Trabalho Nº6

Mail seguro

1º Criação de um certificado.

- Encriptação (conceitos)
    - Encriptação Simétrica (Chave única)
    - Encriptação Assimétrica (Chave privada e Chave Pública)
- O que é um certificado?
- SST/TLS/StartTLS
- Como criar um certificado auto-assinado (Self-signed).

```
root@dlp:~# cd /etc/ssl/private
```

```
root@dlp:/etc/ssl/private# openssl genrsa -aes128 -out server.key 2048
```

```
Generating RSA private key, 2048 bit long modulus (2 primes)
...........................+++++
............+++++
e is 65537 (0x010001)
Enter pass phrase for server.key:              # set passphrase
Verifying - Enter pass phrase for server.key:  # confirm

# remove passphrase from private key

root@dlp:/etc/ssl/private#
openssl rsa -in server.key -out server.key

Enter pass phrase for server.key:
# input passphrase

writing RSA key
```

```
root@dlp:/etc/ssl/private#
openssl req -new -days 3650 -key server.key -out server.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) [AU]:PT                            # country code
```

```
State or Province Name (full name) [Some-State]:Alto Minho        # state
Locality Name (eg, city) []:Viana do Castelo                            # city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IPVC   # company
Organizational Unit Name (eg, section) []:ESTG          # department
Common Name (e.g. server FQDN or YOUR name) []:www.grupo06.pt     # server's FQDN
Email Address []:root@grupo06.pt                                  # admin email a
ddress

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

root@dlp:/etc/ssl/private# openssl x509 -in server.csr -out server.crt -req -
signkey server.key -days 3650
```

```
Signature ok
subject=C = JP, ST = Hiroshima, L = Hiroshima, O = GTS, OU = Server World, CN = d
lp.srv.world, emailAddress = root@srv.world
Getting Private key

root@dlp:/etc/ssl/private# ll (ou ls)
```

```
total 12
-rw-r--r-- 1 root root 1334 Aug 19 19:31 server.crt
-rw-r--r-- 1 root root 1062 Aug 19 19:30 server.csr
-rw------- 1 root root 1675 Aug 19 19:30 server.key
```

Confirmar que estão estes 3 ficheiros no diretório /etc/ssl/private.

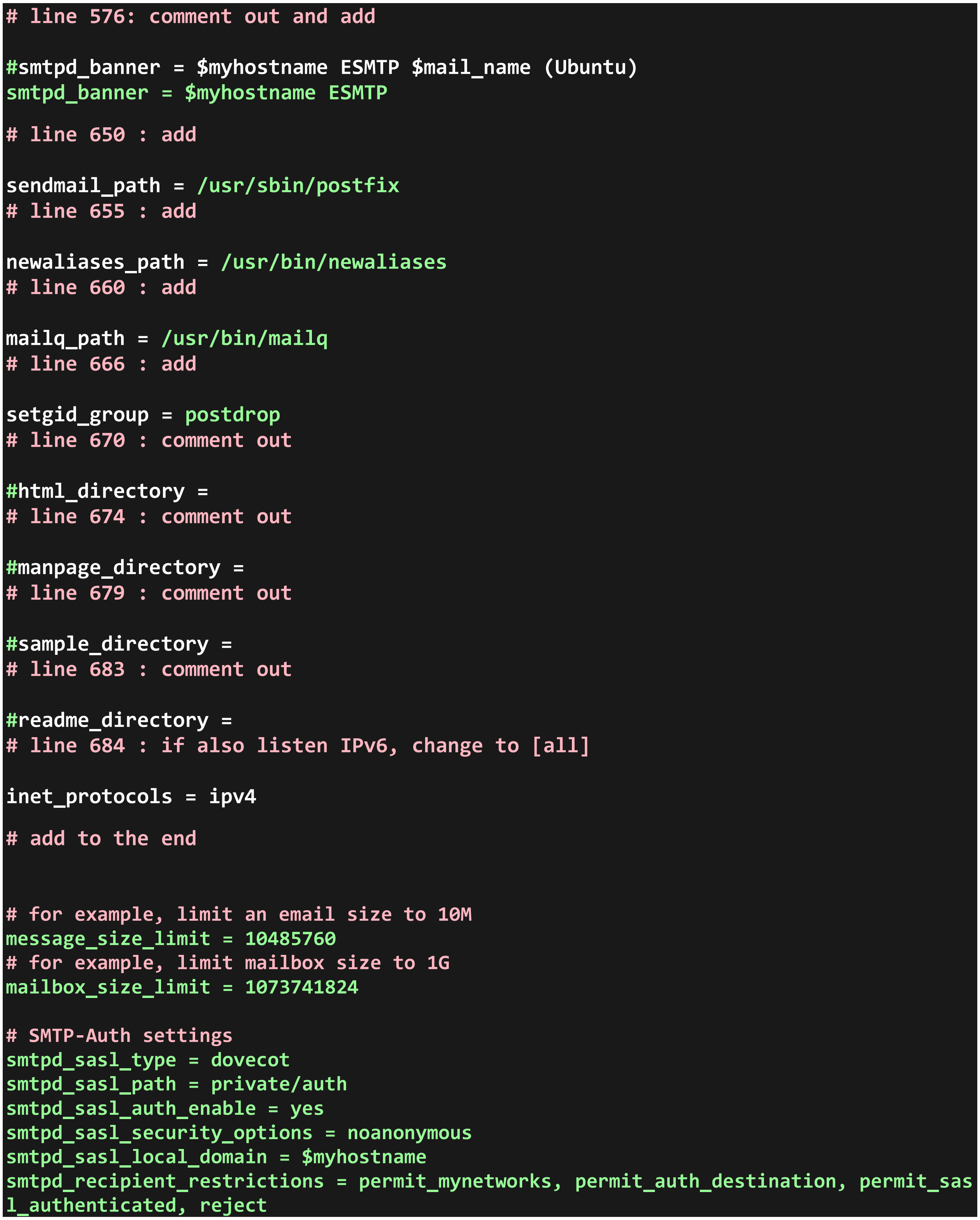
2º Instalar um Servidor SMTP (Postfix)

```
root@mail:~#
apt -y install postfix sasl2-bin

# on this example, proceed to select [No Configuration]
# because configure all manually
```

```
+------+ Postfix Configuration +-------+
| General type of mail configuration:  |
|                                      |
|       No configuration               |
|       Internet Site                  |
|       Internet with smarthost        |
|       Satellite system               |
|       Local only                     |
|                                      |
|                                      |
|       <Ok>           <Cancel>        |
|                                      |
+--------------------------------------+
```

```
root@mail:~#
cp /usr/share/postfix/main.cf.dist /etc/postfix/main.cf
```

```
root@mail:~#
vi /etc/postfix/main.cf

# line 78 : uncomment

mail_owner = postfix

# line 94 : uncomment and specify hostname

myhostname = mail.grupo06.pt
# line 102 : uncomment and specify domainname

mydomain = grupo06.pt
# line 123 : uncomment

myorigin = $mydomain

# line 137 : uncomment

inet_interfaces = all

# line 185 : uncomment

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

# line 228 : uncomment

local_recipient_maps = unix:passwd.byname $alias_maps

# line 270 : uncomment

mynetworks_style = subnet

# line 287 : add your local network

mynetworks = 127.0.0.0/8, 10.0.6.0/24
# line 407 : uncomment

alias_maps = hash:/etc/aliases

# line 418 : uncomment

alias_database = hash:/etc/aliases

# line 440 : uncomment

home_mailbox = Maildir/
```



```
# line 576: comment out and add

#smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
smtpd_banner = $myhostname ESMTP

# line 650 : add

sendmail_path = /usr/sbin/postfix
# line 655 : add

newaliases_path = /usr/bin/newaliases
# line 660 : add

mailq_path = /usr/bin/mailq
# line 666 : add

setgid_group = postdrop
# line 670 : comment out

#html_directory =
# line 674 : comment out

#manpage_directory =
# line 679 : comment out

#sample_directory =
# line 683 : comment out

#readme_directory =
# line 684 : if also listen IPv6, change to [all]

inet_protocols = ipv4

# add to the end


# for example, limit an email size to 10M
message_size_limit = 10485760
# for example, limit mailbox size to 1G
mailbox_size_limit = 1073741824

# SMTP-Auth settings
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
smtpd_recipient_restrictions = permit_mynetworks, permit_auth_destination, permit_sas
l_authenticated, reject
```

2º Instalar um Servidor POP/IMAP (Dovecot)

```
root@mail:~# apt -y install dovecot-core dovecot-pop3d dovecot-imapd

root@mail:~# nano -c /etc/dovecot/dovecot.conf
# line 30 : uncomment

listen = *

root@mail:~# nano -c /etc/dovecot/conf.d/10-auth.conf
# line 10 : uncomment and change (allow plain text auth)

disable_plaintext_auth = no
# line 100 : add

auth_mechanisms = plain login

root@mail:~# nano -c /etc/dovecot/conf.d/10-mail.conf
# line 30 : change to Maildir

mail_location = maildir:~/Maildir

root@mail:~# nano -c /etc/dovecot/conf.d/10-master.conf
# line 107-109 : uncomment and add


  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }

root@mail:~# systemctl restart dovecot
```

3º Adicionar mais contas de mail (neste caso user chamado debian)

```
# install mail client

root@mail:~# apt -y install mailutils
# set environment variables to use Maildir

root@mail:~# echo 'export MAIL=$HOME/Maildir/' >> /etc/profile.d/mail.sh
# add an OS user [debian]
```

```
root@mail:~#adduser debian
```

4º Teste do mail na linha de comandos

```
# send to myself [mail (username)@(hostname)]
```

```
debian@mail:~$ mail debian@localhost
```

```
# input Cc
Cc:
# input subject
Subject: Test Mail#1
# input messages
This is the first mail.

# to finish messages, push [Ctrl + D] key

# see received emails
```

```
debian@mail:~$ mail
```

```
"/home/debian/Maildir/": 1 message 1 new
>N   1 debian             Tue Sep 14 04:11  13/451   Test Mail#1

# input the number you'd like to see an email
? 1
Return-Path: <debian@mail.grupo06.pt>
X-Original-To: debian@localhost
Delivered-To: debian@localhost
Received: by mail.grupo06.pt (Postfix, from userid 1000)
        id 7321DC03AC; Mon, 13 Sep 2021 23:11:29 -0500 (CDT)
To: <debian@localhost>
Subject: Test Mail#1
X-Mailer: mail (GNU Mailutils 3.10)
Message-Id: <20210914041129.7321DC03AC@mail.grupo06.pt>
Date: Mon, 13 Sep 2021 23:11:29 -0500 (CDT)
From: debian <debian@mail.grupo06.pt>

This is the first mail.

# to quit, input [q]
? q
Saved 1 message in /home/debian/mbox
Held 0 messages in /home/debian/Maildir/
```

5ª Configurar os servidores para usarem SSL/TLS .

```
root@mail:~# nano -c /etc/postfix/main.cf
# add to the end
```

```
smtpd_use_tls = yes
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3
smtpd_tls_cert_file = /etc/ssl/private/server.crt
smtpd_tls_key_file = /etc/ssl/private/server.key
```

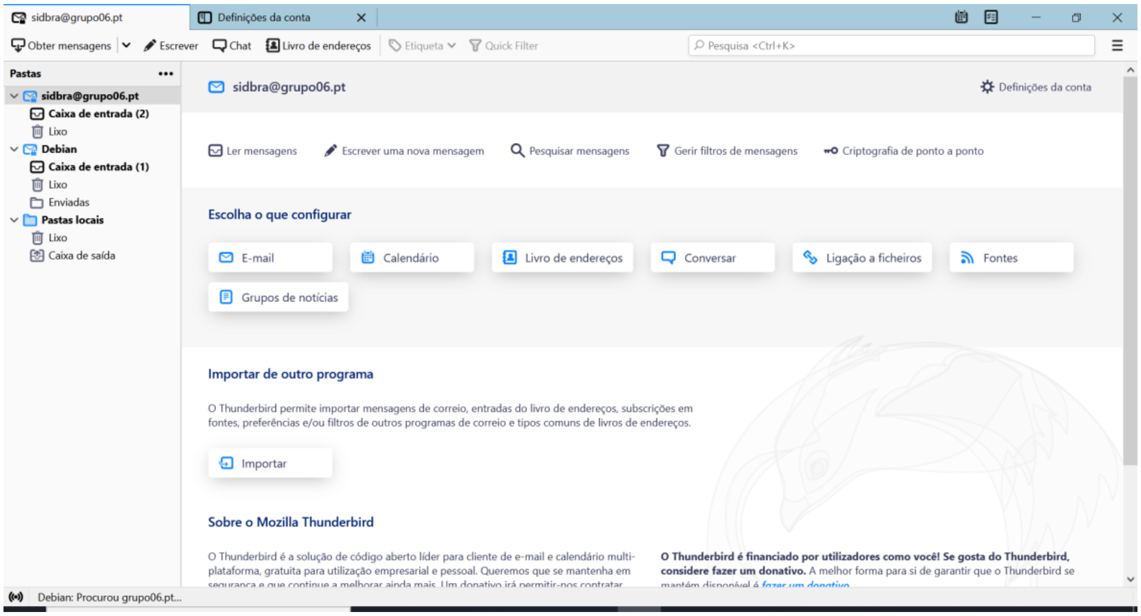
```
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache

root@mail:~# vi /etc/postfix/master.cf
# line 17-20 : uncomment
```

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

# line 29-32 : uncomment
```

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

root@mail:~# nano -c /etc/dovecot/conf.d/10-ssl.conf
# line 6 : change

ssl = yes
# line 12,13 : uncomment and specify certificates

ssl_cert = </etc/ssl/private/server.crt
ssl_key = </etc/ssl/private/server.key
```

```
root@mail:~# systemctl restart postfix dovecot
```

6º Configurar os clientes de Mail (neste caso o Mozilla Thunderbird) .



Escolha o que configurar

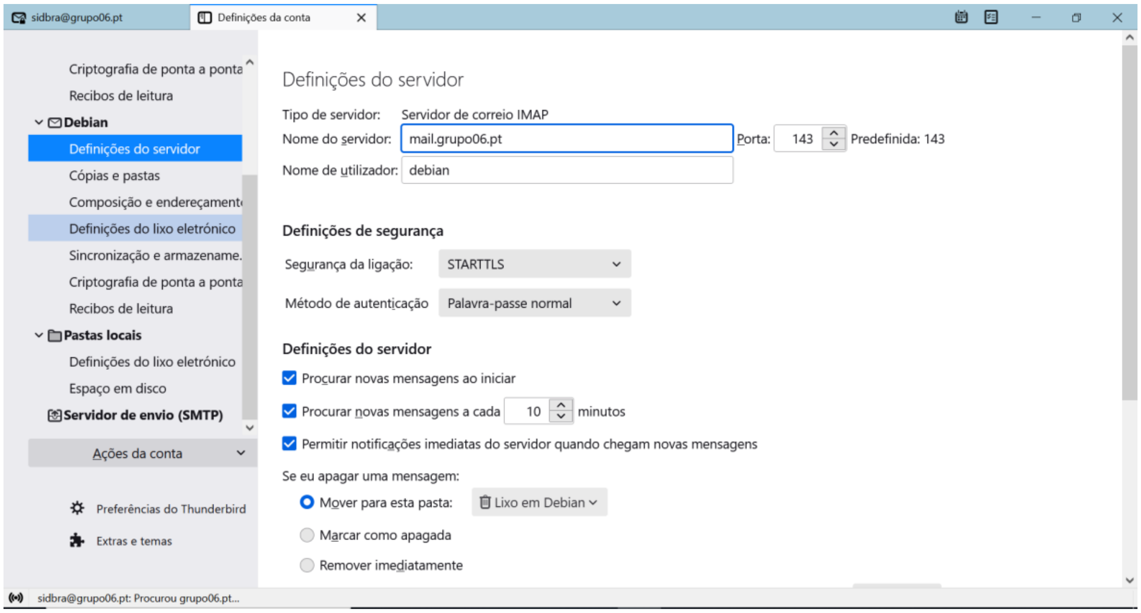
Importar de outro programa

O Thunderbird permite importar mensagens de correio, entradas do livro de endereços, subscrições em fontes, preferências e/ou filtros de outros programas de correio e tipos comuns de livros de endereços.

Sobre o Mozilla Thunderbird

O Thunderbird é a solução de código aberto líder para cliente de e-mail e calendário multi-plataforma, gratuita para utilização empresarial e pessoal. Queremos que se mantenha em segurança e que continue a melhorar ainda mais. Um donativo irá permitir-nos contratar

O Thunderbird é financiado por utilizadores como você! Se gosta do Thunderbird, considere fazer um donativo. A melhor forma para si de garantir que o Thunderbird se mantém disponível é *fazer um donativo*.


sidbra@grupo06.pt
Definições da conta
Criptografia de ponta a ponta
Recibos de leitura
Debian
Definições do servidor
Cópias e pastas
Composição e endereçamento
Definições do lixo eletrónico
Sincronização e armazenamento
Criptografia de ponta a ponta
Recibos de leitura
Pastas locais
Definições do lixo eletrónico
Espaço em disco
Servidor de envio (SMTP)
Ações da conta
Preferências do Thunderbird
Extras e temas
sidbra@grupo06.pt: Procurou grupo06.pt...

Definições do servidor

Tipo de servidor: Servidor de correio IMAP

Nome do servidor: mail.grupo06.pt Porta: 143 Predefinida: 143

Nome de utilizador: debian

Definições de segurança

Segurança da ligação: STARTTLS

Método de autenticação: Palavra-passe normal

Definições do servidor

☑ Procurar novas mensagens ao iniciar

☑ Procurar novas mensagens a cada 10 minutos

☑ Permitir notificações imediatas do servidor quando chegam novas mensagens

Se eu apagar uma mensagem:

● Mover para esta pasta: Lixo em Debian

○ Marcar como apagada

○ Remover imediatamente

7º Instalar um sistema de Webmail (RoundCube) .

Configurar o Apache para usar SSL/TLS (caso não fosse feito no trabalho 5)

```
root@www:~# nano-c /etc/apache2/sites-available/default-ssl.conf
# line 3 : change admin email

ServerAdmin root@grupo06.pt
# line 32,33 : change to the certs gotten in section [1]
```

```

SSLCertificateFile      /etc/ssl/private/server.crt
SSLCertificateKeyFile  /etc/ssl/private/server.key

```

```
# SSLCertificateChainFile /etc/letsencrypt/live/www.srv.world/chain.pem

root@www:~# a2ensite default-ssl
```

```
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2

root@www:~# a2enmod ssl
```

```
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create se
lf-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2

root@www:~#systemctl restart apache2
```

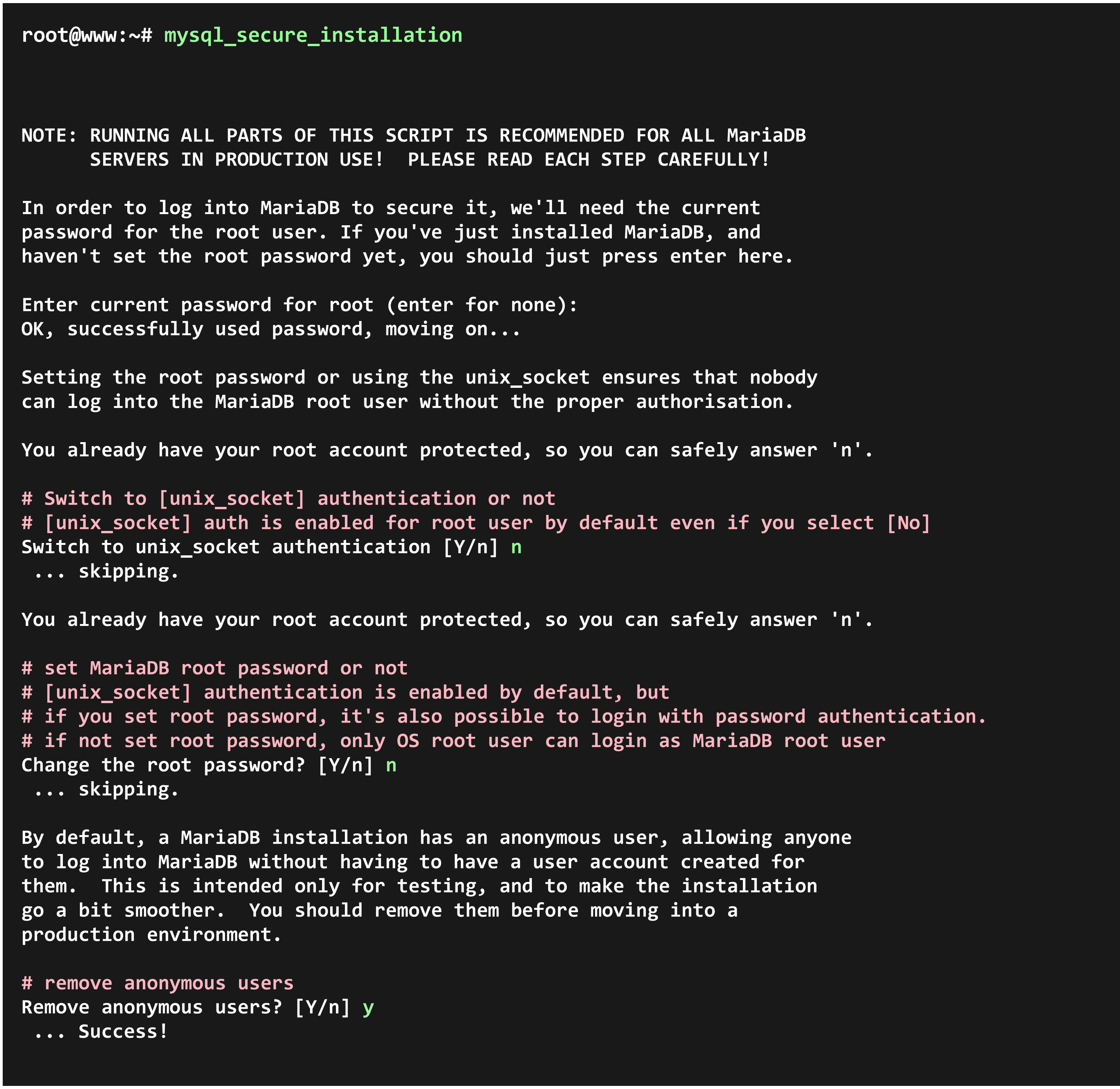
Instalar MariaDB para configurar um Servidor de Base de Dados

```
root@www:~# apt -y install mariadb-server
root@www:~# nano -c /etc/mysql/mariadb.conf.d/50-server.cnf
# line 93 : confirm default charaset
# if use 4 bytes UTF-8, specify [utf8mb4]
```

```
character-set-server  = utf8mb4
collation-server      = utf8mb4_general_ci
```

```
root@www:~# systemctl restart mariadb
```

Settings iniciais para MariaDB



```
root@www:~# mysql_secure_installation



NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

# Switch to [unix_socket] authentication or not
# [unix_socket] auth is enabled for root user by default even if you select [No]
Switch to unix_socket authentication [Y/n] n
 ... skipping.

You already have your root account protected, so you can safely answer 'n'.

# set MariaDB root password or not
# [unix_socket] authentication is enabled by default, but
# if you set root password, it's also possible to login with password authentication.
# if not set root password, only OS root user can login as MariaDB root user
Change the root password? [Y/n] n
 ... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

# remove anonymous users
Remove anonymous users? [Y/n] y
 ... Success!
```

```
Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

# disallow root login remotely
Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

# remove test database
Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

# reload privilege tables
Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!

# connect to MariaDB

root@www:~# mysql


Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 50
Server version: 10.5.11-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

# [Unix_Socket] authentication is enabled by default
MariaDB [(none)]> show grants for root@localhost;
+-----------------------------------------------------------------------------------------------
----------------------------+
| Grants for root@localhost
|
+-----------------------------------------------------------------------------------------------
----------------------------+
| GRANT ALL PRIVILEGES ON *.* TO `root`@`localhost` IDENTIFIED VIA mysql_native_password USING 'i
ix_socket WITH GRANT OPTION |
| GRANT PROXY ON ''@'%' TO 'root'@'localhost' WITH GRANT OPTION
|
+-----------------------------------------------------------------------------------------------
----------------------------+
2 rows in set (0.000 sec)

# show user list
MariaDB [(none)]> select user,host,password from mysql.user;
+-------------+-----------+----------+
| User        | Host      | Password |
+-------------+-----------+----------+
| mariadb.sys | localhost |          |
| root        | localhost | invalid  |
| mysql       | localhost | invalid  |
+-------------+-----------+----------+
3 rows in set (0.001 sec)

# show database list
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.000 sec)

# create test database
MariaDB [(none)]> create database test_database;
Query OK, 1 row affected (0.000 sec)

# create test table on test database
MariaDB [(none)]> create table test_database.test_table (id int, name varchar(50), address varcha
y key (id));
Query OK, 0 rows affected (0.108 sec)

# insert data to test table
MariaDB [(none)]> insert into test_database.test_table(id, name, address) values("001", "Debian",
;
Query OK, 1 row affected (0.036 sec)

# show test table
MariaDB [(none)]> select * from test_database.test_table;
+----+--------+-----------+
| id | name   | address   |
+----+--------+-----------+
|  1 | Debian | Hiroshima |
+----+--------+-----------+
1 row in set (0.000 sec)
```

```
# delete test database
MariaDB [(none)]> drop database test_database;
Query OK, 1 row affected (0.111 sec)

MariaDB [(none)]> exit
Bye
```

Criar uma Base de Dados para RoundCube.

```
root@www:~# mysql
```

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 50
Server version: 10.5.11-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

# create [roundcube] database
# replace [password] to your own password you'd like to set
MariaDB [(none)]> create database roundcube;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> grant all privileges on roundcube.* to roundcube@'localhost' id
entified by 'password';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> exit
Bye
```

] Instalar e Configurar RoundCube.

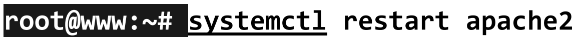
```
root@www:~#
apt -y install roundcube roundcube-mysql

# select [No] on this example (set manually later)
```

```
 +----------------------+ Configuring roundcube-core +-----------------------+
 |                                                                           |
 | The roundcube package must have a database installed and configured     |
 | before it can be used.  This can be optionally handled with              |
 | dbconfig-common.                                                         |
 |                                                                          |
 | If you are an advanced database administrator and know that you want to  |
 | perform this configuration manually, or if your database has already     |
 | been installed and configured, you should refuse this option.  Details   |
 | on what needs to be done should most likely be provided in               |
 | /usr/share/doc/roundcube.                                                |
 |                                                                          |
 | Otherwise, you should probably choose this option.                       |
 |                                                                          |
 | Configure database for roundcube with dbconfig-common?                   |
 |                                                                          |
 |                   <Yes>                          <No>                    |
 |                                                                          |
 +--------------------------------------------------------------------------+
```

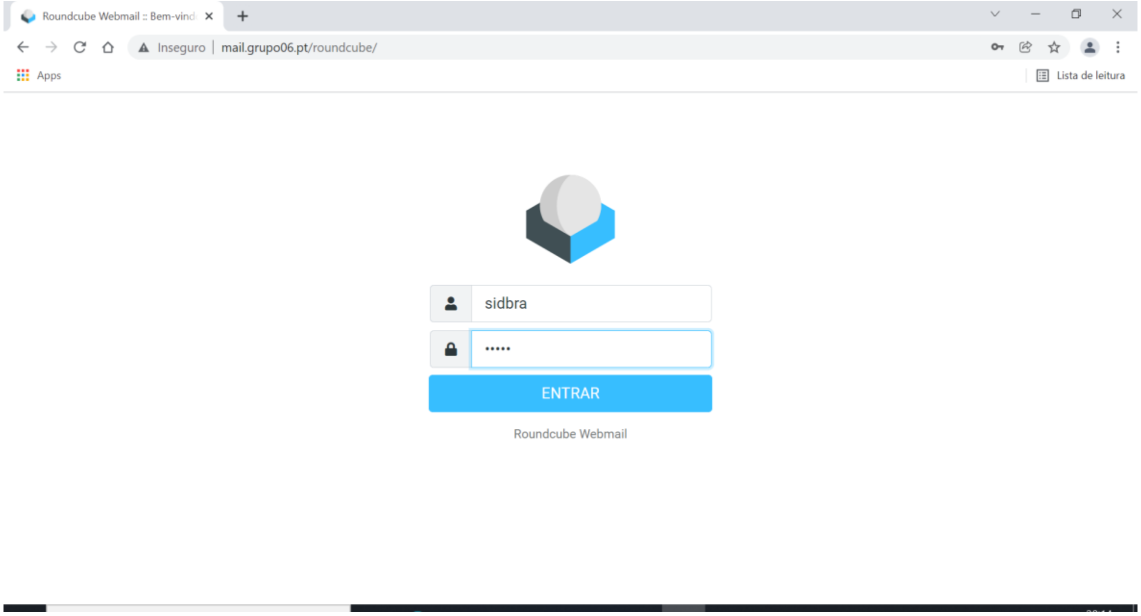
```
root@www:~# cd /usr/share/dbconfig-common/data/roundcube/install

root@www:/usr/share/dbconfig-common/data/roundcube/install# mysql -u roundcube -D
roundcube -p < mysql

Enter password:
# MariaDB roundcube password

root@www:/usr/share/dbconfig-common/data/roundcube/install# cd
```

```
root@www:~# vi /etc/roundcube/debian-db.php
# set database info

$dbuser='roundcube';
$dbpass='12345'; //é a minha password
$basepath='';
$dbname='roundcube';
$dbserver='localhost';
$dbport='3306';
$dbtype='mysql';

root@www:~# nano -c /etc/roundcube/config.inc.php
# line 36 : specify IMAP server (STARTTLS setting)

$config['default_host'] = 'localhost';

# line 48 : specify SMTP server (STARTTLS setting)

$config['smtp_server'] = 'tls://mail.grupo06.pt';

# line 51 : specify SMTP port (STARTTLS setting)

$config['smtp_port'] = 587;

# line 55 : change (use the same user for SMTP auth and IMAP auth)
```

```
$config['smtp_user'] = '%u';

# line 59 : change (use the same password for SMTP auth and IMAP auth)

$config['smtp_pass'] = '%p';

# line 66 : change to any title you like

$config['product_name'] = 'Grupo06 Webmail';

# add follows to the end


# specify IMAP port (STARTTLS setting)
$config['default_port'] = 143;

# specify SMTP auth type
$config['smtp_auth_type'] = 'LOGIN';

# specify SMTP HELO host
$config['smtp_helo_host'] = 'mail.grupo06.pt';

# specify domain name
$config['mail_domain'] = 'grupo06.pt';

# specify UserAgent
$config['useragent'] = 'Grupo06 Webmail';

# specify SMTP and IMAP connection option
$config['imap_conn_options'] = array(
  'ssl'         => array(
    'verify_peer' => true,
    'CN_match' => 'srv.world',
    'allow_self_signed' => true,
    'ciphers' => 'HIGH:!SSLv2:!SSLv3',
  ),
);
$config['smtp_conn_options'] = array(
  'ssl'         => array(
    'verify_peer' => true,
    'CN_match' => 'srv.world',
    'allow_self_signed' => true,
    'ciphers' => 'HIGH:!SSLv2:!SSLv3',
  ),
);

root@www:~# nano -c /etc/apache2/conf-enabled/roundcube.conf
# line 3 : uncomment

Alias /roundcube /var/lib/roundcube/public_html

# line 11 : change access permission if need

Require ip 127.0.0.1 10.0.6.0/24
```



```
root@www:~# systemctl restart apache2
```



Roundcube Webmail :: Bem-vind

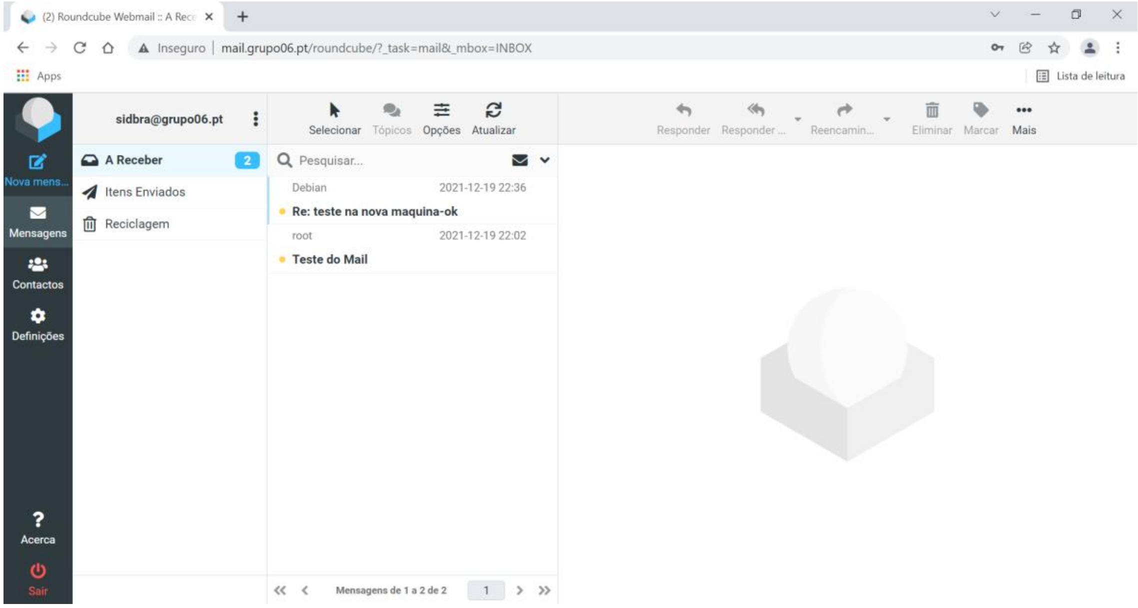
Inseguro | mail.grupo06.pt/roundcube/

sidbra

•••••

ENTRAR

Roundcube Webmail



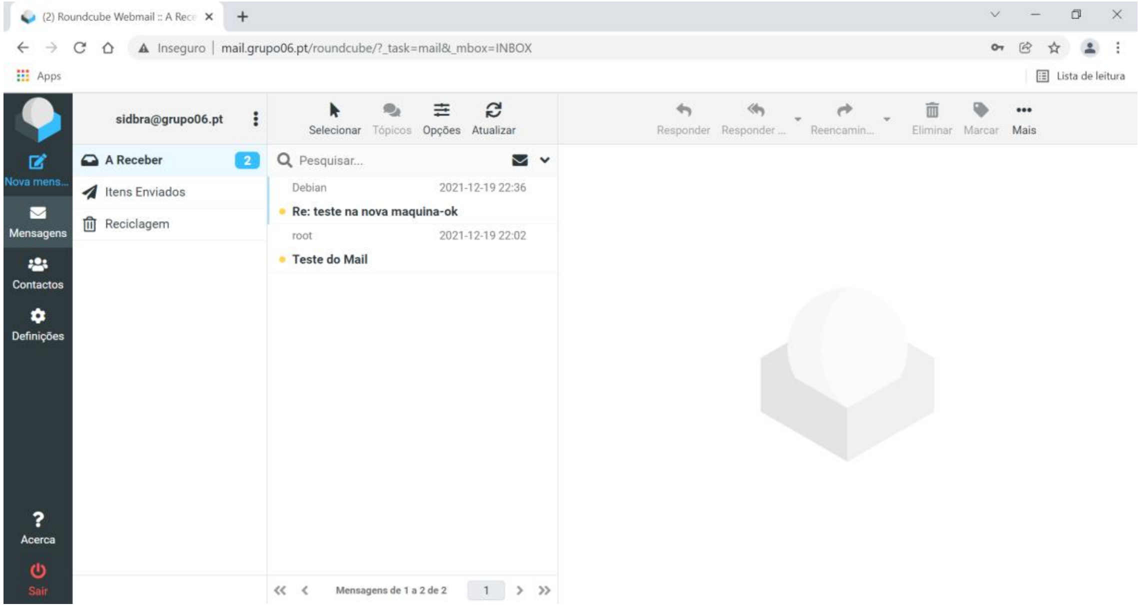
(2) Roundcube Webmail :: A Rece

Inseguro | mail.grupo06.pt/roundcube/?_task=mail&_mbox=INBOX

sidbra@grupo06.pt

Debian	2021-12-19 22:36
Re: teste na nova maquina-ok	
root	2021-12-19 22:02
Teste do Mail	

Mensagens de 1 a 2 de 2



Debian 2021-12-19 22:36
Re: teste na nova maquina-ok

root 2021-12-19 22:02
Teste do Mail

Mensagens de 1 a 2 de 2 1