Correu Electrònic

PostFix

Instal·lar Postfix:
- sudo apt-get install postfix
- sudo apt-get install mailutils (opcional)

Configurar:
- escollim «Lloc d'internet»

Escrivim el domini:
- Escrivim el nostre domini «aula26.local»

Tornar a reconfigurar:
- sudo dpkg-reconfigure postfix
    - Escollim «lloc d'internet»
    - Escrivim el domini
    - Escrivim el nostre nom d'usuari
    - Borrem el domini del vallbona
    - NO forcem actualitzacions
    - Posar mida de la bustia en bytes
    - Deixem per defecte
    - IPv4

Fitxer de configuració:
- sudo nano /etc/postfix/main.cf

LOGS:
- sudo tail -f /var/log/syslog | grep postfix

Error d'enviament *(ensenya els errors quan no s'ha pogut enviar)*:
- sudo tail -f /var/log/mail.err

- sudo tail -f /var/log/msil.org

Restart del log → service postfix restart

Canviar bannner:
- Entrem al fitxer de configuració i on posa banner escrivim el nostre misstage.

```
smtpd_banner = Benvingut a aquest domini(Ubuntu)
```

Entrar al correu localment:

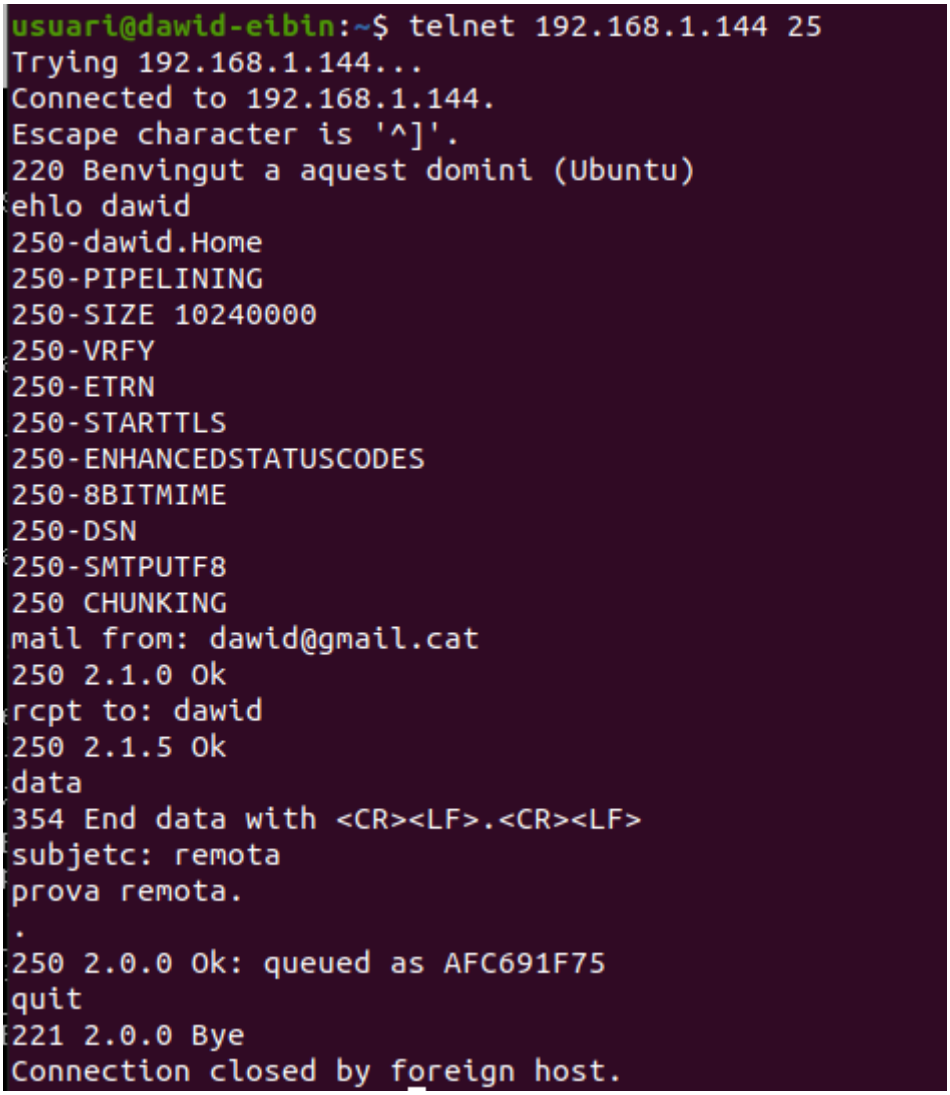
- telnet localhost 25
- Pasos següents:
    - ehlo i el nostre nom
    - MAIL FROM:
    - RCPT TO:
    - DATA
    - Subject:

Si surt «/var/mail/dawid» significa que a funcionat.

Per **llegir el misstage localment** fem un **«cat /var/mail/dawid».**

Entrar al correu remotament:

- telnet ip_del_servidor 25
- Pasos següents:
    - ehlo i el nostre nom
    - MAIL FROM:
    - RCPT TO:
    - DATA
    - Subject:



El mail que s’envian remotametn es pot anar al servidor i entrar des de /var/mail/dawid

Dovecot (per veure ell correu remotament)

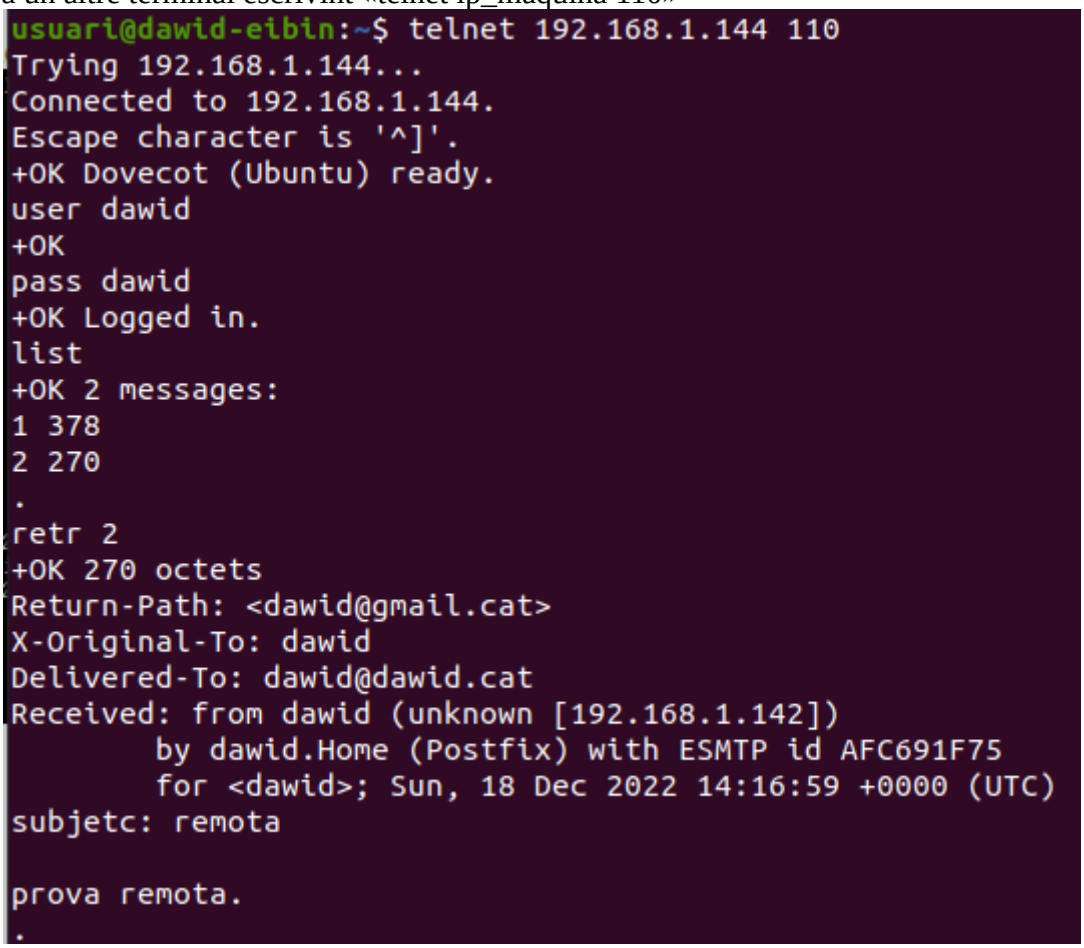
Instal·lar dovecot:
- sudo apt install dovecot-pop3d dovecot-imapd

Fitxer per configurar:
- cd /etc/dovecot (per entrar a la capreta)

I configurem el /conf.d/10-mail.conf i /etc/dovecot/dovecot.conf

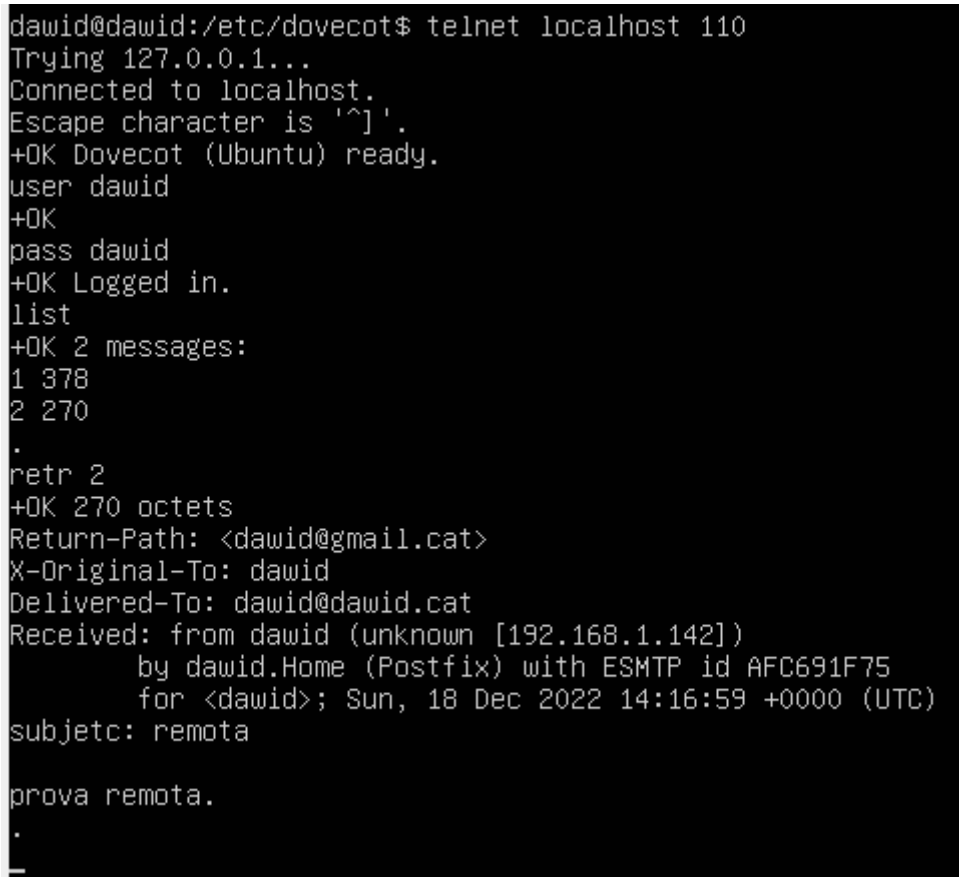
Després de fer el coanvis de configuració fem un «sudo service dovecot restart» o «service dovecot restart».

Entrar Remotament:
Entrem a un altre terminal escrivint «telnet ip_màquina 110»



Entrar Localment:

Entrem a un altre terminal escrivint «telnet localhost110»



IMAP

Localment:

Escrivim «telnet localhost imap».
Escrivim el següent:

- a1 login usuari contrsenya
- a2 list ‘’ ‘’*”
- a3 Examine inbox
- a4 fetch 1 body[] (el numero es el missatge)

```
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS AUTH=PLAIN] Dove
cot (Ubuntu) ready.
a1 login dawid dawid
a1 OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENC
ES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UI
DPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST
-STATUS BINARY MOVE SNIPPET=FUZZY PREVIEW=FUZZY PREVIEW STATUS=SIZE SAVEDATE LITERAL+ NOTIFY SPECIAL
-USE] Logged in
a2 list "" "*"
* LIST (\HasNoChildren) "/" INBOX
a2 OK List completed (0.001 + 0.000 secs).
a3 Examine inbox
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS ()] Read-only mailbox.
* 2 EXISTS
* 0 RECENT
* OK [UNSEEN 1] First unseen.
* OK [UIDVALIDITY 1671376735] UIDs valid
* OK [UIDNEXT 3] Predicted next UID
a3 OK [READ-ONLY] Examine completed (0.001 + 0.000 secs).
a4 fetch 2 body []
a4 BAD Error in IMAP command FETCH: Invalid arguments (0.001 + 0.000 secs).
a4 fetch 2 body[]
* 2 FETCH (BODY[] {270}
Return-Path: <dawid@gmail.cat>
X-Original-To: dawid
Delivered-To: dawid@dawid.cat
Received: from dawid (unknown [192.168.1.142])
        by dawid.Home (Postfix) with ESMTP id AFC691F75
        for <dawid>; Sun, 18 Dec 2022 14:16:59 +0000 (UTC)
subjetc: remota

prova remota.
)
a4 OK Fetch completed (0.001 + 0.000 secs).
```

Remotament:

Escrivim «telnet ip_del_servidor imap».
Escrivim el següent:

- a1 usuari contrsenya
- a2 list ‘’ ‘’*”
- a3 Examine inbox
- a4 fetch 1 body[] (el numero es el missatge)

```
usuari@dawid-eibin:~$ telnet 192.168.1.144 imap
Trying 192.168.1.144...
Connected to 192.168.1.144.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ START
TLS AUTH=PLAIN] Dovecot (Ubuntu) ready.
a1 login dawid dawid
a1 OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DIS
PLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL
 CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTOR
E QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE
SNIPPET=FUZZY PREVIEW=FUZZY PREVIEW STATUS=SIZE SAVEDATE LITERAL+ NOTIFY SPECIAL
-USE] Logged in
a2 list "" "*"
* LIST (\HasNoChildren) "/" INBOX
a2 OK List completed (0.001 + 0.000 secs).
a3 Examine inbox
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS ()] Read-only mailbox.
* 2 EXISTS
* 0 RECENT
* OK [UNSEEN 1] First unseen.
* OK [UIDVALIDITY 1671376735] UIDs valid
* OK [UIDNEXT 3] Predicted next UID
a3 OK [READ-ONLY] Examine completed (0.001 + 0.000 secs).
a4 fetch 1 body[]
* 1 FETCH (BODY[] {378}
Return-Path: <dawid@gmail.com>
X-Original-To: dawid
Delivered-To: dawid@dawid.cat
Received: from dawid (localhost [127.0.0.1])
        by dawid.Home (Postfix) with ESMTP id 5D57C1F5C
        for <dawid>; Sun, 18 Dec 2022 14:11:33 +0000 (UTC)
subject: hola
Message-Id: <20221218141143.5D57C1F5C@dawid.Home>
Date: Sun, 18 Dec 2022 14:11:33 +0000 (UTC)
From: dawid@gmail.com

prova.
)
a4 OK Fetch completed (0.001 + 0.000 secs).
```

OpenSSL

Autofirma amb openssl:

Entrem a la carpeta /etc/ssl

```
dawid@dawid:~$ cd /etc/ssl
dawid@dawid:/etc/ssl$ sudo openssl req -new -x509 -nodes -out certificatpostfix.crt -keyout keypostf
ix.key
```

Els dos arxius el canviem de directori:

```
dawid@dawid:/etc/ssl$ sudo mv certificatpostfix.crt certs/
dawid@dawid:/etc/ssl$ sudo mv keypostfix.key private/
```

Configuració Postfix:

```
dawid@dawid:/etc/ssl$ sudo postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/certificatpostfix.crt'
dawid@dawid:/etc/ssl$ sudo postconf -e 'smtpd_tls_key_file = /etc/ssl/private/keypostfix.key'
```

```
dawid@dawid:~$ sudo postconf -e 'smtp_tls_security_level = may'
sudo postconf -e 'smtpd_tls_security_level = may'
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
sudo postconf -e 'smtpd_tls_loglevel = 1'
sudo postconf -e 'smtpd_tls_received_header = yes'
```

Després entrem al /etc/postfix/master.cf (descomentar lo que està marcado en la foto)

```
  GNU nano 6.2                  /etc/postfix/master.cf *
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================================
smtp      inet  n       -       y       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
#tlsproxy  unix  -       -       y       -       0       tlsproxy
# Choose one: enable submission for loopback clients only, or for any client.
#127.0.0.1:submission inet n -   y       -       -       smtpd
#submission inet n       -       y       -       -       smtpd
#  -o syslog_name=postfix/submission
#  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_tls_auth_only=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
# Choose one: enable smtps for loopback clients only, or for any client.
#127.0.0.1:smtps inet n -   y       -       -       smtpd
smtps     inet  n       -       y       -       -       smtpd
```

Verificar mitjançant telnet:

```
dawid@dawid:/etc/ssl$ openssl s_client -connect localhost:465 -starttls smtp_
```

```
250 CHUNKING
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 92C5A3FE529BF97A17C67B424D42A4520BE0A871930172F0B8E5E476E90C0962
    Session-ID-ctx:
    Resumption PSK: 16BC222282DF7BAF84D37278F98F415D198E732F6EE6C136DAF3BE0341EF5E3A0323BA6A617D8248
25C7D20FA48037BC
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 23 33 4a e4 ac a9 e1 6a-9a e3 09 12 ab c5 56 2d   #3J....j......V-
    0010 - ea fc 60 8a 29 bc d1 8f-3e 24 dd 28 82 0d 1a cd   ..`.)...>$.(....
    0020 - 67 40 a8 e0 b1 3c 53 09-c0 1a c0 12 01 c4 af ea   g@...<S.........
    0030 - b3 63 b9 d1 a4 1b ac 7f-0f 3c e6 2d 27 62 ff 77   .c.......<.-'b.w
    0040 - 01 3d fb 8f 0a 99 ae e7-f0 3e e3 a0 1b 7a 2f 40   .=.......>...z/@
    0050 - 62 a4 e0 b8 5a 2c 9c 11-ad fa 13 3e a9 fc d7 04   b...Z,.....>....
    0060 - 2c e6 85 c3 5b 36 a7 9c-29 bc 54 6d 95 c1 4a 45   ,...[6..).Tm..JE
    0070 - a9 64 9a 0e fa 69 4c 9f-53 9e 48 94 b5 91 dd 68   .d...iL.S.H....h
    0080 - ca 7a ad 1f 2f 58 b1 ab-aa 6d bb 45 91 d9 40 fa   .z../X...m.E..@.
    0090 - 7d 32 8f 42 57 31 91 d4-0e 92 66 40 18 81 3c 0f   }2.BW1....f@..<.
    00a0 - 00 f4 80 b7 f1 0f 27 f9-1b 61 49 5d 2b 48 b6 54   ......'..aI]+H.T
    00b0 - fb fc 22 80 ff 60 b9 a3-4b 9d a4 3c d3 89 22 c8   .."..`..K..<.".
    00c0 - 3f 03 ae cd 67 15 00 56-dc cc 4d 1a 4b 18 6f 2f   ?...g..V..M.K.o/

    Start Time: 1671477290
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
_
```

Configuració dovecot:

```
  GNU nano 6.2                        /etc/dovecot/conf.d/10-auth.conf *
##
## Authentication processes
##

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
# See also ssl=required setting.
disable_plaintext_auth = yes
```

```
  GNU nano 6.2                          /etc/dovecot/conf.d/10-auth.conf *

# Time to delay before replying to failed authentications.
#auth_failure_delay = 2 secs

# Require a valid SSL client certificate or the authentication fails.
#auth_ssl_require_client_cert = no

# Take the username from client's SSL certificate, using
# X509_NAME_get_text_by_NID() which returns the subject's DN's
# CommonName.
#auth_ssl_username_from_cert = no

# Space separated list of wanted authentication mechanisms:
#   plain login digest-md5 cram-md5 ntlm rpa apop anonymous gssapi otp
#   gss-spnego
# NOTE: See also disable_plaintext_auth setting.
auth_mechanisms = plain login
```

Configuració en el 10-ssl.conf

```
  GNU nano 6.2                          /etc/dovecot/conf.d/10-ssl.conf
##
## SSL settings
##

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = rquired

# 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/certificatpostfix.crt
ssl_key = </etc/ssl/private/keypostfix.key
```

Verificar mitjançant telnet:

```
dawid@dawid:/etc/ssl$ openssl s_client -connect localhost:995
```

```
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 018F1A4DF67FE11BD9D342C700FD86091C281D74F250D681060C0E1E00C5D7D4
    Session-ID-ctx:
    Resumption PSK: 99CA520EC8D09443E9DD011A93F84E37E776B04AE31A075C575EFD4CBDCCAB226986C648E6E465A0
C010E3A3737E7607
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - e1 dd 9c 5a bc f4 6b 0c-c5 5e 38 2a 0e de 07 50   ...Z..k..^8*...P
    0010 - ee 53 98 71 6c a6 81 af-4d 7b 4d 5b f4 e9 bb f2   .S.ql...M{M[....
    0020 - 04 8d e2 53 cd 8d 23 ac-7d 9f bb 89 0e 8a 7d 38   ...S..#.}.....}8
    0030 - 0f eb fb 22 b1 56 55 9d-55 73 ed ae cc e8 cc ee   ...".VU.Us......
    0040 - 7f 6a a0 e4 56 a5 85 25-8f ca 37 b8 42 89 6d 41   .j..V..%..7.B.mA
    0050 - 91 b9 b7 2d 18 ff a3 62-af 38 16 c6 13 9e 60 c9   ...-...b.8....`.
    0060 - a9 e6 29 41 ec c8 87 f8-42 9d f3 b6 e7 b2 88 04   ..)A....B.......
    0070 - 2a ab 0b 06 b3 19 18 0a-b5 5d 89 57 d1 85 2c 53   *........].W..,S
    0080 - 2e 95 66 a4 3a 93 40 12-1a e8 ae 3f 25 ea 96 1a   ..f.:.@....?%...
    0090 - 52 e0 a9 1f b0 e7 d1 36-ed 71 f9 57 f3 45 92 60   R......6.q.W.E.`
    00a0 - b7 b5 d8 ab 34 a5 de 17-e7 c6 21 24 d2 00 d6 72   ....4.....!$...r
    00b0 - 50 73 8a 6f c9 b8 d1 3d-9d 27 c7 41 f3 5f c9 53   Ps.o...=.'.A._.S
    00c0 - 6d 12 0a f0 b5 a1 74 f1-f0 da b3 99 46 18 d4 f7   m.....t.....F...

    Start Time: 1670232327
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
+OK Dovecot (Ubuntu) ready.
```