

## Práctica A6.D1: Servicio de correo electrónico

En esta práctica vamos a aprender a instalar y a configurar un servicio de correo electrónico en un sistema Linux sobre una instancia de AWS.

El contenido de los archivos *hostname* y *hosts* es muy importante. Antes de comenzar prestemos atención a la forma de cambiar el hostname en una máquina AWS tal y como indica la [documentación de AWS](#).

Para que la actualización del nombre de host persista, Se debe verificar que la configuración *preserve\_hostname* cloud-init esté establecida en *true*. Modifica el siguiente fichero:

```
sudo nano /etc/cloud/cloud.cfg
```

Si la configuración *preserve\_hostname* no aparece en la lista, agregue la siguiente línea de texto al final del archivo:

```
preserve_hostname: true
```

Ejecute el comando

```
sudo hostnamectl set-hostname mail
```

y esto cambiará el archivo *hostname* al valor indicado; el nombre de tu sistema (sin dominio)

El archivo */etc/hosts* debería quedar de la forma:

```
GNU nano 6.2
127.0.0.1 localhost
127.0.1.1 mail.mlls.line.pm mail

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

En este caso el nombre corto de mi equipo es *mail* y el dominio para el que estamos instalando nuestro correo es *mlls.line.pm*, es decir, las cuentas de nuestro correo serán del tipo *usuario@mlls.line.pm*

En la introducción al servicio de correo ya instalamos Postfix y probamos a enviar correo desde el mismo servidor con la herramienta telnet y con mail.

Como **Amazon bloquea la salida por el puerto 25**, desde nuestro servidor **NO resulta posible enviar correos hacia el exterior** (gmail, yahoo, etc). En cualquier caso, deberíamos revisar las técnicas propuestas para intentar que tu servidor de correo sea considerado fiable: SPF, DKIM y DMARC. En uno de los puntos de esta práctica se os pedirá que implementéis estas técnicas en vuestro servidor de correo y en vuestro dominio dinámico de [dnsexit](#).

## A tener en cuenta:

- El **servidor de correo será instalado en una instancia EC2 de tipo small y con un disco de 16 GB**. Se le debe **asociar una IP elástica** que luego se utilizará para la creación de los registros en dnsexit.
- Antes de crear la instancia sería recomendable **asignarle un Grupo de Seguridad** que permita el tráfico entrante a los puertos TCP siguientes desde cualquier dirección IP (no es necesario incluir todos los puertos ahora, sólo conforme los vayamos usando):

25 (SMTP)

80 (HTTP)

110 (POP3)

143 (IMAP)

443 (HTTPS)

465 (SMTPS)

993 (IMAPS)

995 (POP3S)

El puerto 22 (SSH) debería abrirse pero, en la práctica, sólo para las IP usadas para la administración remota.

- El dominio de correo electrónico que vamos a utilizar será uno dinámico de DNSExit, del tipo **xxx.line.pm** o similar, pero teniendo en cuenta que **debe** incluir tus iniciales **xxx**.

El nombre corto del equipo será **mail** por lo que el nombre largo será **mail.xxx.line.pm**

Tus cuentas de correo serán del tipo **usuario@xxx.line.pm**

Existen numerosas referencias y tutoriales por internet en los que se intenta explicar, con más o menos éxito, el proceso de instalación de un servidor de correo electrónico funcional. En la lista de enlaces interesantes de esta práctica se encuentran varias de esas referencias. Las que he catalogado como **Referencia Base** son las que están probadas y usaremos para resolver los pasos de esta práctica.

Nunca debemos olvidar que la fuente de información principal de cualquier servicio de red debe ser la página oficial de la herramienta o del protocolo en cuestión.

Los siguientes **pasos** deben realizarse sobre la instancia EC2 de AWS con AMI de Ubuntu.

Lanzar una instancia

Amazon EC2 le permite crear máquinas virtuales, o instancias, que se ejecutan en la nube de AWS. Comience rápidamente siguiendo los sencillos pasos que se indican a continuación.

Nombre y etiquetas

Nombre

Postfixmfggh

Agregar etiquetas adicionales

Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon)

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones

Recientes

Inicio rápido

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

ami-04b4f1a9cf54c11d0 (64 bits (x86)) / ami-0a7a4e87939439934 (64 bits (Arm))

Virtualización: hvm    Activado para ENA: true    Tipo de dispositivo raíz: ebs

Apto para la capa gratuita

Descripción

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Canonical, Ubuntu, 24.04, amd64 noble image

Resumen

Número de instancias

1

Imagen de software (AMI)

Canonical, Ubuntu, 24.04, amd64...más información

ami-04b4f1a9cf54c11d0

Tipo de servidor virtual (tipo de instancia)

t2.small

Firewall (grupo de seguridad)

Nuevo grupo de seguridad

Almacenamiento (volúmenes)

Volúmenes: 1 (16 GiB)

Cancelar

Lanzar instancia

Código de versión preliminar

Free Domains Sign UP

Domain name:

mfggh.work.gd

Registration Term:

1 Year

Expiration Date:

2026-02-17 ( Free renew after 2026-01-17 )

Total:

\$ 0.00

Note:

The domain is free forever with the limitation that you can only renew within 30 days of the expiration and max renew 1 year.

Setup the DNS for the domain:

Note:

You can setup Records such as CName, MX, SRV, NS, A, AAAA later.

IP for the domain:

44.209.1.69

Is Dynamic IP?

☐

Check it if you intend to use our Dynamic DNS Clients

SUBMIT

```
ubuntu@ip-172-31-21-181: ~
GNU nano 7.2 /etc/cloud/cloud.cfg *
# The top level settings are used as module
# and base configuration.

# A set of users which may be applied and/or used by various modules
# when a 'default' entry is found it will reference the 'default_user'
# from the distro configuration specified below
users:
- default

# If this is set, 'root' will not be able to ssh in and they
# will get a message to login instead as the default $user
disable_root: true

# This will cause the set+update hostname module to not operate (if true)
preserve_hostname: true
```

```
ubuntu@ip-172-31-21-181: ~$ sudo hostnamectl set-hostname mail
ubuntu@ip-172-31-21-181: ~$ hostnamectl
  Static hostname: mail
        Icon name: computer-vm
        Chassis: vm
        Machine ID: ec25528feb3277efe8605165de67440f
        Boot ID: 651b227e2fef41e1b108ccf41133e2d8
  Virtualization: xen
  Operating System: Ubuntu 24.04.1 LTS
        Kernel: Linux 6.8.0-1021-aws
        Architecture: x86-64
  Hardware Vendor: Xen
  Hardware Model: HVM domU
  Firmware Version: 4.11.amazon
        Firmware Date: Thu 2006-08-24
        Firmware Age: 18y 5month 3w 4d
ubuntu@ip-172-31-21-181: ~$
```

```
Seleccionar ubuntu@ip-172-31-21-181: ~
GNU nano 7.2 /etc/hostname
mail
```

```
ubuntu@mail: ~
GNU nano 7.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 mail.mfgh.work.gd_mail

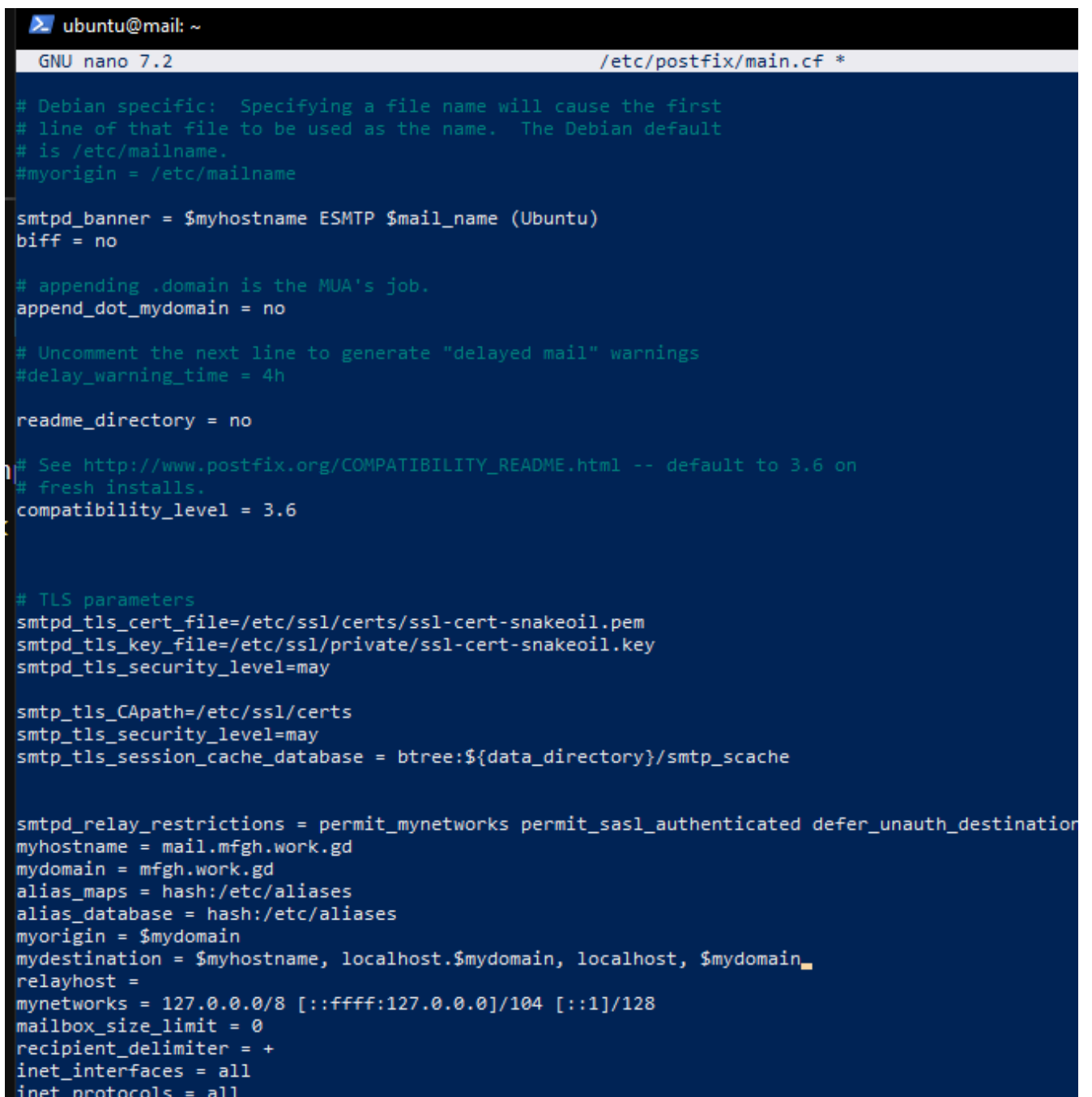
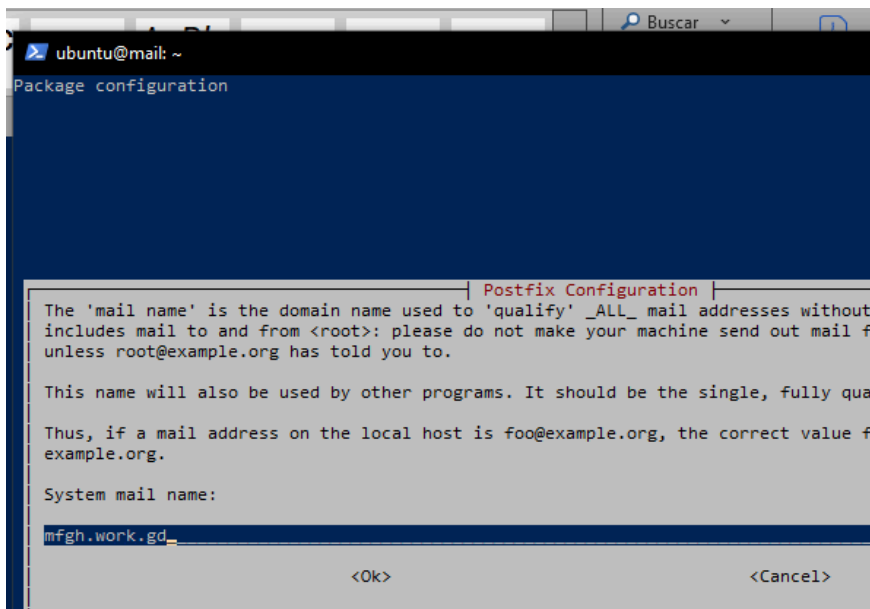
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

ubuntu@mail: ~$ sudo apt-get install mailutils
```

## Paso 1:

(1,5 ptos.)

Instalación del servidor Postfix, configuración básica y prueba de envío de correos en local, y recepción de correos desde un agente externo. Se debe configurar adecuadamente DNSexit, capturando pantallas del mismo.



Host / A Record / Sub Domain

Domain DNS | Add MX | Add Host | Add Alias | Add TXT | Add SRV | Add Self Defined

Add New Host for MFGH.WORK.GD

Host Name : mail.mfgh.work.gd

IP is: ☐ Dynamic ☒ Static

TTL : 8 hours 0 minutes

IP Address : (IPv4 or IPv6) 44.209.1.69

Submit

Services for You: [URL Forwarding](#) | [Web Hosting](#) | [Dynamic IP Update](#)

MX Records (Mail Exchangers)

Domain DNS | Add MX | Add Host | Add Alias | Add TXT | Add SRV | Add Self Defined

Modified -> Save Changes

Add MX for MFGH.WORK.GD

Mail Zone : mfgh.work.gd sub zone ?

Mail Server Name : mail.mfgh.work.gd Select hosts ?

TTL : 8 hours 0 minutes ?

Priority #: 10 (0-999) ?

Add MX

E-Mail Services for You: [Mail Relay](#) | [Mail Redirection](#) | [Business Email](#) | [Mail Forwarding](#) | [Mail Backup](#)

Zone MX Records

MX Records (MX) ? help

Mail Server	Priority #	TTL (hr.min)	Action
Add MX			

Vemos que se resuelve el registro MX.

```
PS C:\Users\2ASIR> nslookup -q=MX mfgh.work.gd
DNS request timed out.
    timeout was 2 seconds.
Servidor: UnKnown
Address: 8.8.8.8

Respuesta no autoritativa:
mfgh.work.gd    MX preference = 10, mail exchanger = mail.mfgh.work.gd
```

Probamos que se envían correos entre sí y además conecta con el exterior, abriendo los puertos necesarios para la práctica.

```
ubuntu@mail:~$ mail root@mfgh.work.gd
Cc:
Subject: prueba
prueba postmail

ubuntu@mail:~$ sudo su
root@mail:/home/ubuntu# mail
"/var/mail/root": 1 message 1 new
>N 1 Ubuntu          Fri Feb 21 12:29 13/423  prueba
?
```

Reglas de entrada (9)

Administ

Q Buscar

	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos
■	-	sgr-02a9e3e188be6cb0a	IPv4	POP3	TCP	110
■	-	sgr-0c393b432987f3f9b	IPv4	SMTPS	TCP	465
■	-	sgr-08e4d5fb8fb393af0	IPv4	IMAP	TCP	143
■	-	sgr-01d83aaa41a00b13b	IPv4	HTTP	TCP	80
■	-	sgr-06565070c3eae4803	IPv4	SSH	TCP	22
■	-	sgr-0a2e54e7ccb036638	IPv4	HTTPS	TCP	443
■	-	sgr-0c4310e65f7729032	IPv4	IMAPS	TCP	993
■	-	sgr-03b84c4aa7737337e	IPv4	SMTP	TCP	25
■	-	sgr-0ed7da7107c2f59df	IPv4	POP3S	TCP	995

prueba

M

Manuel Fernando Gómez Hernández

<mgomher1010@g.educaand.es>

para root

postmail

Responder

Reenviar

```
root@mail:/home/ubuntu# ufw disable
Firewall stopped and disabled on system startup
root@mail:/home/ubuntu# mail
No mail for root
root@mail:/home/ubuntu# mail
No mail for root
root@mail:/home/ubuntu# mail
"/var/mail/root": 1 message 1 new
>N 1 Manuel Fernando G Fri Feb 21 12:31 60/3204 prueba
?
```

**Paso 2:**

Instalación de Dovecot con cifrado TLS. Ahora ya podremos enviar y recibir correos desde una máquina distinta a nuestro servidor, utilizando un cliente de correo como Thunderbird.

Instalo certbot, apache y certbot para apache.

```

ubuntu@mail:~$ sudo apt install certbot
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-acme python3-certbot python3-configargparse python3-icu python3-josepy python3-parsedatetime
  python3-rfc3339
Suggested packages:
  python-certbot-doc python3-certbot-apache python3-certbot-nginx python-acme-doc
The following NEW packages will be installed:
  certbot python3-acme python3-certbot python3-configargparse python3-icu python3-josepy python3-parsedatetime
  python3-rfc3339
0 upgraded, 8 newly installed, 0 to remove and 69 not upgraded.
Need to get 1031 kB of archives.
After this operation, 5323 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 python3-josepy all 1.14.0-1 [22.1 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 python3-rfc3339 all 1.1-4 [6744 B]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 python3-acme all 2.9.0-1 [48.5 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 python3-configargparse all 1.7-1 [31.1 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 python3-parsedatetime all 2.6-3 [32.8 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 python3-certbot all 2.9.0-1 [267 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 python3-icu amd64 2.12-1build2 [534 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 certbot all 2.9.0-1 [89.2 kB]
Fetched 1031 kB in 0s (23.7 MB/s)
Preconfiguring packages ...
Selecting previously unselected package python3-josepy.
(Reading database ...

```

```

ubuntu@mail:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:

```

```

ubuntu@mail:~$ sudo apt install python3-certbot-apache
Reading package lists... Done
Building dependency tree... Done

```

Creo el archivo de configuración de apache y le añadimos contenido.

```

GNU nano 7.2 /etc/apache2/sites-available/sitiocorre.conf *
<VirtualHost *:80>
    ServerName mail.mfgh.work.gd

    DocumentRoot /var/www/html/
</VirtualHost>

```

Activamos este sitio y además reiniciamos apache.

```

ubuntu@mail:~$ sudo a2ensite sitiocorre.conf
Enabling site sitiocorre.
To activate the new configuration, you need to run:
    systemctl reload apache2

```

Desactivamos el sitio por defecto.

```

ubuntu@mail:~$ sudo a2dissite 000-default
Site 000-default disabled.
To activate the new configuration, you need to run:
    systemctl reload apache2
ubuntu@mail:~$ sudo systemctl reload apache2
ubuntu@mail:~$

```

Creamos el certificado.



```

ubuntu@mail: ~$ sudo systemctl reload apache2
ubuntu@mail: ~$ sudo certbot certonly -a apache --agree-tos --no-eff-email --staple-ocsp --email root@mfigh.work.gd -d mail.mfigh.work.gd
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Account registered.

```

Podemos ver que el sitio funciona.



Añadimos esto en `/etc/postfix/master.cf`

```

ubuntu@mail: ~$
GNU nano 7.2 /etc/postfix/master.cf *
#
# =====
# See the Postfix UUCP_README file for configuration details.
#
uucp    unix    -      n      n      -      -      pipe
 flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
#
# Other external delivery methods.
#
ifmail  unix    -      n      n      -      -      pipe
 flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp   unix    -      n      n      -      -      pipe
 flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
scalemail-backend unix -      n      n      -      2      pipe
 flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${u
mailman  unix    -      n      n      -      -      pipe
 flags=FRX user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py ${nexthop} ${u
submission inet    n      -      y      -      -      smtpd
 -o syslog_name=postfix/submission
 -o smtpd_tls_security_level=encrypt
 -o smtpd_tls_wrappermode=no
 -o smtpd_sasl_auth_enable=yes
 -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
 -o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject
 -o smtpd_sasl_type=dovecot
 -o smtpd_sasl_path=private/auth

```

Editamos las ultimas partes de las rutas de los certificados.

```
# TLS parameters
smtpd_tls_cert_file=/etc/letsencrypt/live/mail.mfgh.work.gd/fullchain.pem
smtpd_tls_key_file=/etc/letsencrypt/live/mail.mfgh.work.gd/privkey.pem
smtpd_tls_security_level=may
```

El servicio está activo

```
ubuntu@mail:~$ sudo ss -lnt | grep master
LISTEN 0      100          0.0.0.0:587    0.0.0.0:*    users:((("master",pid=5643,fd=95))
LISTEN 0      100          0.0.0.0:25     0.0.0.0:*    users:((("master",pid=5643,fd=13))
LISTEN 0      100          [::]:587      [::]:*       users:((("master",pid=5643,fd=96))
LISTEN 0      100          [::]:25       [::]:*       users:((("master",pid=5643,fd=14))
ubuntu@mail:~$
```

Instalo dovecot.

```
ubuntu@mail:~$ sudo apt install dovecot-core dovecot-imapd
```

```
ubuntu@mail:~$ sudo apt install dovecot-pop3d
Reading package lists... Done
```

Entramos al fichero de configuración y descomentamos.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/dovecot.conf *
# Enable installed protocols
protocols = imap
!include_try /usr/share/dovecot/protocols.d/*.protocol
```

En este archivo de configuración modificamos este valor.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/conf.d/10-mail.conf *
# <doc/wiki/MailLocation.txt>
#
mail_location = maildir:~/Maildir
```

Añadimos el usuario correspondiente e instalamos lmtpd.

```
ubuntu@mail:~$ ubuntu@mail:~$ sudo adduser dovecot mail
info: Adding user `dovecot' to group `mail' ...
ubuntu@mail:~$ sudo apt install dovecot-lmtpd
```

En dovecot.conf añadimos los protocolos.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/dovecot.conf *
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

# Enable installed protocols
protocols = imap pop3 lmtp
!include_try /usr/share/dovecot/protocols.d/*.protocol
```

Accedemos a /etc/dovecot/conf.d/10-master.conf y añadimos esto.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/conf.d/10-master.conf *
#user = $default_internal_user
}

service auth-worker {
  # Auth worker process is run as root by default, so that it can access
  # /etc/shadow. If this isn't necessary, the user should be changed to
  # $default_internal_user.
  #user = root
}

service dict {
  # If dict proxy is used, mail processes should have access to its socket.
  # For example: mode=0660, group=vmail and global mail_access_groups=vmail
  unix_listener dict {
    #mode = 0600
    #user =
    #group =
  }
}

service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    mode = 0600
    user = postfix
    group = postfix
  }
}
```

Accedemos a `/etc/postfix/main.cf` y añadimos esto.

```
inet_interfaces = all
inet_protocols = all
mailbox_transport = lmtp:unix:private/dovecot-lmtp
smtpUTF8_enable = no
```

Entramos a `/etc/dovecot/conf.d/10-auth.conf` y descomentamos esto.

```
ubuntu@mail: ~
GNU nano 7.2 /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
```

Añadimos esto.

```
# 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
```

Vamos a `10-ssl.conf` y cambiamos esto.

```
ubuntu@mail: ~
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/letsencrypt/live/mail.mfgh.work.gd/fullchain.pem
ssl_key = </etc/letsencrypt/live/mail.mfgh.work.gd/privkey.pem
```

Descomentamos.

```
# Version, and LATEST matches
ssl_min_protocol = TLSv1.2
```

Vamos a /etc/ssl/openssl.cnf y comentamos esto.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/ssl/openssl.cnf *
# Policies used by the TSA examples.
tsa_policy1 = 1.2.3.4.1
tsa_policy2 = 1.2.3.4.5.6
tsa_policy3 = 1.2.3.4.5.7

# For FIPS
# Optionally include a file that is generated by the OpenSSL fipsinstall
# application. This file contains configuration data required by the OpenSSL
# fips provider. It contains a named section e.g. [fips_sect] which is
# referenced from the [provider_sect] below.
# Refer to the OpenSSL security policy for more information.
# .include fipsmodule.cnf

[openssl_init]
#providers = provider_sect
```

Vamos a /etc/dovecot/conf.d/10-master.conf y cambiamos para que tenga esto.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/conf.d/10-master.conf *
service auth {
# auth_socket_path points to this userdb socket by default. It's typically
# used by dovecot-lda, doveadm, possibly imap process, etc. Users that have
# full permissions to this socket are able to get a list of all usernames and
# get the results of everyone's userdb lookups.
#
# The default 0666 mode allows anyone to connect to the socket, but the
# userdb lookups will succeed only if the userdb returns an "uid" field that
# matches the caller process's UID. Also if caller's uid or gid matches the
# socket's uid or gid the lookup succeeds. Anything else causes a failure.
#
# To give the caller full permissions to lookup all users, set the mode to
# something else than 0666 and Dovecot lets the kernel enforce the
# permissions (e.g. 0777 allows everyone full permissions).
unix_listener auth-userdb {
#mode = 0666
#user =
#group =
}

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

(Este cambio lo hice en mi casa por eso el cambio en el fondo) Descomento esa línea para que al enviar el correo busque el nombre sin el @ en el sistema.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/conf.d/10-auth.conf *
# Username character translations before it's looked up from databases. The
# value contains series of from -> to characters. For example "#@/@" means
# that '#' and '/' characters are translated to '@'.
#auth_username_translation =

# Username formatting before it's looked up from databases. You can use
# the standard variables here, eg. %Lu would lowercase the username, %n would
# drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
# "-AT-". This translation is done after auth_username_translation changes.
auth_username_format = %n|
```

Entramos a `/etc/dovecot/conf.d/15-mailboxes.conf` y añadimos a todas las mailbox `auto = create`

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/conf.d/15-mailboxes.conf
# privileges can override the default value for entries with a custom
# value.

# NOTE: Assumes "namespace inbox" has been defined in 10-mail.conf.
namespace inbox {
  # These mailboxes are widely used and could perhaps be created automatically:
  mailbox Drafts {
    special_use = \Drafts
    auto = create
  }
  mailbox Junk {
    auto = create
    special_use = \Junk
  }
  mailbox Trash {
    auto = create
    special_use = \Trash
  }

  # For \Sent mailboxes there are two widely used names. We'll mark both of
  # them as \Sent. User typically deletes one of them if duplicates are created.
  mailbox Sent {
    auto = create
    special_use = \Sent
  }
  mailbox "Sent Messages" {
    auto = create
    special_use = \Sent
  }
}
```

Reiniciamos dovecot.

```
ubuntu@mail:~$ sudo systemctl restart postfix dovecot
ubuntu@mail:~$
```

Para la prueba, vamos a darle una contraseña a Ubuntu.

```
ubuntu@mail:~$ sudo passwd ubuntu
New password:
Retype new password:
passwd: password updated successfully
ubuntu@mail:~$
```

Instalamos thunderbird en la máquina Windows, y vemos que funciona.

Nombre completo  
ubuntu

Dirección de correo electrónico  
ubuntu@mfigh.work.gd

Contraseña  
••••••••

☒ Recordar contraseña

✓ Configuración encontrada probando nombres de servidor comunes.

Configuraciones disponibles

☒ IMAP  
Mantener sus carpetas y correos electrónicos sincronizados en su servidor

Entrante IMAP SSL/TLS  
mail.mfigh.work.gd

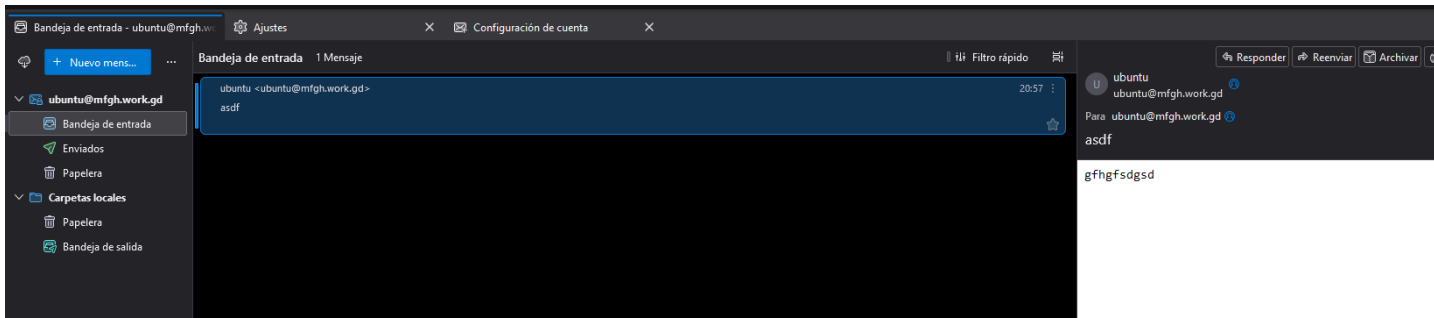
Saliente SMTP STARTTLS  
mail.mfigh.work.gd

Nombre de usuario  
ubuntu

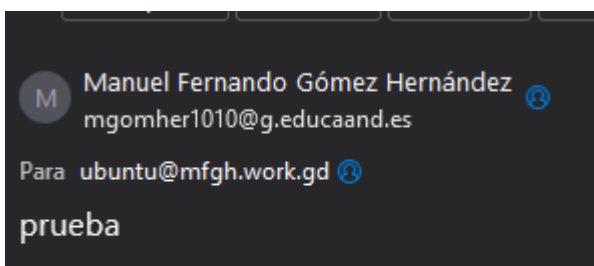
☐ POP3  
Mantener sus carpetas y correos electrónicos en su equipo

Configurar manualmente Cancelar Hecho

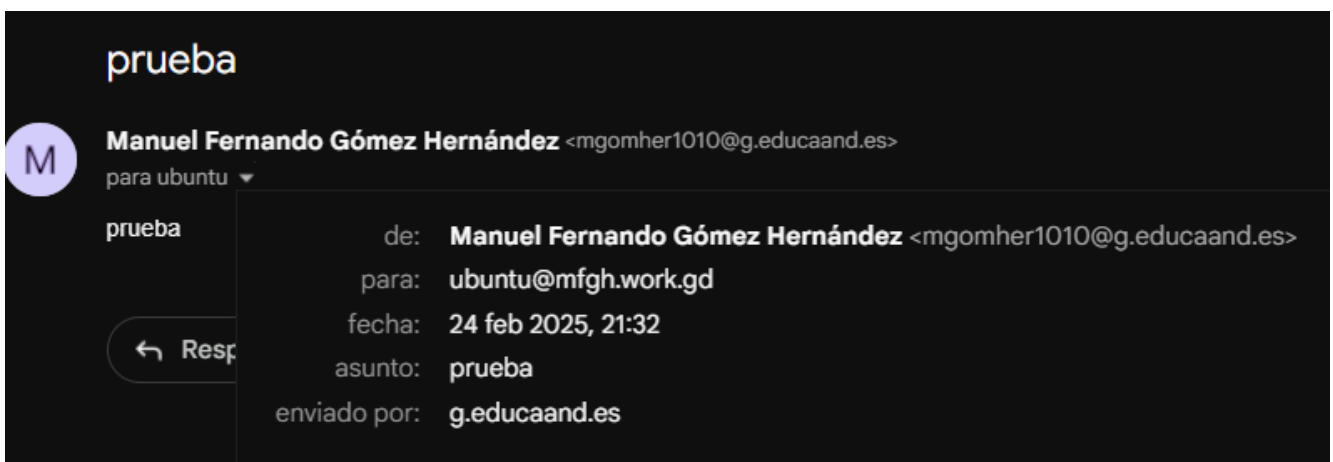
Vamos a enviar un email de prueba.



Ha funcionado, ahora, desde mi correo administrativo, voy a enviar un correo.



prueba



Creo otro usuario para las pruebas.

```
Last login: Mon Feb 24 19:41:09 2025
ubuntu@mail:~$ sudo adduser manu
info: Adding user `manu'...
```

Nombre completo

manu

Dirección de correo electrónico

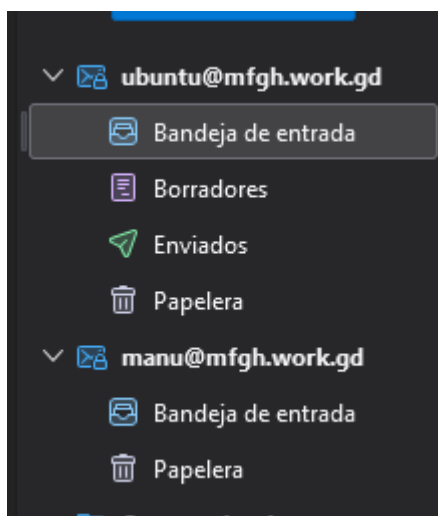
manu@mfggh.work.gd

Contraseña

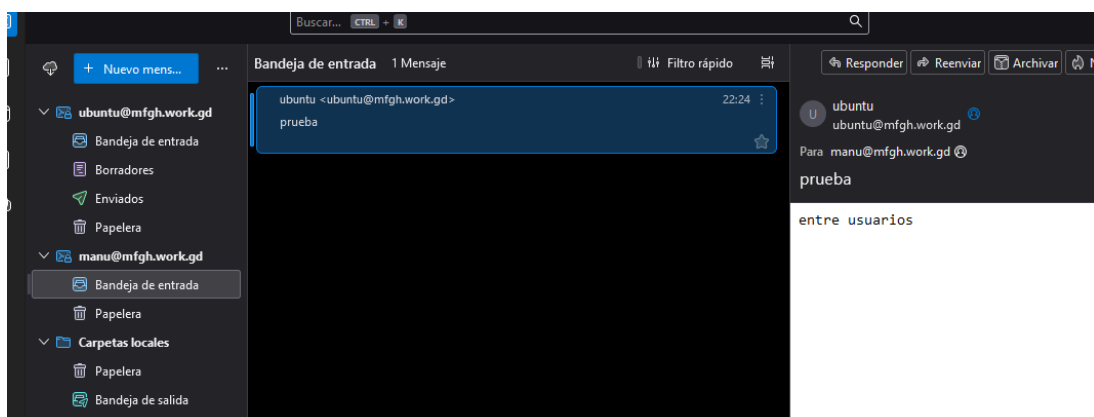
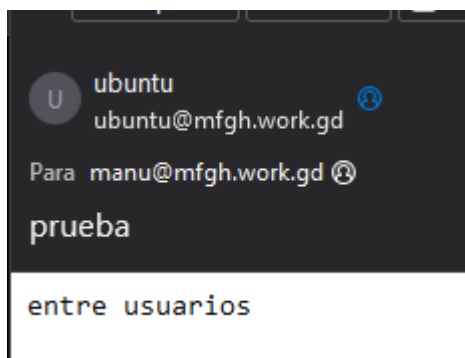
••••••••

☒ Recordar contraseña

Tenemos las dos bandejas de entrada.



Envío correo de prueba.





### Paso 3:

Creación de cuentas de correo virtuales utilizando MariaDB y PostfixAdmin. Configura tu dominio de correo xxx.line.pm, crea varios usuarios virtuales y prueba el envío y recepción de correo. Para enviar correos y evitar el bloqueo del puerto 25, puede utilizar el cliente de correo desde una máquina Windows Server en AWS.

```
Last login: Mon Feb 24 21:20:19 2025 from 213.94.3.8
ubuntu@mail:~$ sudo apt install mariadb-server mariadb-client
Reading package lists... Done
```

```
ubuntu@mail:~$ sudo systemctl status mariadb
● mariadb.service - MariaDB 10.11.8 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-02-25 21:50:23 UTC; 25s ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Main PID: 2181 (mariabdb)
   Status: "Taking your SQL requests now..."
     Tasks: 12 (Limit: 15435)
   Memory: 78.8M (peak: 81.7M)
      CPU: 333ms
   CGroup: /system.slice/mariadb.service
           └─2181 /usr/sbin/mariabdb
```

Hago la instalación segura.

```
ubuntu@mail:~$ sudo 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 [Y/n] n
... skipping.

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

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

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? [Y/n]
... 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? [Y/n]
... 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 and access to it? [Y/n] |
```

Descargamos postfixadmin.

```

wget: unable to resolve host address 'github'
ubuntu@mail:~$ wget https://github.com/postfixadmin/postfixadmin/archive/postfixadmin-3.3.11.tar.gz
--2025-02-25 21:54:52-- https://github.com/postfixadmin/postfixadmin/archive/postfixadmin-3.3.11.tar.gz
Resolving github.com (github.com)... 140.82.113.4
Connecting to github.com (github.com)|140.82.113.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/postfixadmin/postfixadmin/tar.gz/refs/tags/postfixadmin-3.3.11 [following]
--2025-02-25 21:54:52-- https://codeload.github.com/postfixadmin/postfixadmin/tar.gz/refs/tags/postfixadmin-3.3.11
Resolving codeload.github.com (codeload.github.com)... 140.82.113.10
Connecting to codeload.github.com (codeload.github.com)|140.82.113.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: 'postfixadmin-3.3.11.tar.gz'

postfixadmin-3.3.11.tar.gz      [ <=> ] 1.78M 11.2MB/s  in 0.2s

2025-02-25 21:54:52 (11.2 MB/s) - 'postfixadmin-3.3.11.tar.gz' saved [1869783]

ubuntu@mail:~$ sudo mkdir -p /var/www/
ubuntu@mail:~$ sudo tar xvf postfixadmin-3.3.11.tar.gz -C /var/www/
postfixadmin-postfixadmin-3.3.11/

```

Nos aseguramos de cambiarle el nombre.

```

ubuntu@mail:~$ sudo mv /var/www/postfixadmin-postfixadmin-3.3.11/ /var/www/postfixadmin

```

Necesitamos un directorio templates\_c.

```

ubuntu@mail:~$ sudo mkdir -p /var/www/postfixadmin/templates_c
ubuntu@mail:~$ sudo apt install acl
Reading package lists... Done

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@mail:~$ sudo setfacl -R -m u:www-data:rwX /var/www/postfixadmin/templates_c/
ubuntu@mail:~$ sudo setfacl -R -m u:www-data:rx /etc/letsencrypt/live/ /etc/letsencrypt/archive/
ubuntu@mail:~$

```

Vamos a crear una base de datos usuario para PostFixAdmin.

```

ubuntu@mail:~$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 39
Server version: 10.11.8-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

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

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

MariaDB [(none)]> CREATE DATABASE postfixadmin;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> CREATE USER 'postfixadmin'@'localhost' IDENTIFIED BY 'alumno2425m';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON postfixadmin.* TO 'postfixadmin'@'localhost';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> |

```

El archivo de configuración predeterminado de PostfixAdmin es config.inc.php. Necesitamos crear un fichero config.local.php y agregar configuraciones personalizadas.

```
ubuntu@mail: ~
GNU nano 7.2 /var/www/postfixadmin/config.local.php *
<?php
$CONF['configured'] = true;
$CONF['database_type'] = 'mysqli';
$CONF['database_host'] = 'localhost';
$CONF['database_port'] = '3306';
$CONF['database_user'] = 'postfixadmin';
$CONF['database_password'] = 'alumno2425m';
$CONF['database_name'] = 'postfixadmin';
$CONF['encrypt'] = 'dovecot:ARGON2I';

$CONF['dovecotpw'] = "/usr/bin/doveadm pw -r 5";
if (@file_exists('/usr/bin/doveadm')) {
    $CONF['dovecotpw'] = "/usr/bin/doveadm pw -r 5"; # Debian
}
|
```

```
ubuntu@mail:~$ sudo doveadm pw -l
SHA1 SHA512 SCRAM-SHA-256 BLF-CRYPT PLAIN HMAC-MD5 OTP SHA512 SHA DES-CRYPT CRYPT SSHA MD5-CRYPT PLAIN-MD4 PLAIN-MD5 SC
RAM-SHA-1 SHA512-CRYPT CLEAR CLEARTXT ARGON2I ARGON2ID SSHA256 MD5 PBKDF2 SHA256 CRAM-MD5 PLAIN-TRUNC SHA256-CRYPT SMD5
DIGEST-MD5 LDAP-MD5
ubuntu@mail:~$
```

Creamos un sitio virtual en apache y lo activamos.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/apache2/sites-available/postfixadmin.conf *
<VirtualHost *:80>
    ServerName mfggh.work.gd
    DocumentRoot /var/www/postfixadmin/public

    ErrorLog ${APACHE_LOG_DIR}/postfixadmin_error.log
    CustomLog ${APACHE_LOG_DIR}/postfixadmin_access.log combined

    <Directory />
        Options FollowSymLinks
        AllowOverride All
    </Directory>

    <Directory /var/www/postfixadmin/>
        Options FollowSymLinks MultiViews
        AllowOverride All
        Order allow,deny
        Allow from all
    </Directory>
</VirtualHost>
```

```
ubuntu@mail:~$ sudo a2ensite postfixadmin.conf
Enabling site postfixadmin.
To activate the new configuration, you need to run:
systemctl reload apache2
ubuntu@mail:~$ sudo systemctl reload apache2
ubuntu@mail:~$
```

Descargamos todo lo de php en la versión 8.3

```
ubuntu@mail:~$ sudo apt install php8.3-fpm php8.3-imap php8.3-mbstring php8.3-mysql php8.3-curl php8.3-zip php8.3-xml ph
p8.3-bz2 php8.3-intl php8.3-gmp php8.3-redis
```

También la librería de apache.

```
ubuntu@mail:~$ sudo apt install libapache2-mod-php
```

Añadimos lo siguiente en dovecot.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/conf.d/10-master.conf
#process_limit = 1024
}

service submission {
  # Max. number of SMTP Submission processes (connections)
  #process_limit = 1024
}

service auth {
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
  }
}

# Auth process is run as this user.
#user = $default_internal_user

service auth-worker {
  # Auth worker process is run as root by default, so that it can access
  # /etc/shadow. If this isn't necessary, the user should be changed to
  # $default_internal_user.
  #user = root
}

service dict {
  # If dict proxy is used, mail processes should have access to its socket.
  # For example: mode=0660, group=vmail and global mail_access_groups=vmail
  unix_listener dict {
    #mode = 0660
    #user =
    #group =
  }
}

service stats {
  unix_listener stats-reader {
    user = www-data
    group = www-data
    mode = 0660
  }
}

unix_listener stats-writer {
  user = www-data
  group = www-data
  mode = 0660
}
}
```

Añadimos a dovecot al servidor web y le damos permisos.

```
ubuntu@mail:~$ sudo gpasswd -a www-data dovecot
Adding user www-data to group dovecot
```

```
ubuntu@mail:~$ sudo systemctl restart dovecot
ubuntu@mail:~$ sudo setfacl -R -m u:www-data:rwX /var/run/dovecot/stats-reader /var/run/dovecot/stats-writer
```

Ahora accedemos al setup.php.

Configure and Setup Postfixadmin

This page helps you setup PostfixAdmin. For further help see the [documentation](#).

**Warning: connection not secure, switch to https if possible**

- TODO You need to have a setup\_password hash configured in a `config.local.php` file
- TODO You need to authenticate using the setup\_password before you can perform some environment and hosting checks.

One you have logged in with the setup\_password, this page will ...

- run some simple hosting/environment checks which may help identify problems with your environment
- create/update your database of choice,
- allow you to list / add super user accounts

For a new installation, you must generate a 'setup\_password' to go into your `config.local.php` file.

You can use the form below, or run something like the following in a shell - `php -r 'echo password_hash("password", PASSWORD_DEFAULT);'`

**Generate setup\_password**

Setup password

Setup password (again)

[Generate setup\\_password hash](#)

**Hosting Environment Check**

Hosting Environment warnings found. [Login to see details.](#)

**Database Update**

Everything seems fine... attempting to create/update database structure

Updating database:

Introduzco mi contraseña (alumno2425m) y me genera un Hash, y esa línea que nos da vamos a añadirla a config.local.php.

### Generate setup\_password

Setup password

Setup password (again)

[Generate setup\\_password hash](#)

If you want to use the password you entered as setup password, edit config.inc.php or config.local.php and set

```
$CONF['setup_password'] = '$2y$10$8239Bj4yPKryKh7k7d346.YJ6pQz2sPCzMUAhUPcxGLIn/7jzgkpw';
```

After adding, refresh this page and log in using it.

```
GNU nano 7.2 /var/www/postfixadmin/config.local.php *
<?php
$CONF['configured'] = true;
$CONF['database_type'] = 'mysql';
$CONF['database_host'] = 'localhost';
$CONF['database_port'] = '3306';
$CONF['database_user'] = 'postfixadmin';
$CONF['database_password'] = 'alumno2425m';
$CONF['database_name'] = 'postfixadmin';
$CONF['encrypt'] = 'dovecot:ARGON2I';

$CONF['dovecotpw'] = "/usr/bin/doveadm pw -r 5";
if (@file_exists('/usr/bin/doveadm')) {
    $CONF['dovecotpw'] = "/usr/bin/doveadm pw -r 5"; # Debian
}
$CONF['setup_password'] = '$2y$10$8239Bj4yPKryKh7k7d346.YJ6pQz2sPCzMUAhUPcxGLIn/7jzgkpw';
```

Ahora recargamos la página y añadimos un super admin.

### Warnings

- Database - PostgreSQL (pdo\_pgsql) extension not found
- Database support - SQLite (pdo\_sqlite) extension not found

### Database Update

Everything seems fine... attempting to create/update database structure

Database is up to date: 1844/0

Admin addition failed; check field error messages or server logs.

### Add Superadmin Account

Setup password

Administrador

Administrador no es un e-mail válido!

Contraseña

Contraseña (repetir)

[Add superadmin](#)

### Super admins

The following 'super-admin' accounts have already been added to the database.

- ubuntu@mfigh.work.gd

### Add Superadmin Account

Setup password

Administrador

Contraseña

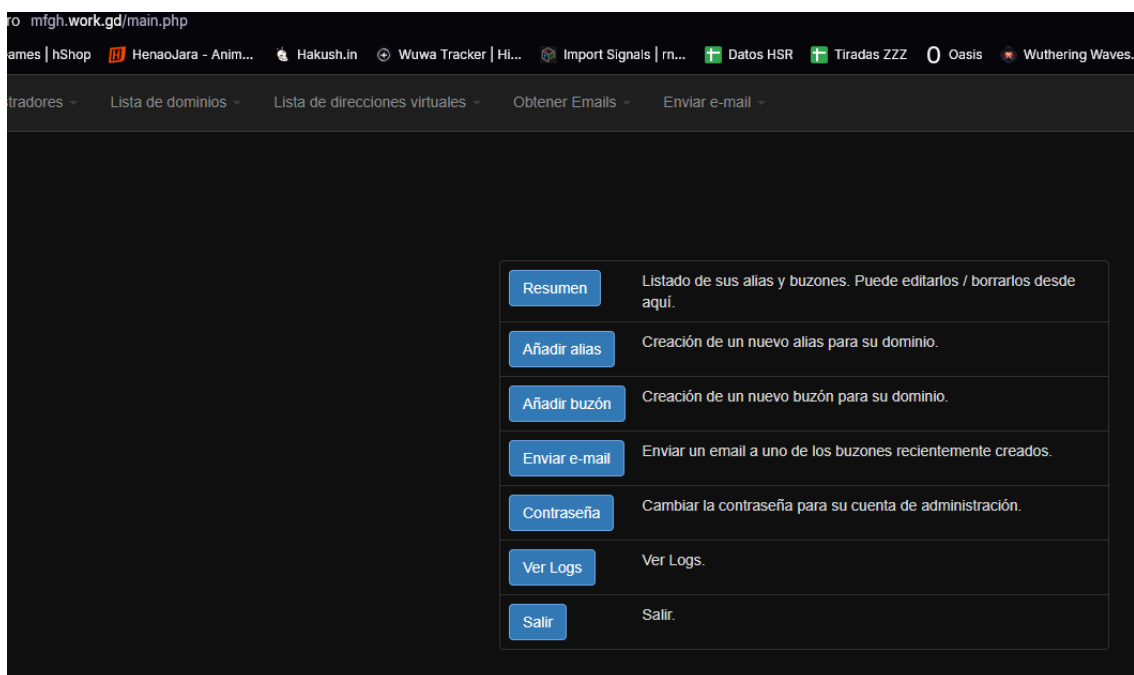
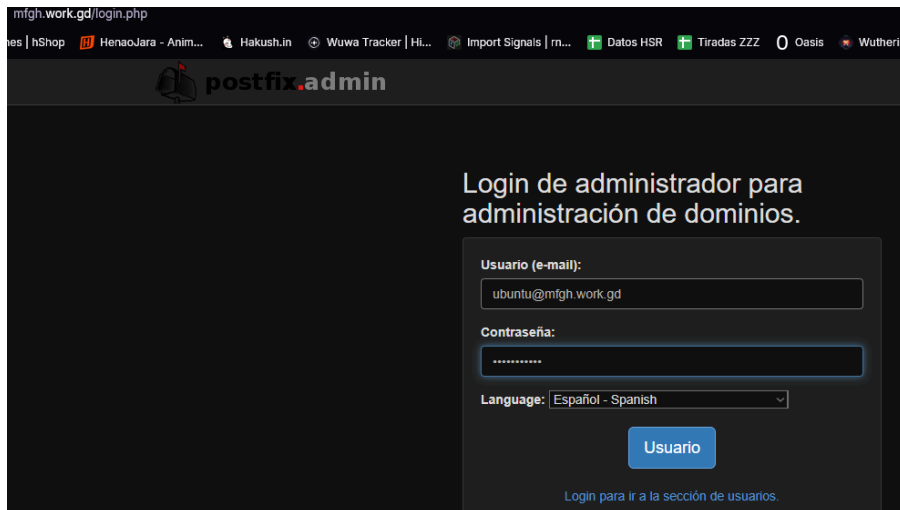
Contraseña (repetir)

[Añadir administrador](#)

¡El administrador ha sido añadido! (ubuntu@mfigh.work.gd)

You are done with your basic setup. You can now login to PostfixAdmin using the account you just created.

Ahora podemos ir a login.php y logear.



Ahora vamos a main.cf y añadimos esto (empezando desde virtual\_mailbox\_domains).

```

GNU nano 7.2 /etc/postfix/main.cf *
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4
mailbox_transport = lmtp:unix:private/dovecot-lmtp
smtpUTF8_enable = no

virtual_mailbox_domains = proxy:mysql:/etc/postfix/sql/mysql_virtual_domains_maps.cf

virtual_mailbox_maps =
    proxy:mysql:/etc/postfix/sql/mysql_virtual_mailbox_maps.cf,
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_mailbox_maps.cf

virtual_alias_maps =
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_maps.cf,
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_maps.cf,
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_catchall_maps.cf
  
```

```

ubuntu@mail:~$ sudo apt install postfix-mysql
Reading package lists... Done
  
```

De forma predeterminada, Postfix envía correos electrónicos solo a usuarios con una cuenta Unix local, así que debemos configurar Postfix para que utilice dominios de buzones virtuales.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/postfix/sql/mysql_virtual_domains_maps.cf *
user = postfixadmin
password = alumno2425m
hosts = localhost
dbname = postfixadmin
query = SELECT domain FROM domain WHERE domain='%s' AND active = '1'

ubuntu@mail: ~
GNU nano 7.2 /etc/postfix/sql/mysql_virtual_mailbox_maps.cf *
user = postfixadmin
password = alumno2425m
hosts = localhost
dbname = postfix admin
query = SELECT maildir FROM mailbox WHERE username='s' AND active = '1'|

ubuntu@mail: ~
GNU nano 7.2 /etc/postfix/sql/mysql_virtual_alias_domain_mailbox_maps.cf *
user = postfixadmin
password = alumno2425m
hosts = localhost
dbname = postfixadmin
query = SELECT maildir FROM mailbox,alias_domain WHERE alias_domain.alias_domain = '%d' and mailbox.username = CONCAT('

ubuntu@mail: ~
GNU nano 7.2 /etc/postfix/sql/mysql_virtual_alias_maps.cf *
user = postfixadmin
password = alumno2425m
hosts = localhost
dbname = postfixadmin
query = SELECT goto FROM alias WHERE address='%s' AND active = '1'

ubuntu@mail: ~
GNU nano 7.2 /etc/postfix/sql/mysql_virtual_alias_domain_maps.cf *
user = postfixadmin
password = alumno2425m|
hosts = localhost
dbname = postfixadmin
query = SELECT goto FROM alias,alias_domain WHERE alias_domain.alias_domain = '%d' and alias.address = CONCAT('%u', '@'

ubuntu@mail: ~
GNU nano 7.2 /etc/postfix/sql/mysql_virtual_alias_domain_catchall_maps.cf *
user = postfixadmin
password = alumno2425m|
hosts = localhost
dbname = postfixadmin
query = SELECT goto FROM alias,alias_domain WHERE alias_domain.alias_domain = '%d' and alias.address = CONCAT('@', alia
```

Dado que las contraseñas de la base de datos se almacenan como texto sin formato, solo los usuarios postfix y root pueden leerlos lo que se hace ejecutando los siguientes comandos:

```
ubuntu@mail:~$ sudo chmod 0640 /etc/postfix/sql/*
sudo setfacl -R -m u:postfix:rx /etc/postfix/sql/
```



El mydestination contiene una lista de nombres de dominio que recibirán correos electrónicos entregados a cuentas Unix locales. En la parte 1, agregamos el nombre de dominio de apex a mydestination

A continuación, debemos cambiar el valor del mydestination en Postfix.

```
ubuntu@mail:~$ postconf mydestination
mydestination = mail.mfgh.work.gd, localhost.mfgh.work.gd, localhost, mfgh.work.gd, $myhostname, localhost.$mydomain
ubuntu@mail:~$
```

Volvamos a main.cf a añadir lo siguiente.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/postfix/main.cf *

virtual_mailbox_domains = proxy:mysql:/etc/postfix/sql/mysql_virtual_domains_maps.cf

virtual_mailbox_maps =
    proxy:mysql:/etc/postfix/sql/mysql_virtual_mailbox_maps.cf,
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_mailbox_maps.cf

virtual_alias_maps =
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_maps.cf,
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_maps.cf,
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_catchall_maps.cf

virtual_transport = lmtp:unix:private/dovecot-lmtp

virtual_mailbox_base = /var/vmail
virtual_minimum_uid = 2000
virtual_uid_maps = static:2000
virtual_gid_maps = static:2000
```

Reseteamos y creamos al usuario vmail y creamos, dando permisos, la carpeta /var/mail:

```
ubuntu@mail:~$ sudo systemctl restart postfix
ubuntu@mail:~$ sudo adduser vmail --system --group --uid 2000 --disabled-login --no-create-home
info: Adding system user 'vmail' (UID 2000) ...
info: Adding new group 'vmail' (GID 2000) ...
info: Adding new user 'vmail' (UID 2000) with group 'vmail' ...
useradd warning: vmail's uid 2000 is greater than SYS_UID_MAX 999
info: Not creating '/nonexistent'.
ubuntu@mail:~$ sudo mkdir /var/vmail/
ubuntu@mail:~$ sudo chown vmail:vmail /var/vmail -R
ubuntu@mail:~$
```

```
ubuntu@mail:~$ sudo apt install dovecot-mysql
Reading package lists... Done
```

Ahora vamos a 10-mail.conf a añadir lo siguiente.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/conf.d/10-mail.conf *

# mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location = maildir:~/Maildir
mail_home = /var/vmail/%d/%n/
```



Ahora a 10-auth.conf y ajustamos lo siguiente.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/conf.d/10-auth.conf *
# first.
#auth_realms =

# Default realm/domain to use if none was specified. This is used for both
# SASL realms and appending @domain to username in plaintext logins.
auth_default_realm = example.com

# List of allowed characters in username. If the user-given username contains
# a character not listed in here, the login automatically fails. This is just
# an extra check to make sure user can't exploit any potential quote escaping
# vulnerabilities with SQL/LDAP databases. If you want to allow all characters,
# set this value to empty.
#auth_username_chars = abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567890.-_@

# Username character translations before it's looked up from databases. The
# value contains series of from -> to characters. For example "#@/@" means
# that '#' and '/' characters are translated to '@'.
#auth_username_translation =

# Username formatting before it's looked up from databases. You can use
# the standard variables here, eg. %Lu would lowercase the username, %n would
# drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
# "-AT-". This translation is done after auth_username_translation changes.
auth_username_format = %u
```

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/conf.d/10-auth.conf *
# 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

##
## Password and user databases
##

# Password database is used to verify user's password (and nothing more).
# You can have multiple passdbs and userdbs. This is useful if you want to
# allow both system users (/etc/passwd) and virtual users to login without
# duplicating the system users into virtual database.
# <doc/wiki>PasswordDatabase.txt>
#
# User database specifies where mails are located and what user/group IDs
# own them. For single-UID configuration use "static" userdb.
# <doc/wiki/UserDatabase.txt>
#!include auth-deny.conf.ext
#!include auth-master.conf.ext

#!include auth-system.conf.ext
!include auth-sql.conf.ext
#!include auth-ldap.conf.ext
#!include auth-passwdfile.conf.ext
#!include auth-checkpassword.conf.ext
#!include auth-static.conf.ext
```

Ahora vamos a dovecot-sql.conf.ext y añadimos lo siguiente al final.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/dovecot/dovecot-sql.conf.ext *
# None of these are strictly required. If you use a single UID and GID, and
# home or mail directory fits to a template string, you could use userdb static
# instead. For a list of all fields that can be returned, see
# http://wiki2.dovecot.org/UserDatabase/ExtraFields
#
# Examples:
# user_query = SELECT home, uid, gid FROM users WHERE userid = '%u'
# user_query = SELECT dir AS home, user AS uid, group AS gid FROM users where userid = '%u'
# user_query = SELECT home, 501 AS uid, 501 AS gid FROM users WHERE userid = '%u'
#
#user_query = \
# SELECT home, uid, gid \
# FROM users WHERE username = '%n' AND domain = '%d'

# If you wish to avoid two SQL lookups (passdb + userdb), you can use
# userdb prefetch instead of userdb sql in dovecot.conf. In that case you'll
# also have to return userdb fields in password_query prefixed with "userdb_"
# string. For example:
#password_query = \
# SELECT userid AS user, password, \
# home AS userdb_home, uid AS userdb_uid, gid AS userdb_gid \
# FROM users WHERE userid = '%u'

# Query to get a list of all usernames.
#iterate_query = SELECT username AS user FROM users
driver = mysql

connect = host=localhost dbname=postfixadmin user=postfixadmin password=alumno2425m

default_pass_scheme = ARGON2I

password_query = SELECT username AS user,password FROM mailbox WHERE username = '%u' AND active='1'

user_query = SELECT maildir, 2000 AS uid, 2000 AS gid FROM mailbox WHERE username = '%u' AND active='1'

iterate_query = SELECT username AS user FROM mailbox
```

Con esto hecho, ya podemos volver al dominio. Y vamos a añadir un nuevo dominio.

### Añadir nuevo dominio

<b>Dominio</b>	<input type="text" value="mfgh.work.gd"/>
<b>Descripción</b>	<input type="text" value="Correo de Manuel Gómez"/>
<b>Alias</b>	<input type="text" value="10"/> <small>-1 = deshabilitar   0 = ilimitado</small>
<b>Buzones</b>	<input type="text" value="10"/> <small>-1 = deshabilitar   0 = ilimitado</small>
<b>El servidor de correo es backup MX</b>	<input type="checkbox"/>
<b>Activo</b>	<input checked="" type="checkbox"/>
<b>Añadir alias por defecto</b>	<input checked="" type="checkbox"/>
<b>Pass expires</b>	<input type="text" value="365"/> <small>Date when password will expire</small>

Añadir dominio

Y también un usuario para el dominio.

### Crear un nuevo buzón para su dominio.

<b>Usuario</b>	<input type="text" value="manufgh"/>
	<input type="text" value="mfgh.work.gd"/>
<b>Contraseña</b>	<input type="password" value="....."/> <small>Contraseña para POP3/IMAP</small>
<b>Contraseña (repetir)</b>	<input type="password" value="....."/>
<b>Nombre</b>	<input type="text" value="Manuel gomez"/> <small>Nombre completo</small>
<b>Cuota</b>	<input type="text"/> <small>MB</small>
<b>Activo</b>	<input checked="" type="checkbox"/>
<b>Enviar correo bienvenida</b>	<input checked="" type="checkbox"/>
<b>Other e-mail</b>	<input type="text"/> <small>Used if the password is forgotten</small>

Añadir buzón

Iniciamos sesión con el mismo en Thunderbird, y configuramos los puertos manualmente.

Nombre completo  
manufgh

Dirección de correo electrónico  
manufgh@mfigh.work.gd

Contraseña  
••••••••

☒ Recordar contraseña

✓ Se encontraron las siguientes configuraciones al sondear el servidor indicado:

**Configuración manual**

**SERVIDOR ENTRANTE**

Protocolo: IMAP

Nombre del servidor: mail.mfigh.work.gd

Puerto: 143

Seguridad de la conexión: STARTTLS

Método de autenticación: Contraseña normal

Nombre de usuario: manufgh

**SERVIDOR SALIENTE**

Nombre del servidor: mail.mfigh.work.gd

Puerto: 587

Seguridad de la conexión: STARTTLS

Método de autenticación: Contraseña normal

Nombre de usuario: manufgh

[Configuración avanzada](#)

Volver a comprobar Cancelar Hecho

Y listo.

✓ Cuenta creada correctamente

Ahora puede usar esta cuenta con Thunderbird.  
Puede mejorar la experiencia conectando servicios relacionados y configurando los ajustes de cuenta avanzados.

manufgh manufgh@mfigh.work.gd IMAP

Configuración de la cuenta

Cifrado de extremo a extremo Añadir una firma

Descargar diccionarios

Conectar sus servicios vinculados

Buscando calendarios...

Conectarse a una libreta de direcciones CardDAV

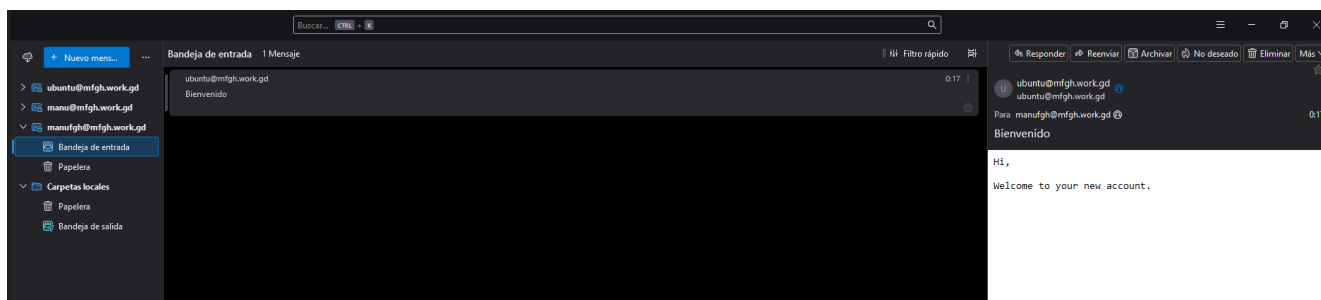
Conectarse a una libreta de direcciones LDAP

Conectarse a un calendario remoto

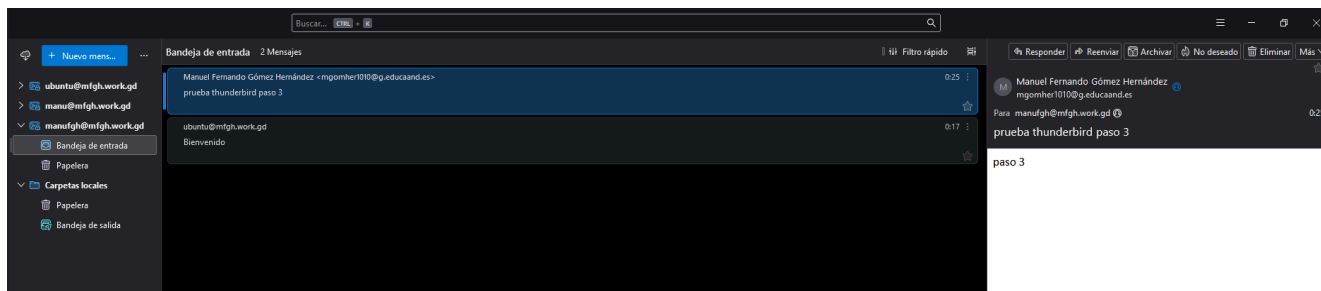
Finalizar

¿No está seguro de qué seleccionar?  
[Documentación de configuración](#) · [Foro de asistencia](#) · [Política de privacidad](#)

También ha llegado el correo de bienvenida.



El correo desde mi cuenta de educaand ha funcionado.



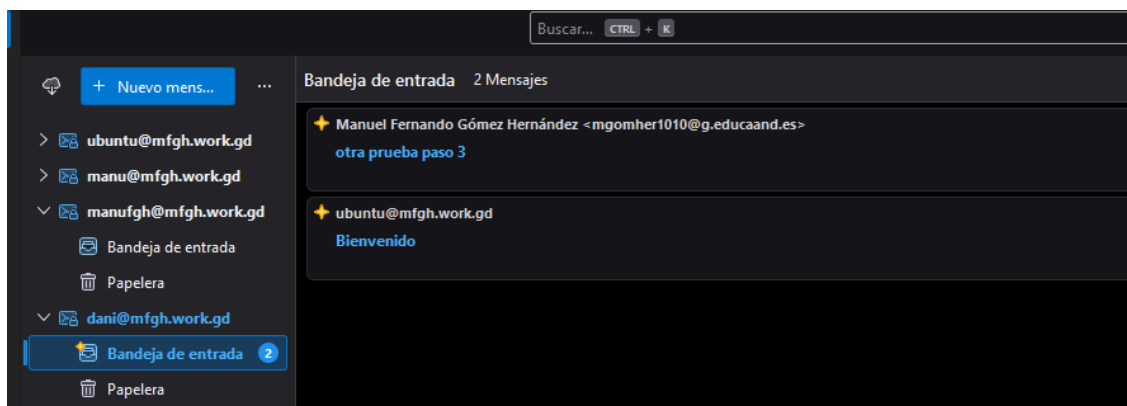
Probando con más usuarios.

:: Alias						
Alias	Destino	Última Modificación	Activo			
abuse@mfgh.work.gd	abuse@change-this-to-your.domain.tld	2025-02-25	SI	editar	borrar	
hostmaster@mfgh.work.gd	hostmaster@change-this-to-your.domain.tld	2025-02-25	SI	editar	borrar	
postmaster@mfgh.work.gd	postmaster@change-this-to-your.domain.tld	2025-02-25	SI	editar	borrar	
webmaster@mfgh.work.gd	webmaster@change-this-to-your.domain.tld	2025-02-25	SI	editar	borrar	
				Añadir alias	Download this list as CSV file	

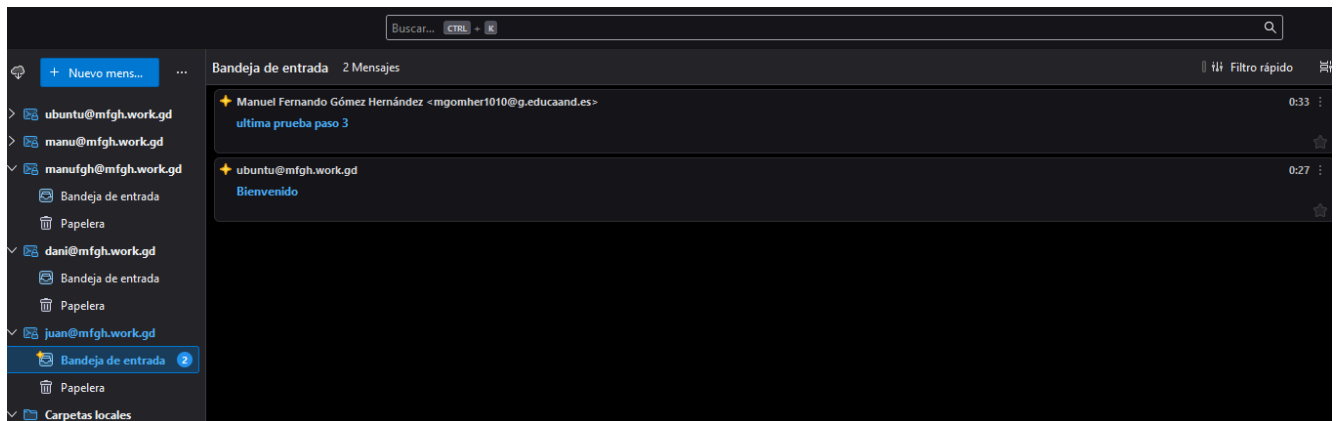
  

:: Buzones						
E-mail	Destino	Nombre	Última Modificación	Activo		
dani@mfgh.work.gd	Mailbox	dani	2025-02-25 23:27:35	SI	Alias	editar borrar
juan@mfgh.work.gd	Mailbox	juan	2025-02-25 23:27:19	SI	Alias	editar borrar
manufgh@mfgh.work.gd	Mailbox	Manuel gomez	2025-02-25 23:17:37	SI	Alias	editar borrar
				Añadir buzón	Download this list as CSV file	

Con el usuario dani funciona.



Y con el usuario Juan también funciona.

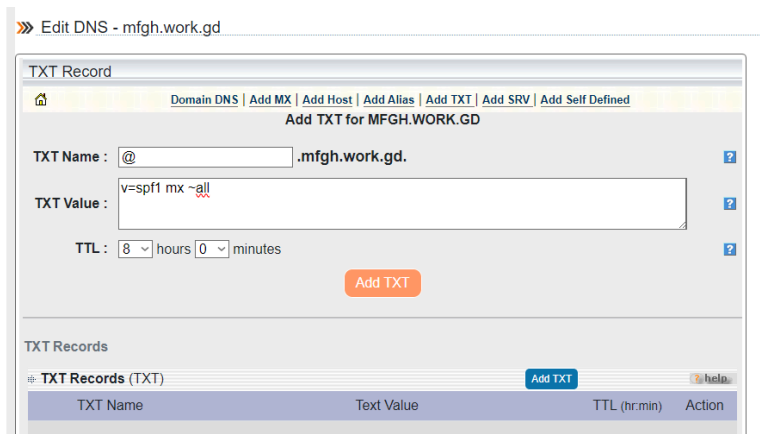


## Paso 4:

Para luchar contra el spam y tener un servidor de correo confiable para el mundo exterior, es necesaria la instalación de varias técnicas: SPF y DKIM. Configura estas mejoras al correo y verifica su correcto funcionamiento mediante el correcto PASS de los controles en los códigos fuentes de los correos electrónicos y, mediante el uso de herramientas de chequeo externas como las que te indican en el tutorial de referencia. Se debe configurar adecuadamente DNSexit capturando pantallas del mismo.

La guía que estamos utilizando también implementa la técnica de autenticación de correo DMARC. En esta práctica sólo se va a pedir su implementación de manera opcional para **subir 1 punto** la calificación final de la misma.

Vamos a empezar por crear un nuevo registro TXT en el dominio.



Vemos que se ha creado exitosamente.

```
ubuntu@mail:~$ dig mfgh.work.gd txt
; <<>> DiG 9.18.30-ubuntu0.24.04.2-Ubuntu <<>> mfgh.work.gd txt
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 30531
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 65494
;; QUESTION SECTION:
;mfgh.work.gd.                IN      TXT
;; AUTHORITY SECTION:
mfgh.work.gd.                1200    IN      SOA     ns1.dnsexit.com. admin.netdorm.com. 2000060701 86000 180000 1814400 1200
;; Query time: 1631 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Feb 25 23:41:28 UTC 2025
;; MSG SIZE rcvd: 106
```

Vamos a instalar lo siguiente.

```
ubuntu@mail:~$ sudo apt install postfix-policyd-spf-python
Reading package lists... Done
```

Añadimos esta línea al final de master.cf

```

GNU nano 7.2 /etc/postfix/master.cf *
#
uucp    unix    -    n    n    -    -    pipe
flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
#
# Other external delivery methods.
#
# ifmail    unix    -    n    n    -    -    pipe
# flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
# bsmtp     unix    -    n    n    -    -    pipe
# flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
# scalemail-backend unix - n n - 2 pipe
# flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${user} ${extension}
# mailman   unix    -    n    n    -    -    pipe
# flags=FRX user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py ${nexthop} ${user}
submission inet    n    -    y    -    -    smtpd
-o syslog_name=postfix/submission
-o smtpd_tls_security_level=encrypt
-o smtpd_tls_wrappermode=no
-o smtpd_sasl_auth_enable=yes
-o smtpd_relay_restrictions=permit_sasl_authenticated,reject
-o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject
-o smtpd_sasl_type=dovecot
-o smtpd_sasl_path=private/auth
policyd-spf unix    -    n    n    -    0    spawn
user=policyd-spf argv=/usr/bin/policyd-spf

```

Ahora en main.cf

```

GNU nano 7.2 /etc/postfix/main.cf *
virtual_alias_maps =
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_maps.cf,
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_maps.cf,
    proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_catchall_maps.cf

virtual_transport = lmtp:unix:private/dovecot-lmtp

virtual_mailbox_base = /var/vmail
virtual_minimum_uid = 2000
virtual_uid_maps = static:2000
virtual_gid_maps = static:2000

policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_unauth_destination,
    check_policy_service unix:private/policyd-spf

```

```
ubuntu@mail:~$ sudo systemctl restart postfix
ubuntu@mail:~$
```

Ahora instalaremos las tools de opendkim.

```
ubuntu@mail:~$ sudo apt install opendkim opendkim-tools
Reading package lists... Done
```

Añadimos al usuario postfix al grupo que se ha debido crear.

```
ubuntu@mail:~$ sudo gpasswd -a postfix opendkim
Adding user postfix to group opendkim
ubuntu@mail:~$
```

Ahora entramos a sudo /etc/opendkim.conf y lo editamos para que esté así.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/opendkim.conf
# This is a basic configuration for signing and verifying. It can easily be
# adapted to suit a basic installation. See opendkim.conf(5) and
# /usr/share/doc/opendkim/examples/opendkim.conf.sample for complete
# documentation of available configuration parameters.

Syslog          yes
LogWhy          yes
SyslogSuccess   yes
#LogWhy         no

# Common signing and verification parameters. In Debian, the "From" header is
# oversigned, because it is often the identity key used by reputation systems
# and thus somewhat security sensitive.
Canonicalization relaxed/simple
Mode            sv
SubDomains      no
OversignHeaders From

AutoRestart     yes
AutoRestartRate 10/1M
Background      yes
DNSTimeout      5
SignatureAlgorithm rsa-sha256
# Signing domain, selector, and key (required). For example, perform signing
```

```
ubuntu@mail: ~
GNU nano 7.2 /etc/opendkim.conf *
OversignHeaders From

AutoRestart     yes
AutoRestartRate 10/1M
Background      yes
DNSTimeout      5
SignatureAlgorithm rsa-sha256
# Signing domain, selector, and key (required). For example, perform signing
# for domain "example.com" with selector "2020" (2020._domainkey.example.com),
# using the private key stored in /etc/dkimkeys/example.private. More granular
# setup options can be found in /usr/share/doc/opendkim/README.opendkim.
#Domain         example.com
#Selector       2020
#KeyFile         /etc/dkimkeys/example.private

# In Debian, opendkim runs as user "opendkim". A umask of 007 is required when
# using a local socket with MTAs that access the socket as a non-privileged
# user (for example, Postfix). You may need to add user "postfix" to group
# "opendkim" in that case.
UserID          opendkim
UMask           007

# Map domains in From addresses to keys used to sign messages
KeyTable         refile:/etc/opendkim/key.table
SigningTable     refile:/etc/opendkim/signing.table

# Hosts to ignore when verifying signatures
ExternalIgnoreList /etc/opendkim/trusted.hosts

# A set of internal hosts whose mail should be signed
InternalHosts    /etc/opendkim/trusted.hosts
```

Creamos la carpeta de las keys.

```
ubuntu@mail:~$ sudo mkdir /etc/opendkim
ubuntu@mail:~$ sudo mkdir /etc/opendkim/keys
ubuntu@mail:~$ sudo chown -R opendkim:opendkim /etc/opendkim
ubuntu@mail:~$ sudo chmod go-rw /etc/opendkim/keys/
ubuntu@mail:~$
```

Creamos las signing tables.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/opendkim/signing.table *
*@mfgh.work.gd default._domainkey.mfgh.work.gd
*/*.mfgh.work.gd default._domainkey.mfgh.work.gd
```

Ahora creo la key table.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/openssl/key.table *
default._domainkey.mfgh.work.gd mfgh.work.gd:default:/etc/openssl/keys/mfgh.work.gd/default.private
```

Ahora los trusted hosts.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/openssl/trusted.hosts *
127.0.0.1
localhost
.mfgh.work.gd
```

Creo la propia llave privada junto a su carpeta.

```
ubuntu@mail:~$ sudo mkdir /etc/openssl/keys/mfgh.work.gd
ubuntu@mail:~$ sudo openssl-genkey -b 2048 -d mfgh.work.gd -D /etc/openssl/keys/mfgh.work.gd -s default -v
openssl-genkey: generating private key
openssl-genkey: private key written to default.private
openssl-genkey: extracting public key
openssl-genkey: DNS TXT record written to default.txt

ubuntu@mail:~$ sudo chown openssl:openssl /etc/openssl/keys/mfgh.work.gd/default.private
ubuntu@mail:~$ sudo chmod 600 /etc/openssl/keys/mfgh.work.gd/default.private
ubuntu@mail:~$
```

Comprobamos que se ha creado bien.

```
ubuntu@mail:~$ sudo cat /etc/openssl/keys/mfgh.work.gd/default.txt
default._domainkey IN TXT ( "v=DKIM1; h=sha256; k=rsa; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5IialHOCpusJNA8FXFntvMeckT2afVL4LJyPLtMXI9q9PoyFEhyLQwj4nm+SK32
uuJ000EMbpv4nN74YXLthw5DVt/LUDaH4V8wZ81deB9ijgZVZ90Q0yH1SeC//VLLs20MJ+jp0cLRH1vnjE+ERHvwaUVewbW3lOCsKFe4ueo77zMLJf+f6Sf8
LYbf/CchmrsQP5NpWPIz02G"
"n9udMrk53GYAn7k92/cFyYuVpzhjnREw/+Nj/SIV9K/uaKt2FZbS2xc7HmQZTR4pRdQFgEztI9xZo3QAHgqGVDxm/sk+Y2LbvggD2YD2ZwTi
ioJwYtdsd5XgpsiCQkPrBgCFD0QIDAQAB" ) ; ----- DKIM key default for mfgh.work.gd
ubuntu@mail:~$
```

Esta clave debemos añadirla ahora en otro txt en nuestro freedns:

TXT Records				
TXT Records (TXT)				
TXT Name		Text Value	TTL (hr:min)	Action
@.mfgh.work.gd.		v=spf1 mx ~all	08:00	<a href="#">Edit</a>   <a href="#">Delete</a>
default._domainkey.mfgh.work.gd.		p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5IialHOCpusJNA8FXFntvMeckT2afVL4LJyPLtMXI9q9PoyFEhyLQwj4nm+SK32uuJ000EMbpv4nN74YXLthw5DVt/LUDaH4V8wZ81deB9ijgZVZ90Q0yH1SeC//VLLs20MJ+jp0cLRH1vnjE+ERHvwaUVewbW3lOCsKFe4ueo77zMLJf+f6Sf8LYbf/CchmrsQP5NpWPIz02G  n9udMrk53GYAn7k92/cFyYuVpzhjnREw/+Nj/SIV9K/uaKt2FZbS2xc7HmQZTR4pRdQFgEztI9xZo3QAHgqGVDxm/sk+Y2LbvggD2YD2ZwTiioJwYtdsd5XgpsiCQkPrBgCFD0QIDAQAB	08:00	<a href="#">Edit</a>   <a href="#">Delete</a>



Comprobamos, aunque a nosotros nos sale not secure.

```
ubuntu@mail:~$ sudo opendkim-testkey -d mfggh.work.gd -s default -vvv
opendkim-testkey: using default configfile /etc/opendkim.conf
opendkim-testkey: checking key 'default._domainkey.mfggh.work.gd'
opendkim-testkey: key not secure
opendkim-testkey: key OK
```

Creamos la siguiente carpeta.

```
ubuntu@mail:~$ sudo mkdir /var/spool/postfix/opendkim
sudo chown opendkim:postfix /var/spool/postfix/opendkim
ubuntu@mail:~$ sudo chown opendkim:postfix /var/spool/postfix/opendkim
```

Entramos a /etc/opendkim.conf y comentamos la primera línea de socket y descomentamos la última. ()

```
ubuntu@mail: ~
GNU nano 7.2 /etc/opendkim.conf *
SigningTable      refile:/etc/opendkim/signing.table

# Hosts to ignore when verifying signatures
ExternalIgnoreList /etc/opendkim/trusted.hosts

# A set of internal hosts whose mail should be signed
InternalHosts     /etc/opendkim/trusted.hosts

# Socket for the MTA connection (required). If the MTA is inside a chroot jail,
# it must be ensured that the socket is accessible. In Debian, Postfix runs in
# a chroot in /var/spool/postfix, therefore a Unix socket would have to be
# configured as shown on the last line below.
#Socket           local:/run/opendkim/opendkim.sock
#Socket           inet:8891@localhost
#Socket           inet:8891
Socket            local:/var/spool/postfix/opendkim/opendkim.sock
```

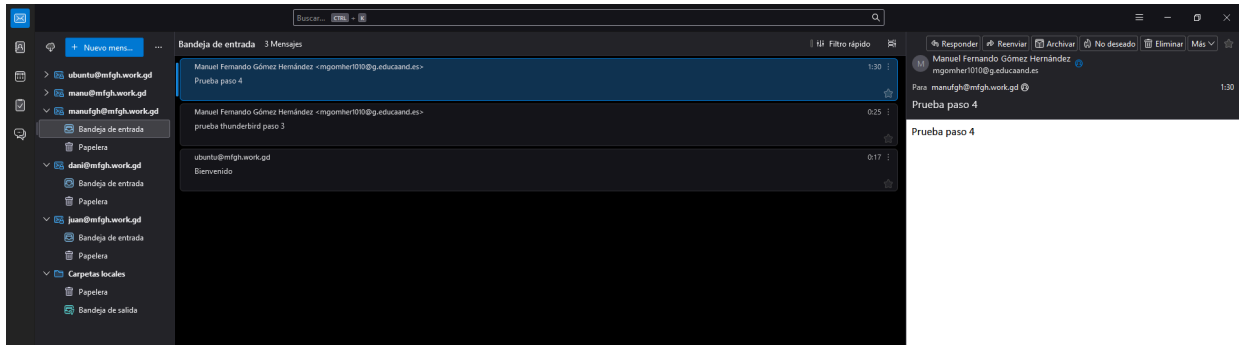
Ahora vamos a main.cf y añadimos lo siguiente de Milter al final.

```
ubuntu@mail: ~
GNU nano 7.2 /etc/postfix/main.cf *
virtual_uid_maps = static:2000
virtual_gid_maps = static:2000

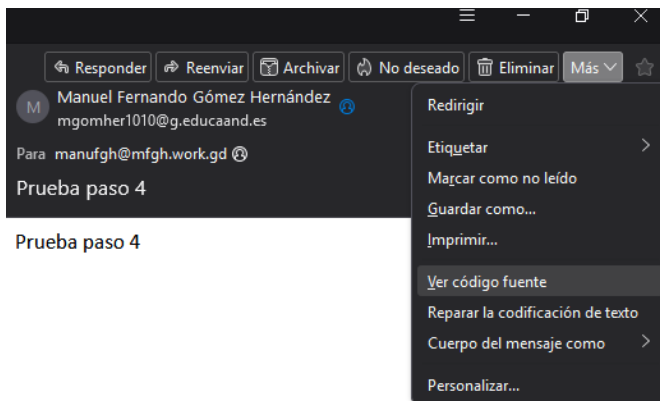
policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_unauth_destination,
    check_policy_service unix:private/policyd-spf

# Milter configuration
milter_default_action = accept
milter_protocol = 6
smtpd_milters = local:opendkim/opendkim.sock
non_smtpd_milters = $smtpd_milters
```

Vamos a enviar un mail de prueba.



Si pulsamos en más->Ver código fuente podemos observar lo siguiente.



```
Fuente de: imap://manufgh%40mfgh.work.gd@mail.mfgh.work.gd:143/?ch=3&ui=3&inbox=3&3 - Mozilla Thunderbird
Archivo  Editar  Ver  Ayuda

X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <mgomher1010@educaand.es>
Delivered-To: manufgh@mfgh.work.gd
Received: from mail-qv1-f53.google.com (mail-qv1-f53.google.com [209.85.219.53])
  by mail.mfgh.work.gd (Postfix) with ESMTPS id 78A544166
  id T1CR1KVgmcFTWAA69KGA
  (envelope-from <mgomher1010@educaand.es>)
  for <manufgh@mfgh.work.gd>; Wed, 26 Feb 2025 00:30:29 +0000
Received-SPF: Pass (mailfrom identity=mailfrom; client-ip=209.85.219.53; helo=mail-qv1-f53.google.com; envelope-from=mgomher1010@educaand.es; receiver=mfgh.work.gd)
Received: from mail-qv1-f53.google.com (Postfix) with ESMTPS id 78A544166
  for <manufgh@mfgh.work.gd>; Wed, 26 Feb 2025 00:30:29 +0000 (UTC)
Received: by mail-qv1-f53.google.com with SMTP id 6a1803df08f44-6e88983cedaso384046d6.1
  for <manufgh@mfgh.work.gd>; Tue, 25 Feb 2025 16:30:29 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=g-educaand.es.20230601.gappssmtp.com; s=20230601; t=1740529826; x=1741134626;
  h=to:subject:message-id:date:from:mime-version:from:to:cc:subject;
  :date:message-id:reply-to;
  bh=20eSRvY0z2rqVlbGfgntKODE2b0nAB3V1hPzyWqs+;
  b=Bn2c8BAahQp6Efc++Vfmy6y8fWfYhhuC1/nDeupnugn81A02SRk3Z2z1JFLUCyUd1
  MaNehH5GxpwnnFicer/mu7D0hwVYG6ShIX2tW1VIGj3U1u4Scm4CwedgK40U8nYt6mC
  aeknIG3Wpn101r8r3IS/UQbraHPX9a1Mx1I38fp3Vg+Ev7a39EMPaAsm612Xn3Fn/Fr
  OmpXmHddnZfXVQXpQd4eGvShwDZQafm65JKaZ7kLuPMc2H2BocOtaCde8g/mgQFU7D
  IFxugP1ebaZ145z4DXta1f0V+pdUGS1pL4X15eE7eJp1/G2oYU19r+ndmy1zky7TH
  E++=
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  u=1e100.net; s=20230601; t=1740529826; x=1741134626;
  h=to:subject:message-id:date:from:mime-version:x-gm-message-state
  :from:to:cc:subject:date:message-id:reply-to;
  bh=20eSRvY0z2rqVlbGfgntKODE2b0nAB3V1hPzyWqs+;
  b=SF2G5Uy2hzWC9A/6B2ayGHYSm0CRVqm3Csh4YQmk1nyJ4qns3ge0BskpLKB6MqUTK
  6kmsvtDMP1GD1x1T3uQsEAQDVmY1Fz+/UuLntH2jMeFiaPVfVGSdbPuHG7ZCnwMG
  AxpV0VEH81ZcecbnfY1J0usSmwhfV6Vgsivxcu00jkrIns/Q9sUc9soQ0Qh
  oBz+s8zcwXk41L2uPzGzC122uJ11tGmFgRbR0Xs=1x0f23fQ0b08GTF5NSH1
  1CUGRRFfcQbunnehgQB2Nf4Hm6Cp3V0E2nPLCX+181VufP1+V3ktSTg4och1+BFx/
  GZ6Q==
X-Gm-Message-State: AOJ0uYzYyW7ytugu7epPDBmBvR7BnRSEPUOvcXv309n8sx5bWusZD
  FHLuMPb1LstDPXgeuC27NL9Q/BlrVbh+148yPM5WvkkEUEG1mpABxuZeim+LVJNay4CS6
  NmP1G54hXhXpZ1ZouKfXce+I9JPg81E6Uv0e01h1LuoX5r+
X-Gm-Gg: ASBncveft7fecQbF6nPKA+UDSHyBygZ3EmAz7U1U13azR0EPNo3nAy3mhT+0tXL
  JVeulI8gVtpg3Dc1XJTW6hGCK+Fa+j0J2P1H20T+MdoZn0Z61ajtIdn4UKV0LBuKLSvygHCQ
  s1f88=
X-Gm-Smt-Source: AGHT-IEJ8lquYUoVUK3olSxXmU18VkrOP0KKNVODGpuyHtMNgYj3xV1z0/wSs/39fd+AAvtgTNI9AxUG85hK3Jm0=
X-Received: by 2002:a05:6214:29c7:b0:6ee:5b17:aec with SMTP id
  6a1803df08f44-6e889827femr281767966d6.6.1740529825788; Tue, 25 Feb 2025
  16:30:25 -0800 (PST)
MIME-Version: 1.0
From: -RUT-87QManuel_Fernando_G-C3-B3mez_Hern-C3-A1ndez?<mgomher1010@educaand.es>
Date: Wed, 26 Feb 2025 01:30:14 +0100
X-Gm-Features: AMEUv2NDKdaxBEXZ2w08S118dKB8I 480VvRTfzF5EHJna2fu_Dyp_13Es-xx
Message-ID: <CAGW921F0ZfgWUQc6neZSV3MBQ4_YsuaQyzeuMcB0Nudw0EQ@mail.gmail.com>
Subject: Prueba paso 4
```

El resto de tutoriales de esta serie también funcionan en Ubuntu 22.04 perfectamente y son de mucha utilidad para un servidor de correo electrónico en producción. No se pide su realización por motivos de tiempo.

Esta práctica debe ser documentada pero también será mostrada y explicada al profesor en sus objetivos principales.

No se evaluará nada fuera de plazo.

Enlaces de ayuda:

- Plataforma Pledin [Servicio de correo electrónico](#)
  - [Postfix Home Page](#)
  - [Dovecot Home Page](#)
  - **Referencias Base utilizadas para la práctica**
    - Paso 1 [Build Your Own Email Server on Ubuntu: Basic Postfix Setup - LinuxBabe](#)
    - Paso 2 [Part 2: Install Dovecot IMAP server on Ubuntu & Enable TLS Encryption](#)
    - Paso 3 [Part 3: PostfixAdmin – Create Virtual Mailboxes on Ubuntu Mail Server](#)
    - Paso 4 [Part 4: How to Set up SPF and DKIM with Postfix on Ubuntu Server](#)
  - Otra referencia útiles
    - [A Mailserver on Ubuntu 16.04: Postfix, Dovecot, MySQL – Ex Ratione](#)
    - [How to set up a mail server on a GNU / Linux system](#)
    - [Correo electrónico con Postfix, Dovecot y Thunderbird en Ubuntu 20.04 \(actualizado a Ubuntu 22.04 :-\)](#)
    - [Servidor de correo: Postfix y Dovecot](#)
-