  Dispositivos  Ayuda
250 CHUNKING
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol: TLSv1.3
    Cipher: TLS_AES_256_GCM_SHA384
    Session-ID: D3B510CEE77620BCC176AFFB0EF9B144812DF2C1DFFD03B0A8ED03ADA1A6AE6
    Session-ID-ctx:
    Resumption PSK: 4476645913BF436FA2BF3BAE917D1DBD61AFD6A82D6E9F40BADA571B4876BD4DA6C3668297E2A85740846C569D21
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
0000 - d3 30 c7 f0 b7 ae 83 fc 7f ea 0a 7a b6 2e ba d0 .0.....Z....
0010 - 53 46 d5 95 5c 41 90 40 50 b4 b2 af bd fb c5 bb 50 S...A...P.....F
0020 - ee 3c 39 13 63 92 79 74 14 b6 4b 0b 01 92 41 51 .9.c.x).H...AQ
0030 - c1 6a ec d4 93 41 39 dc 50 7e c2 f6 78 22 87 .r.l...Q P...s*
0040 - 1b 27 22 39 a3 9a 2e 52 b4 88 ee ac 0c 7a 68 03 .004...R.....zh
0050 - 11 09 3a a6 25 29 eb 1b ca b3 0f b6 24 62 71 f8 .1.2.2.0.....$bq
0060 - 27 b0 44 a6 95 eb d6 9f e1 4f ea ba c9 2d e4 6a .7H.....0...s d
0070 - 9f 54 ea 74 04 5f 66 15 1d 8a d3 19 21 e3 90 98 .T...f.....t...
0080 - e5 de bd f3 e4 86 e8 5b c3 e6 df b4 7e 86 4f a0 .0.....f.....0.
0090 - 39 10 ae 68 9b 65 fc f7 7e d3 03 af cb 32 b9 9f .9...h.c...C...o.Z...
00a0 - b3 29 c2 14 07 2b ea c3 00 44 ec 3d 82 3e e1 71 .)b.....D...>q
00b0 - 40 38 c4 92 21 b5 93 3b 27 2e 08 ba cd a7 88 85 08...f.....0...
00c0 - 4f 25 98 80 fa 04 97 00 8d 20 ca 9b d1 29 78 72 02.....0....x
Start Time: 1752473821
Timeout: 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0

read R BLOCK
EHLO localhost
250 mail.contracts.local
250 PIPELINING
250 SIZE 10240000
250 VRFY
250 ETAM
250 AUTH PLAIN LOGIN
250 ENHANCEDSTATUSCODES
250 BR/IN/IT/NE
250 DSN
250 SMTPUTF8
250 CHUNKING
22
[121] Stopped
obokuser@kali:~$ openssl s_client -starttls smtp -connect 192.168.100.1:587

```

```
sudo openssl req -new -x509 -days 3650 -nodes \
-out /etc/ssl/certs/mail.codearts.local.crt \
-keyout /etc/ssl/private/mail.codearts.local.key \
-subj "/CN=mail.codearts.local"
sudo chmod 600 /etc/ssl/private/mail.codearts.local.key
```

[illegible]

```
GNU nano 7.2 /etc/dovecot/conf.d/10-ssl.conf *
##
## SSL settings
##
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = required

# 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/ssl/certs/mail.codearts.local.crt
ssl_key = </etc/ssl/private/mail.codearts.local.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 =

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
^C Location   ^_ Undo       ^M-U Undo     ^M-E Redo     ^M-C Copy
```

Ahora para instalar y configurar DKIM lo hacemos introduciendo el comando:

```
sudo apt install opendkim opendkim-tools
```

Y generamos una clave con los comandos:

```
sudo mkdir -p /etc/opendkim/keys/codearts.local
cd /etc/opendkim/keys/codearts.local
sudo opendkim-genkey -s selector1 -d mail.codearts.local
sudo chown opendkim:opendkim selector1*
```

Ahora modificamos la configuración del archivo **/etc/opendkim.conf**:

```
AutoRestart      Yes
Domain           mail.codearts.local
KeyFile          /etc/opendkim/keys/codearts.local/selector1.private
Selector         selector1
Socket           inet:12301@localhost
Canonicalization relaxed/simple
Mode             sv
```

```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: /etc/opendkim/keys/codearts.local
File Edit View Search Terminal Help
GNU nano 7.2 /etc/opendkim.conf *
PidFile /run/opendkim/opendkim.pid

# Hosts for which to sign rather than verify, default is 127.0.0.1. See the
# OPERATION section of opendkim(8) for more information.
#InternalHosts 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12

# The trust anchor enables DNSSEC. In Debian, the trust anchor file is provided
# by the package dns-root-data.
TrustAnchorFile /usr/share/dns/root.key
#Nameservers 127.0.0.1

# Configura /etc/opendkim.conf (fragmento)
AutoRestart Yes
Domain mail.codearts.local
KeyFile /etc/opendkim/keys/codearts.local/selector1.private
Selector selector1
Socket inet:12301@localhost
Canonicalization relaxed/simple
Mode sv

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
^C Location   ^_ Undo       ^M-U Undo     ^M-E Redo     ^M-C Copy
```

Y en el archivo [main.cf](#) añadimos la política militer:

```
militer_default_action = accept
militer_protocol = 2
smtpd_milters = inet:localhost:12301
non_smtpd_milters = $smtpd_milters
```

Ahora vamos a establecer listas negras y filtrado antispam. Esto lo hacemos primero añadiendo en el archivo [main.cf](#) las siguientes lineas:

```
postscreen_dnsbl_sites = zen.spamhaus.org b.barracudacentral.org
postscreen_dnsbl_action = enforce
```

Ahora lanzamos los comandos:

```
sudo apt install spamassassin spamc
sudo systemctl enable --now spamassassin
```

Conectar con Postfix vía spamc/spamd usando el militer de spamass-milter

```
sudo apt install spamass-milter
sudo systemctl enable --now spamass-milter
```

```
sudo apt install rspamd
```

Y verificamos en el cliente con el comando:

```
openssl s_client -connect mail.codearts.local:587 -starttls smtp
```

Y también con:

```
openssl s_client -connect mail.codearts.local:993
```

```
pc-administracion1 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

0090 - f6 0c bd 3d 39 55 21 22-34 b5 72 d0 19 d2 76 6b ...=9U"4.r...uk
00a0 - af b0 81 81 5a 81 1b 2d-48 a4 5c c4 1c d5 2a 65 ...2...H...e
00b0 - a2 8a e1 97 6e 9c 7f 1f-17 d2 33 2a 10 19 d3 4f ...n...3*...0
00c0 - 11 72 8a ad 3e 84 71 0e-6d d8 7e aa 55 bc b0 da ...>.q.m...U...
00d0 - bd 4e 24 23 5a cf 5e 8f-10 7a 36 c7 27 4f 2e b7 ...N$#2...z6.'0...

Start Time: 1752480916
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0

read R BLOCK

Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol : TLSv1.3
    Cipher : TLS_AES_256_GCM_SHA384
    Session-ID: 3920947A445914EA0160C6D1B21CE9C6354972A3F1870A76E4021BFE0C9B4A09
    Session-ID-ctx:
    Resumption PSK: 051C3B42B71562C4F562280C0622BEBE170594893C26C94EB165A7A08784FA0585465F07B14D80B379A06B7C3150DD75
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 0e 0d 2b 68 8e 53 8c 07-08 94 02 53 47 d8 c5 86 ...+h.S...S6...
    0010 - 07 a5 3b 39 a3 05 fe d8-6b 51 65 72 04 a3 5d 74 ...;9...kQer..It
    0020 - 0a 33 c2 f2 0b 6c 64 a1-77 93 1a e4 31 85 53 95 ...3...ld.u...1.S.
    0030 - fd b9 46 44 eb d6 8b ad-4d 30 08 d0 ee 5a 6d ae ...FD...M0...2m.
    0040 - d1 30 b0 36 50 cf a0 cf-f4 f7 89 92 2b a6 74 3a ...0.6P.....+t:
    0050 - 99 44 f6 89 c6 18 5f cf-21 d4 26 ad a7 85 d5 97 ...D.....t.&.....
    0060 - 9b 61 c6 af 75 79 1b c3-06 94 53 98 77 8b bb 99 ...a..ug...Y.u...
    0070 - ed ea a5 53 b6 e6 40 39-4e db b6 3c ba a6 63 2e ...S..H9M...<...e.
    0080 - d8 a9 8d aa c5 47 a9 0b-1a be c9 c4 09 17 d7 6d ......G.....m
    0090 - b2 2f 18 4a 87 d2 8f a8-d3 4a ae fb ba 5a db bb ...J...J...Z...
    00a0 - 82 86 04 03 3d 80 44 11-7d bb 0a 6b 39 6f bd 16 ......=,D...J.k9o...
    00b0 - 8a a7 00 79 2d 24 fb 4f-b8 ad d3 b2 13 a8 62 70 ...y-$..0.....bp
    00c0 - 9b 00 4b 55 c4 d5 02 44-90 4b ae cb 48 4d bb 89 ...KU...D.K..HM...
    00d0 - d2 01 ba c7 c4 a1 ad 1a-3a 74 a9 52 33 a5 06 f1 .....t.R3...

Start Time: 1752480916
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0

read R BLOCK
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot (Ubuntu) ready.
```