

## Instalación del servicio de correo en Ubuntu Server

1. Primero actualizaremos nuestro sistema operativo para que esta en la ultima versión con el siguiente comando

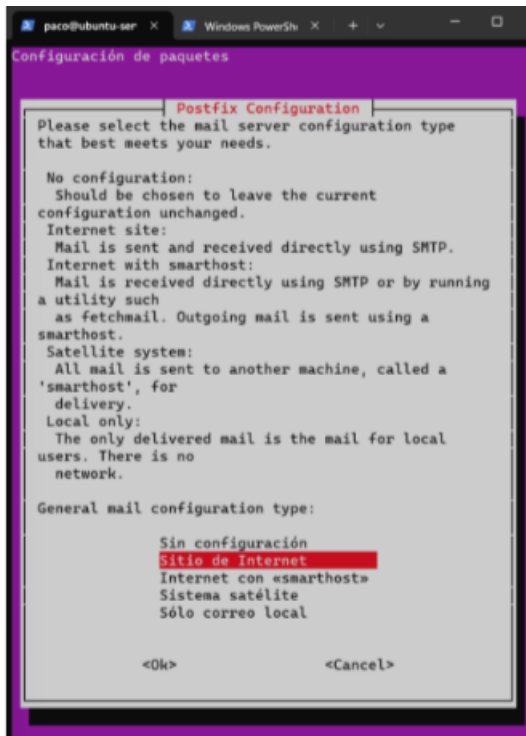
```
root@fidel:/home/fidel# sudo apt update
```

```
[sudo] password for fidel:
root@fidel:/home/fidel#
root@fidel:/home/fidel# sudo apt update
Obj:1 http://mx.archive.ubuntu.com/ubuntu lunar InRelease
Des:2 http://mx.archive.ubuntu.com/ubuntu lunar-updates InRelease [109 kB]
Obj:3 http://mx.archive.ubuntu.com/ubuntu lunar-backports InRelease
Des:4 http://mx.archive.ubuntu.com/ubuntu lunar-security InRelease [109 kB]
Des:5 http://mx.archive.ubuntu.com/ubuntu lunar-updates/main amd64 Packages
[538 kB]
Des:6 http://mx.archive.ubuntu.com/ubuntu lunar-updates/main Translation-en
[128 kB]
Des:7 http://mx.archive.ubuntu.com/ubuntu lunar-updates/restricted amd64 Pac
kages [457 kB]
Des:8 http://mx.archive.ubuntu.com/ubuntu lunar-updates/restricted Translati
on-en [74,8 kB]
Des:9 http://mx.archive.ubuntu.com/ubuntu lunar-updates/universe amd64 Packa
ges [842 kB]
Des:10 http://mx.archive.ubuntu.com/ubuntu lunar-updates/universe Translatio
n-en [109 kB]
Des:11 http://mx.archive.ubuntu.com/ubuntu lunar-security/main amd64 Package
s [430 kB]
Des:12 http://mx.archive.ubuntu.com/ubuntu lunar-security/main Translation-e
n [96,9 kB]
Des:13 http://mx.archive.ubuntu.com/ubuntu lunar-security/restricted amd64 P
ackages [457 kB]
Des:14 http://mx.archive.ubuntu.com/ubuntu lunar-security/restricted Transla
tion-en [74,8 kB]
Des:15 http://mx.archive.ubuntu.com/ubuntu lunar-security/universe amd64 Pac
kages [749 kB]
Des:16 http://mx.archive.ubuntu.com/ubuntu lunar-security/universe Translati
on-en [80,3 kB]
Descargados 4.256 kB en 3s (1.272 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Se pueden actualizar 53 paquetes. Ejecute «apt list --upgradable» para verlo
s.
root@fidel:/home/fidel#
root@fidel:/home/fidel# |
```

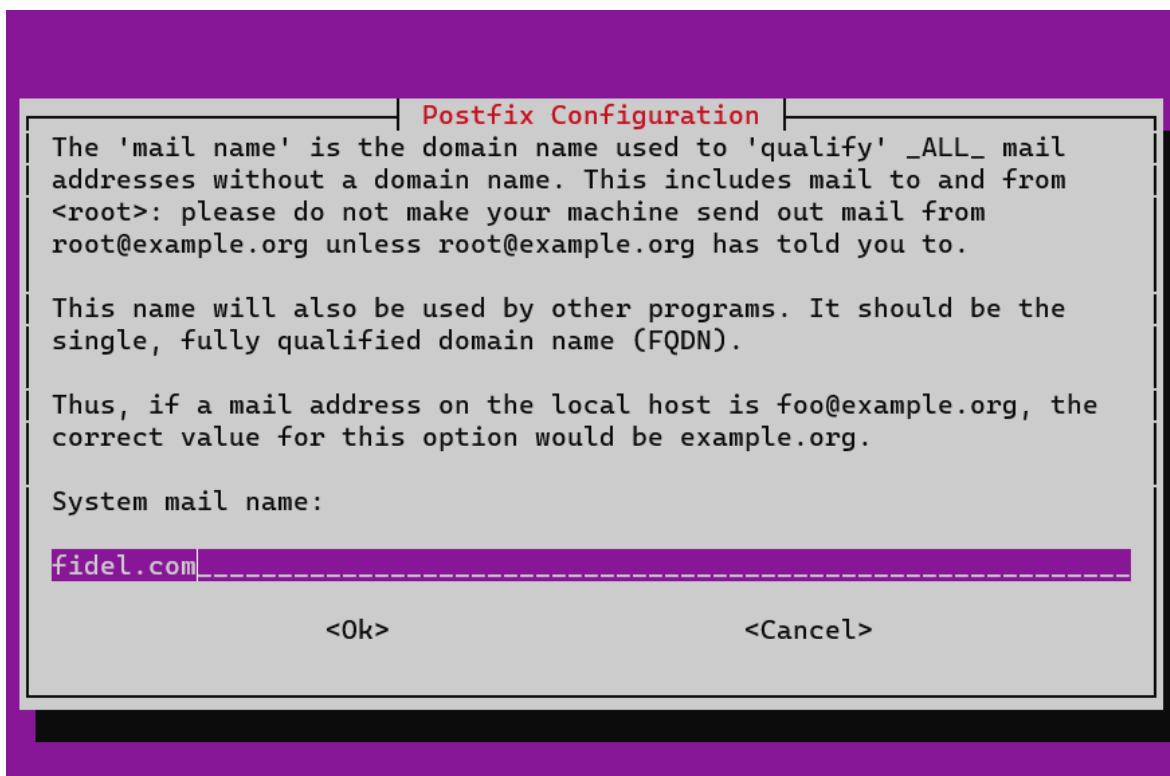
2. Ahora comenzaremos instalando postfix como el primer servicio

```
root@fidel:/home/fidel# sudo apt install postfix|
```

De forma automática se abrirá una pantalla grafica que se controla con las flechas del teclado, deben seleccionar la que dice "Sitio de internet"



Después se tendrá que escribir el nombre del dominio de correo que prefieran y darle ok



3. El siguiente paso será configurar un archivo de postfix, pero antes debemos de realizarle una copia por seguridad con el siguiente comando

```
root@fidel:/home/fidel# cp /etc/postfix/main.cf /etc/postfix/main.cf.copy
```

```
sudo nano /etc/postfix/main.cf
```

Se modifican tres cosas:

- “Myhostname”: en esta parte se coloca el nombre del dominio que pusimos al instalar postfix
- “Mydestination”: en este no es necesario mover nada, solo observar que el dominio que creamos al instalar postfix aparezca ahí.
- “mynetworks”: únicamente debemos agregar sin borrar nada, nuestra ip local en la que estamos trabajando, en mi caso es la 10.0.1.0/24, con su sufijo de mascara dependiendo el que tengan.

```
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer
myhostname = fidel.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, fidel.com, fidel, localhost.localdomain, local
relayhost =
mynetworks = 10.0.1.0/24 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

- Una vez configurado todo, guardamos el archivo y salimos, para reiniciar el servicio con lo siguiente

```
service postfix reload
```

- Después instalaremos la siguiente librería

```
sudo apt install mailutils
```

- Debemos volver a abrir el archivo del paso 3 y agregar esta línea hasta el final

```
home_mailbox=Maildir/
```

- Después se debe salir e instalar la siguiente librería

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

- Ingresamos a este archivo que se muestra

```
sudo nano /etc/dovecot/conf.d/10-mail.conf
```

Debemos modificar esta línea que se muestra y agregarle lo siguiente

```
mail_location = maildir:~/Maildir
```

9. Lo siguiente es ingresar al archivo que se especifica

```
sudo nano /etc/dovecot/conf.d/10-ssl.conf
```

La línea que dice “ssl = yes”, deben cambiarla por no

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

# 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/dovecot/private/dovecot.pem
#ssl_key = </etc/dovecot/private/dovecot.key

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path>.
#ssl_key_password =

# PEM encoded trusted certificate authority. Set this only if you intend to
# ssl_verify_client_cert=yes. The file should contain the CA certificate(s)
# followed by the matching CRL(s). (e.g. ssl_ca = </etc/ssl/certs/ca.pem)
#ssl_ca =

# Require that CRL check succeeds for client certificates.
#ssl_require_crl = yes
```

10. Nos metemos al siguiente archivo

```
sudo nano /etc/dovecot/conf.d/10-auth.conf
```

En este cambiamos de que diga “yes” a “no”

```

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 = no

# Authentication cache size (e.g. 10M). 0 means it's disabled. Note that
# bsdauth and PAM require cache_key to be set for caching to be used.
#auth_cache_size = 0
# Time to live for cached data. After TTL expires the cached record is no
# longer used, *except* if the main database lookup returns internal failure.
# We also try to handle password changes automatically: If user's previous
# authentication was successful, but this one wasn't, the cache isn't used.
# For now this works only with plaintext authentication.
#auth_cache_ttl = 1 hour
# TTL for negative hits (user not found, password mismatch).
# 0 disables caching them completely.

```

11. Ahora reiniciamos el servicio de dovecot, para ejecutar todos los cambios

```

root@fidel:/home/fidel# sudo service dovecot reload

```

12. Por último, se deben de crear dos cuentas para probar el correo e instalar en sus computadoras clientes un software llamado Thunderbird para probar su correo conectados la red que este el servidor

Se debe colocar la información de un usuario como en esta pantalla y después el otro usuario

**Configuración manual**

**SERVIDOR ENTRANTE**

Protocolo: **IMAP** ▼

Nombre del servidor: **mail.red.ian**

Puerto: **143** ▲ ▼

Seguridad de la conexión: **Ninguna** ▼

Método de autenticación: **Contraseña normal** ▼

Nombre de usuario: **paco2**

**SERVIDOR SALIENTE**

Nombre del servidor: **mail.red.ian**

Puerto: **25** ▲ ▼

Seguridad de la conexión: **STARTTLS** ▼

Método de autenticación: **Contraseña normal** ▼

Nombre de usuario: **paco2**

[Configuración avanzada](#)

[Documentación](#)

[Volver a comprobar](#) [Cancelar](#) [Hecho](#)

Thunderbird intentará detectar automáticamente los campos que se han

Aquí se realiza la prueba enviando un correo entre los usuarios

