

Servicios de red e internet

Flipped Classroom

2º ASIR

1 Actividad Práctica 1 - Análisis de Infraestructura (45-60 minutos)

Auditoría de Configuración DNS para Correo Electrónico

1.1 Descripción

El alumnado debe analizar la infraestructura de correo de dominios reales asignados.

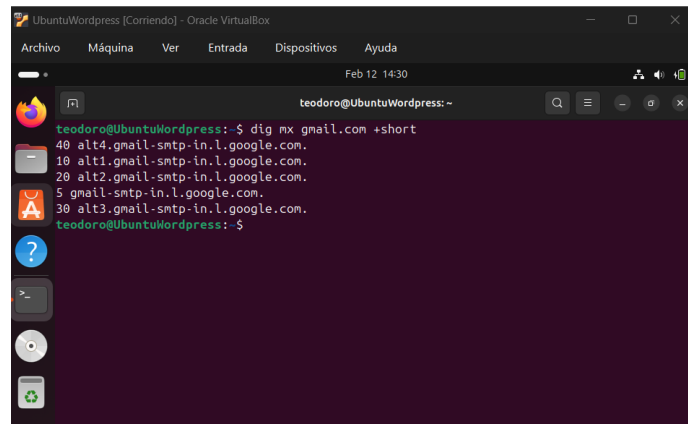
1.2 Tareas

1. Identificar los registros MX y sus prioridades.
2. Verificar la existencia de SPF y validar su sintaxis.
3. Buscar los registros DKIM (usando selectores comunes: 'default', 'selector1', 'google', etc.)
4. Verificar la política DMARC.
5. Realizar el reverse DNS (PTR) de las IPs de los servidores MX.
6. Documentar los hallazgos en una tabla comparativa.

1.3 Dominios sugeridos

- gmail.com (Google Workspace)
- outlook.com (Microsoft 365)
- yahoo.com
- protonmail.com
- Un dominio de una empresa local/regional

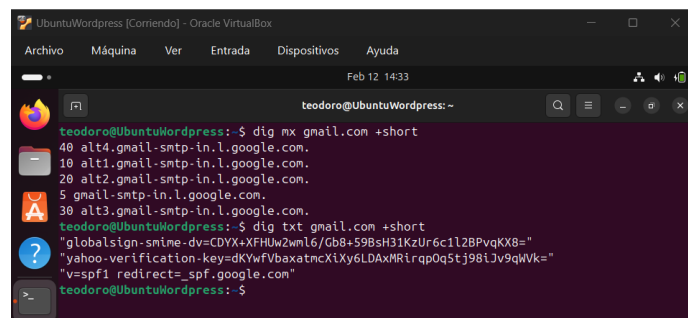
Empezaremos por abrir el terminal con privilegios de administrador y procederemos a utilizar uno de los siguientes comandos a nuestra discreción, puesto que ambos cumplen el propósito para esta actividad. En mi caso utilizaré dig debido a que ofrece más detalles sobre las consultas que nslookup.



```
teodoro@UbuntuWordPress:~$ dig mx gmail.com +short
40 alt4.gmail-smtp-in.l.google.com.
10 alt1.gmail-smtp-in.l.google.com.
20 alt2.gmail-smtp-in.l.google.com.
5 gmail-smtp-in.l.google.com.
30 alt3.gmail-smtp-in.l.google.com.
teodoro@UbuntuWordPress:~$
```

Figure 1: 1

Verás una lista con números (prioridad) y nombres de servidores. Ejemplo: 5 gmail-smtp-in.l.google.com. Nuestro siguiente paso es buscar los registros TXT que validan qué IPs pueden enviar correo. Para ello, usaremos el comando dig nuevamente:

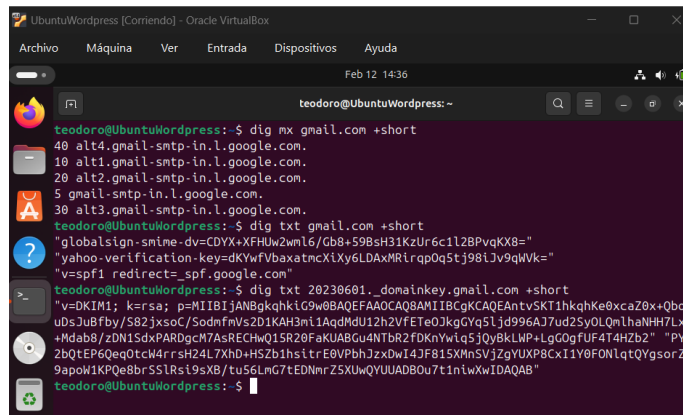


```
teodoro@UbuntuWordPress:~$ dig txt gmail.com +short
"globalsign-smime-dv=CDYX+XFHw2wml6/Cb8+59BsH3IKzUr6c1l2BPvqKX8="
"yahoo-verification-key=dKYwFVbaxatmcXiXy6LDAXMRirp0q5tj98ljv9qWVk="
"v=spf1 redirect=spf.google.com"
teodoro@UbuntuWordPress:~$
```

Figure 2: 2

Buscaremos una línea que empiece por "v=spf1...". Debemos analizar si termina en -all (estricto) o all (suave).

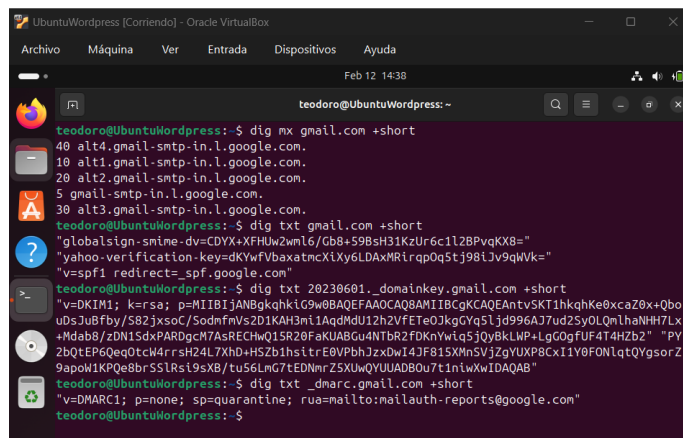
El siguiente paso es verificar la firma criptográfica. Para ello, nuevamente el comando `dig` nos permite confirmar la firma:



```
teodoro@UbuntuWordPress:~$ dig mx gmail.com +short
40 alt4.gmail-smtp-in.l.google.com.
10 alt1.gmail-smtp-in.l.google.com.
20 alt2.gmail-smtp-in.l.google.com.
5 gmail-smtp-in.l.google.com.
30 alt3.gmail-smtp-in.l.google.com.
teodoro@UbuntuWordPress:~$ dig txt gmail.com +short
"globalsign-smime-dv=CDYX+XFHw2wml6/Cb8+59Bsh3IKzUr6c1l28PvqKX8="
"yahoo-verification-key=dKYwFVbaxatmcXiY6LDAXMRirapQq5tj98Ijv9qWVvk="
"v=spf1 redirect=spf.google.com"
teodoro@UbuntuWordPress:~$ dig txt 20230601._domainkey.gmail.com +short
"v=DKIM1; k=rsa; p=MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBcGKCAQEAntvSKT1hkqhKe0xcaZ0x+Qbo
uDsJu8fby/S82jxsoC/SodmFmVs2D1KAH3mi1AqdMdU12h2VfETe0JkgGYq5ljd996AJ7ud25yOLm1haNH7Lx
+Mdab8/zDN1SdxPARDgcM7AsREChwQ15R20FaKUABGu4Ntbr2fDKnYwIq5jQy8kLWP+LgGogFUF4T4Hzb2" "PY
2bQTEP6QeQdtcW4rrsH24L7Xhd+HSZb1hstRE0VPbhJzxDwI4JF815XmN5VjZgYUXP8Cx11Y0FONlqtQYgsorZ
9apow1KPQe8brSS1Rsi9sXB/tu56LmG7tEDNmrZ5XUwQYUADBOu7t1niWxIDAQAB"
teodoro@UbuntuWordPress:~$
```

Figure 3: 3

Nuestro siguiente paso es verificar la política DMARC. Esto nos permite definir qué hacer si fallan SPF o DKIM. Nuevamente con el comando `dig`:

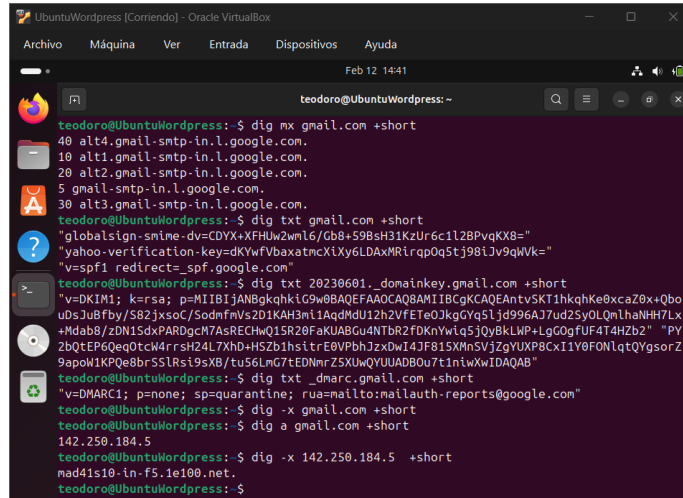


```
teodoro@UbuntuWordPress:~$ dig mx gmail.com +short
40 alt4.gmail-smtp-in.l.google.com.
10 alt1.gmail-smtp-in.l.google.com.
20 alt2.gmail-smtp-in.l.google.com.
5 gmail-smtp-in.l.google.com.
30 alt3.gmail-smtp-in.l.google.com.
teodoro@UbuntuWordPress:~$ dig txt gmail.com +short
"globalsign-smime-dv=CDYX+XFHw2wml6/Cb8+59Bsh3IKzUr6c1l28PvqKX8="
"yahoo-verification-key=dKYwFVbaxatmcXiY6LDAXMRirapQq5tj98Ijv9qWVvk="
"v=spf1 redirect=spf.google.com"
teodoro@UbuntuWordPress:~$ dig txt 20230601._domainkey.gmail.com +short
"v=DKIM1; k=rsa; p=MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBcGKCAQEAntvSKT1hkqhKe0xcaZ0x+Qbo
uDsJu8fby/S82jxsoC/SodmFmVs2D1KAH3mi1AqdMdU12h2VfETe0JkgGYq5ljd996AJ7ud25yOLm1haNH7Lx
+Mdab8/zDN1SdxPARDgcM7AsREChwQ15R20FaKUABGu4Ntbr2fDKnYwIq5jQy8kLWP+LgGogFUF4T4Hzb2" "PY
2bQTEP6QeQdtcW4rrsH24L7Xhd+HSZb1hstRE0VPbhJzxDwI4JF815XmN5VjZgYUXP8Cx11Y0FONlqtQYgsorZ
9apow1KPQe8brSS1Rsi9sXB/tu56LmG7tEDNmrZ5XUwQYUADBOu7t1niWxIDAQAB"
teodoro@UbuntuWordPress:~$ dig txt _dmarc.gmail.com +short
"v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-reports@google.com"
teodoro@UbuntuWordPress:~$
```

Figure 4: 4

Por último, verificamos que la IP del servidor MX resuelva al nombre del servidor. Usaremos `dig` para este paso también.

Pues ya estarían los pasos necesarios, solo queda incluir varias consultas a una tabla comparativa con los hallazgos de: gmail.com, outlook.com, yahoo.com, y un dominio local de tu elección.



```
teodoro@UbuntuWordPress: ~  
teodoro@UbuntuWordPress:~$ dig mx gmail.com +short  
40 alt4.gmail-smtp-in.l.google.com.  
10 alt1.gmail-smtp-in.l.google.com.  
20 alt2.gmail-smtp-in.l.google.com.  
5 gmail-smtp-in.l.google.com.  
30 alt3.gmail-smtp-in.l.google.com.  
teodoro@UbuntuWordPress:~$ dig txt gmail.com +short  
"globalsign-smime-dv=CDYX+XfHw2wml6/Gb8+59Bsh31KzUr6c1l28PvqKX8="  
"yahoo-verification-key=dKYwFvbxatmcXLY6LDAXMRirp0q05tj98ljv9qWVke="   
"v=spf1 redirect=spf.google.com"  
teodoro@UbuntuWordPress:~$ dig txt 20230601_domainkey.gmail.com +short  
"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBGKCAQEAntv5KT1hkqhKe0xcaZ0x+Qbo  
uDsJu8fby/S82jxsoC/SodmfnVs2D1KAH3mi1AqdMdU12h2VfETe0JkgGYqSLjd996AJ7ud2SyOLQmlhaNHH7Lx  
+Mdab8/zDN1SdxPARDgcM7AsRECHwQ15R20FakUABGu4NTbR2fDknYwiq5jQyBkLWP+LgG0gfUF4T4HZb2" "PY  
2bQtEP6QeqOtcW4rrsH24L7XhD+HSZb1hsitrE0VPbhJzxDwI4JF815XMnSVjZgYUXP8CxiIY0FONlqtQYgsorZ  
9apoWIKPQe8brSSlRs19sXB/tu56LmG7tEDNmrZ5XUwQYUADBOu7t1niwKwIDAQAB"  
teodoro@UbuntuWordPress:~$ dig txt _dmarc.gmail.com +short  
"v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-reports@google.com"  
teodoro@UbuntuWordPress:~$ dig -x gmail.com +short  
teodoro@UbuntuWordPress:~$ dig a gmail.com +short  
142.250.184.5  
teodoro@UbuntuWordPress:~$ dig -x 142.250.184.5 +short  
mad41s10-in-f5.1e100.net.  
teodoro@UbuntuWordPress:~$
```

Figure 5: 5

1.4 Entregable

Un documento Word o PDF con la tabla comparativa, además de las conclusiones sobre las buenas prácticas encontradas.

2 Actividad Práctica 2 - Configuración de Servidor** (60-90 minutos)

Configuración Básica de Postfix y Dovecot

2.1 Descripción

Configurar un servidor de correo funcional en entorno virtualizado.

2.2 Prerequisitos técnicos

- Máquina virtual Ubuntu Server o Debian.
- Acceso root.
- Conexión a Internet.

2.3 Tareas

1. Instalar Postfix y Dovecot.
2. Configurar los siguientes parámetros básicos en 'main.cf':
 - 'myhostname', 'mydomain', 'myorigin'
 - 'inet_interfaces = all'
 - 'mydestination' para entrega local
3. Crear varios usuarios de sistema para simular buzones.
4. Configurar Dovecot para acceso IMAP:
 - 'mail_location = maildir: /Maildir'
 - Habilitar protocolos imap
5. Enviar correo de prueba local usando 'mail' o 'swaks'
6. Leer el correo usando un cliente IMAP (Thunderbird o Evolution)
7. Analizar los logs en '/var/log/mail.log'

El primer paso es instalar Postfix y Dovecot. Para ello ejecutamos en el terminal el siguiente comando:

```
sudo apt update
sudo apt install postfix dovecot-imapd dovecot-core mailutils
```

Lo siguiente es editar el archivo de configuración, para ello utilizamos el comando:

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

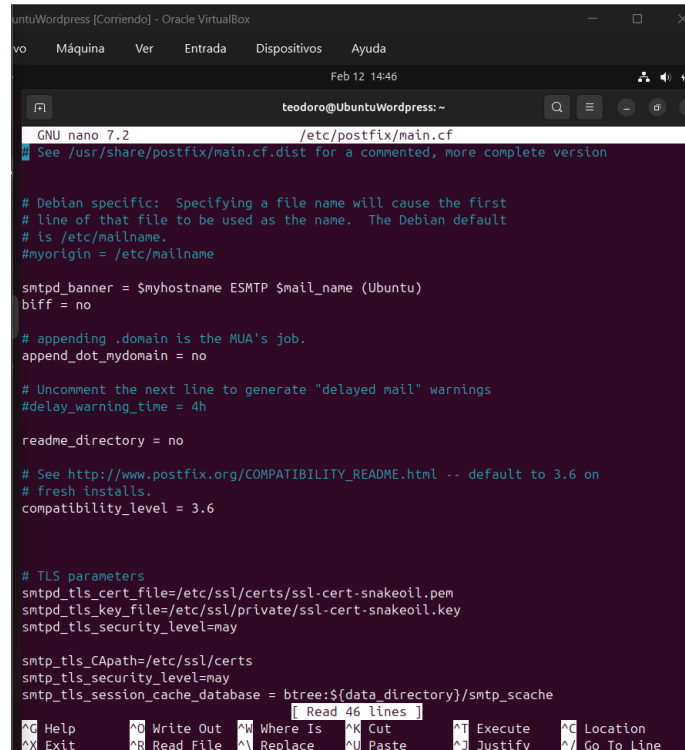


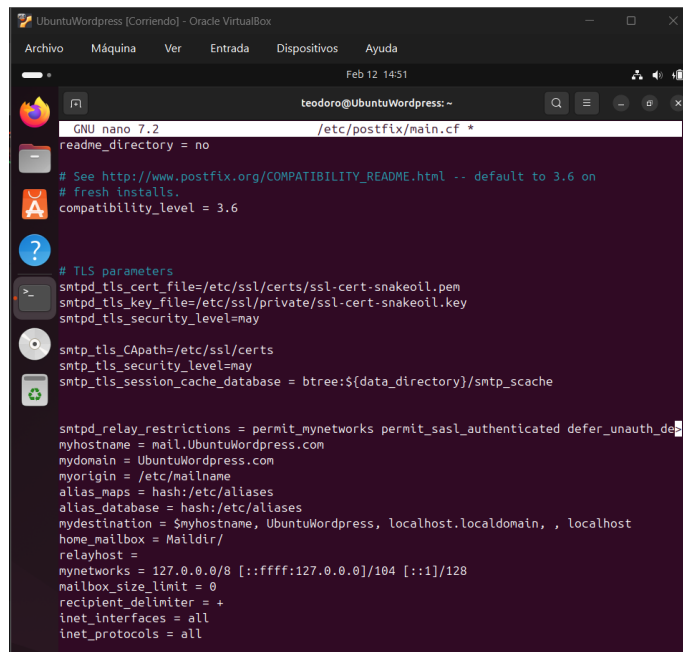
Figure 6: 6

Debemos editar el archivo y añadir lo siguiente:

```
myhostname = mail.miservidor.com # Ajusta a tu hostname
mydomain = miservidor.com
myorigin = /etc/mailname          # O $mydomain
inet_interfaces = all             # Escuchar en todas las interfaces
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
home_mailbox = Maildir/          # Importante para compatibilidad con Dovecot
```

Nuestro siguiente paso es configurar Dovecot:

```
sudo nano /etc/dovecot/dovecot.conf
```



The screenshot shows a terminal window titled 'UbuntuWordpress [Corriendo] - Oracle VirtualBox'. The user is logged in as 'teodoro@UbuntuWordpress: ~'. The terminal shows the nano 7.2 editor editing the file '/etc/postfix/main.cf'. The configuration includes settings for TLS, relay restrictions, myhostname, mydomain, myorigin, alias_maps, alias_database, mydestination, home_mailbox, relayhost, mynetworks, mailbox_size_limit, recipient_delimiter, inet_interfaces, and inet_protocols.

```
GNU nano 7.2 /etc/postfix/main.cf *
readme_directory = no

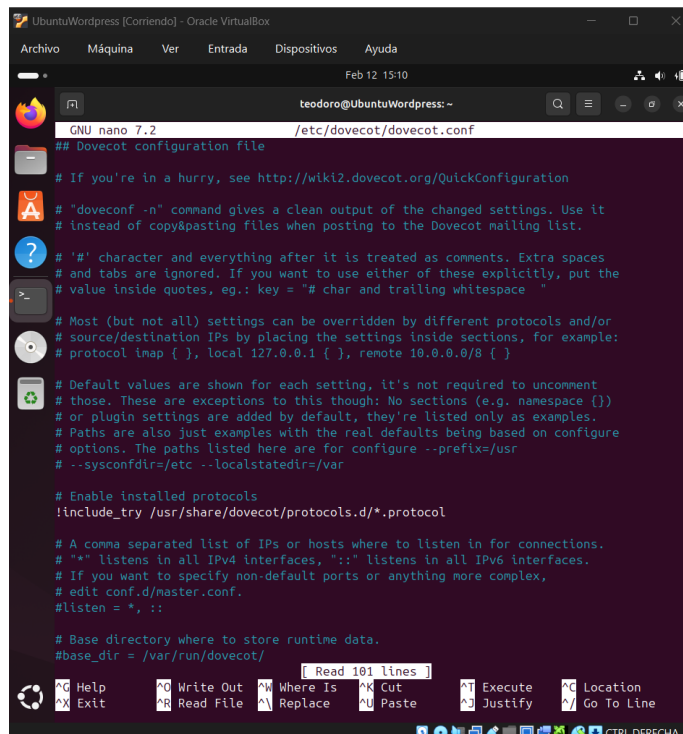
# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6

# 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_unauth_de
myhostname = mail.UbuntuWordpress.com
mydomain = UbuntuWordpress.com
myorigin = /etc/mailname
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $myhostname, UbuntuWordpress, localhost.localdomain, , localhost
home_mailbox = Maildir/
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

Figure 7: 7



The screenshot shows a terminal window titled 'UbuntuWordpress [Corriendo] - Oracle VirtualBox'. The user is logged in as 'teodoro@UbuntuWordpress: ~'. The terminal shows the nano 7.2 editor editing the file '/etc/dovecot/dovecot.conf'. The configuration includes settings for protocols, listen, and base_dir. A status bar at the bottom indicates 'Read 101 lines'.

```
GNU nano 7.2 /etc/dovecot/dovecot.conf
## Dovecot configuration file

# If you're in a hurry, see http://wiki2.dovecot.org/QuickConfiguration

# "doveconf -n" command gives a clean output of the changed settings. Use it
# instead of copy&pasting files when posting to the Dovecot mailing list.

# '#' character and everything after it is treated as comments. Extra spaces
# and tabs are ignored. If you want to use either of these explicitly, put the
# value inside quotes, eg.: key = "# char and trailing whitespace"

# Most (but not all) settings can be overridden by different protocols and/or
# source/destination IPs by placing the settings inside sections, for example:
# protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }

# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# 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

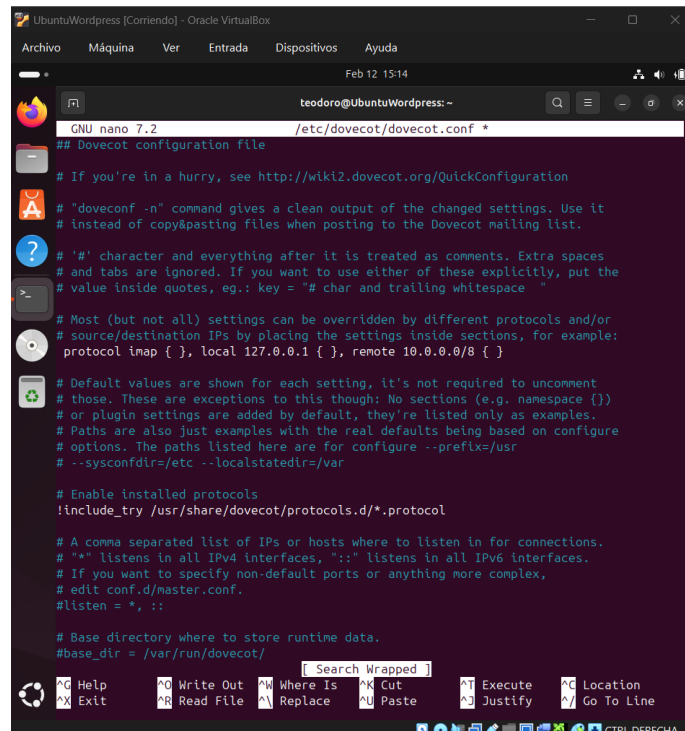
# Enable installed protocols
!include_try /usr/share/dovecot/protocols.d/*.protocol

# A comma separated list of IPs or hosts where to listen in for connections.
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
# edit conf.d/master.conf.
#listen = *, ::

# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/
```

Figure 8: 8

Editamos el archivo y quitamos comentarios en la línea de protocolos de imap



The screenshot shows a terminal window titled 'UbuntuWordPress [Corriendo] - Oracle VirtualBox'. The window has a menu bar with 'Archivo', 'Máquina', 'Ver', 'Entrada', 'Dispositivos', and 'Ayuda'. The terminal shows the user 'teodoro@UbuntuWordPress:~' at 'Feb 12 15:14'. The user is editing the file '/etc/dovecot/dovecot.conf' using the 'GNU nano 7.2' editor. The file content includes various configuration comments and settings for Dovecot, such as enabling protocols, setting listen addresses, and defining base directories. The terminal also displays a status bar with various keyboard shortcuts like '^O Help', '^X Exit', '^W Write Out', '^R Read File', '^M Where Is', '^H Replace', '^K Cut', '^U Paste', '^T Execute', '^J Justify', '^C Location', and '^_/ Go To Line'.

```
GNU nano 7.2 /etc/dovecot/dovecot.conf
## Dovecot configuration file

# If you're in a hurry, see http://wiki2.dovecot.org/QuickConfiguration

# "doveconf -n" command gives a clean output of the changed settings. Use it
# instead of copy&pasting files when posting to the Dovecot mailing list.

# '#' character and everything after it is treated as comments. Extra spaces
# and tabs are ignored. If you want to use either of these explicitly, put the
# value inside quotes, eg.: key = "# char and trailing whitespace"

# Most (but not all) settings can be overridden by different protocols and/or
# source/destination IPs by placing the settings inside sections, for example:
protocol imap {
  local 127.0.0.1 {
  remote 10.0.0.0/8 {
  }
}

# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# 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
!include_try /usr/share/dovecot/protocols.d/*.protocol

# A comma separated list of IPs or hosts where to listen in for connections.
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
# edit conf.d/master.conf.
#listen = *, ::

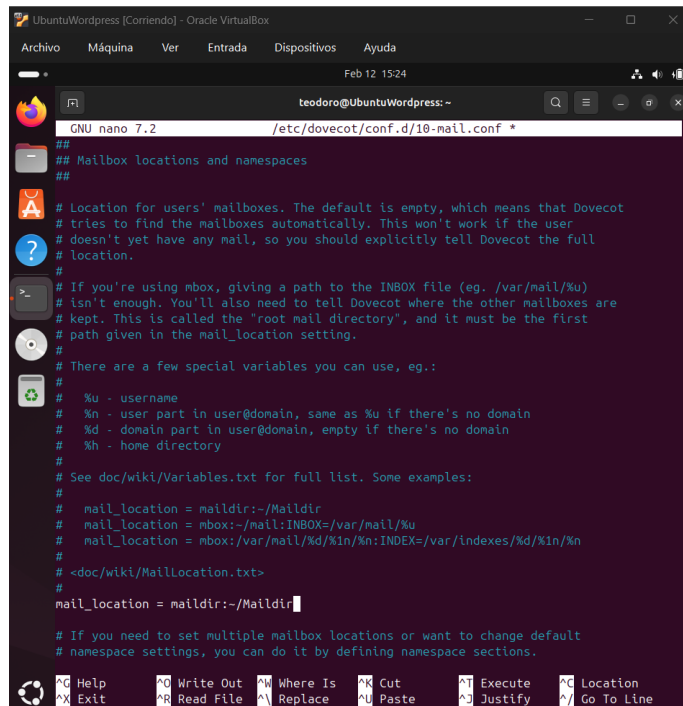
# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/
```

Figure 9: 9

Ahora debemos editar el siguiente archivo de configuración:

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


Editamos la linea que ponga mail_location:

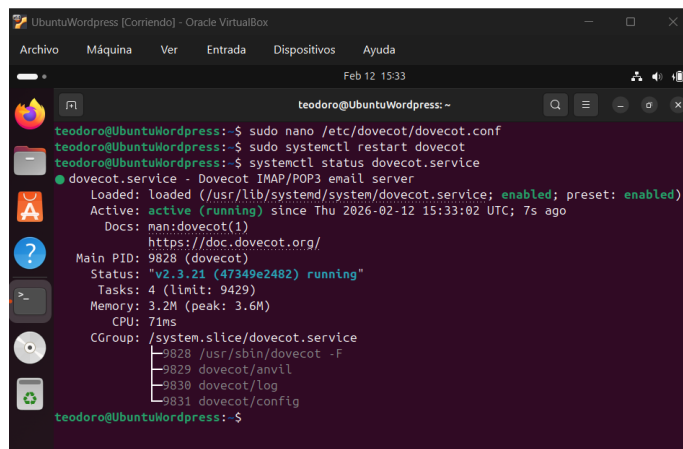


```
GNU nano 7.2 /etc/dovecot/conf.d/10-mail.conf
##
## Mailbox locations and namespaces
##
# Location for users' mailboxes. The default is empty, which means that Dovecot
# tries to find the mailboxes automatically. This won't work if the user
# doesn't yet have any mail, so you should explicitly tell Dovecot the full
# location.
#
# If you're using mbox, giving a path to the INBOX file (eg. /var/mail/%u)
# isn't enough. You'll also need to tell Dovecot where the other mailboxes are
# kept. This is called the "root mail directory", and it must be the first
# path given in the mail_location setting.
#
# There are a few special variables you can use, eg.:
#
# %u - username
# %n - user part in user@domain, same as %u if there's no domain
# %d - domain part in user@domain, empty if there's no domain
# %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
# mail_location = maildir:~/Maildir
# mail_location = mbox:~/mail:INBOX=/var/mail/%u
# mail_location = mbox:/var/mail/%d/%n/INDEX=/var/indexes/%d/%n/%n
#
# <doc/wiki/MailLocation.txt>
mail_location = maildir:~/Maildir

# If you need to set multiple mailbox locations or want to change default
# namespace settings, you can do it by defining namespace sections.
```

Figure 10: 10

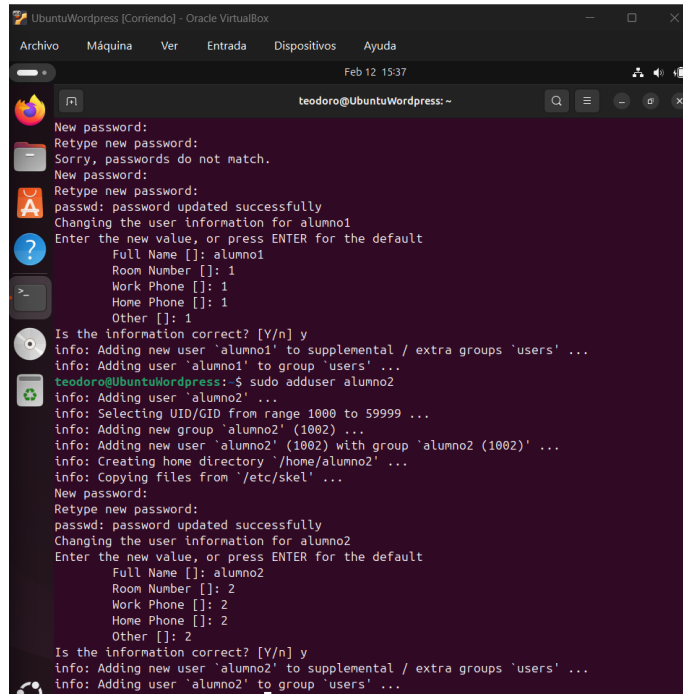
Y ahora reiniciamos el servicio de Dovecot:



```
teodoro@UbuntuWordPress:~$ sudo nano /etc/dovecot/dovecot.conf
teodoro@UbuntuWordPress:~$ sudo systemctl restart dovecot
teodoro@UbuntuWordPress:~$ systemctl status dovecot.service
● dovecot.service - Dovecot IMAP/POP3 email server
   Loaded: loaded (/usr/lib/systemd/system/dovecot.service; enabled; preset: enabled)
   Active: active (running) since Thu 2026-02-12 15:33:02 UTC; 7s ago
     Docs: man:dovecot(1)
           https://doc.dovecot.org/
   Main PID: 9828 (dovecot)
    Status: "v2.3.21 (47349e2482) running"
     Tasks: 4 (limit: 9429)
    Memory: 3.2M (peak: 3.6M)
       CPU: 71ms
    CGroup: /system.slice/dovecot.service
            └─9828 /usr/sbin/dovecot -F
              └─9829 dovecot/anvil
                └─9830 dovecot/log
                  └─9831 dovecot/config
teodoro@UbuntuWordPress:~$
```

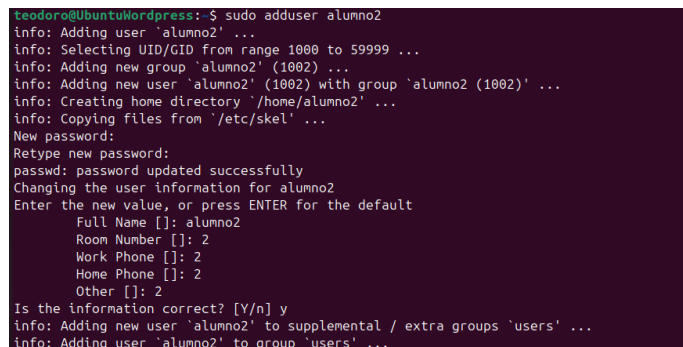
Figure 11: 11

Creamos nuevos usuarios (usuario1, usuario2), para comprobar el servicio (con contraseña llerma!-1234).



```
teodoro@UbuntuWordPress: ~$ sudo adduser alumno1
New password:
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for alumno1
Enter the new value, or press ENTER for the default
  Full Name []: alumno1
    Room Number []: 1
    Work Phone []: 1
    Home Phone []: 1
      Other []: 1
Is the information correct? [Y/n] y
info: Adding new user 'alumno1' to supplemental / extra groups 'users' ...
info: Adding user 'alumno1' to group 'users' ...
teodoro@UbuntuWordPress: ~$ sudo adduser alumno2
info: Adding user 'alumno2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'alumno2' (1002) ...
info: Adding new user 'alumno2' (1002) with group 'alumno2 (1002)' ...
info: Creating home directory '/home/alumno2' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for alumno2
Enter the new value, or press ENTER for the default
  Full Name []: alumno2
    Room Number []: 2
    Work Phone []: 2
    Home Phone []: 2
      Other []: 2
Is the information correct? [Y/n] y
info: Adding new user 'alumno2' to supplemental / extra groups 'users' ...
info: Adding user 'alumno2' to group 'users' ...
```

Figure 12: 12



```
teodoro@UbuntuWordPress: ~$ sudo adduser alumno2
info: Adding user 'alumno2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'alumno2' (1002) ...
info: Adding new user 'alumno2' (1002) with group 'alumno2 (1002)' ...
info: Creating home directory '/home/alumno2' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for alumno2
Enter the new value, or press ENTER for the default
  Full Name []: alumno2
    Room Number []: 2
    Work Phone []: 2
    Home Phone []: 2
      Other []: 2
Is the information correct? [Y/n] y
info: Adding new user 'alumno2' to supplemental / extra groups 'users' ...
info: Adding user 'alumno2' to group 'users' ...
```

Figure 13: 13

Ahora iniciamos sesión con uno de los alumnos (alumno1) Y abrimos el terminal de comandos, donde en-

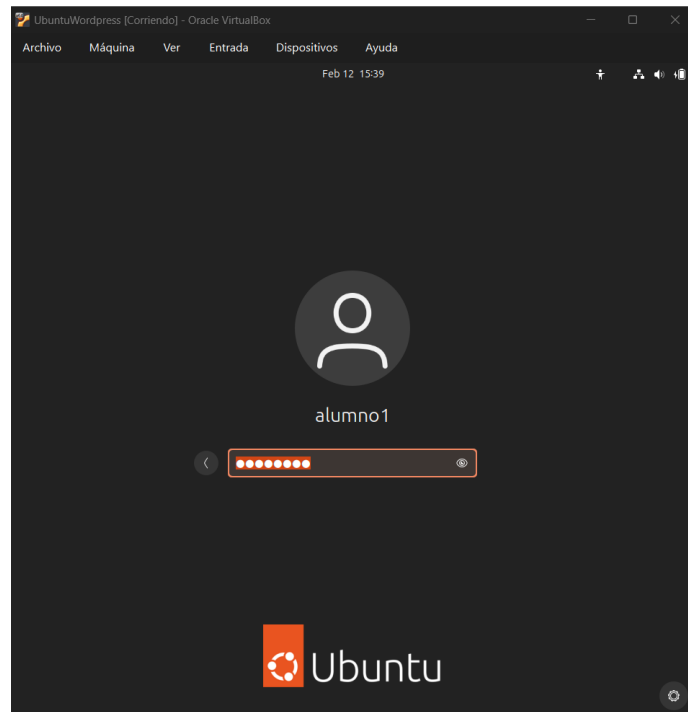


Figure 14: 14

viaremos un mensaje a alumno2 mediante lo siguiente:

```
echo "Hola, esto es una prueba" | mail -s "Prueba 1" alumno2@localhost
```

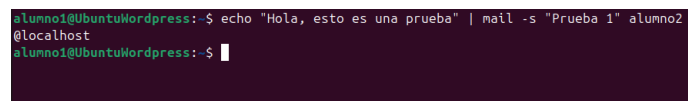


Figure 15: 15

Nuestro último paso sería leer el correo. Para ello puedes instalar un cliente ligero como mutt o configurar Thunderbird en tu máquina anfitriona apuntando a la IP de tu máquina virtual (Puerto 143, usuario alumno2, contraseña la que creaste).

2.4 Checklist de validación

Postfix acepta conexiones en puerto 25.

Dovecot acepta conexiones IMAP en puerto 143.

Se puede enviar correo entre usuarios locales.

Se puede leer correo con cliente IMAP.

Los logs muestran entrega exitosa (código 250).

2.5 Entregable

Documento Word o PDF con capturas de pantalla de:

1. Archivo `‘/etc/postfix/main.cf’` configurado.
2. Salida de `‘postqueue -p’` mostrando cola vacía.
3. Cliente de correo mostrando mensaje recibido.
4. Fragmento de `‘/var/log/mail.log’` con entrega exitosa.