

---

# Unidad 8: Correo electrónico

**Curso de Administración de Servidores GNU/Linux**  
**Centro de Formación Permanente**  
**Universidad de Sevilla**

Autores: Jorge Juan Chico y Enrique Ostúa 2010-2014.

Usted es libre de copiar, distribuir y comunicar públicamente la obra y de hacer obras derivadas bajo las condiciones de la licencia Attribution-Share alike de Creative Commons.

Puede consultar el texto completo de la licencia en <http://creativecommons.org/licenses/by-sa/3.0/>

## Configuración de red

---

- IP: 10.1.15.XXX
- Netmask: 255.255.252.0
- Gateway: 10.1.12.1
- Nombre ordenador: pc-XXX
- **Dominio: curso.linux**
- **Servidor DNS: 10.1.15.78**

# Contenidos

---

1. Elementos del sistema de correo
2. Modo de Operación
3. Configuración de clientes
4. POSTFIX: Configuración básica de un MTA
5. DOVECOT: Servicios POP e IMAP
6. Integración y Autenticación de salida SASL.
7. Otras opciones de configuración
  1. Escuchar en otro nº puerto
  2. Buzones mbox vs maildir
  3. Servicio antispam y antivirus
  4. Webmail
  5. Integración con LDAP o MySQL

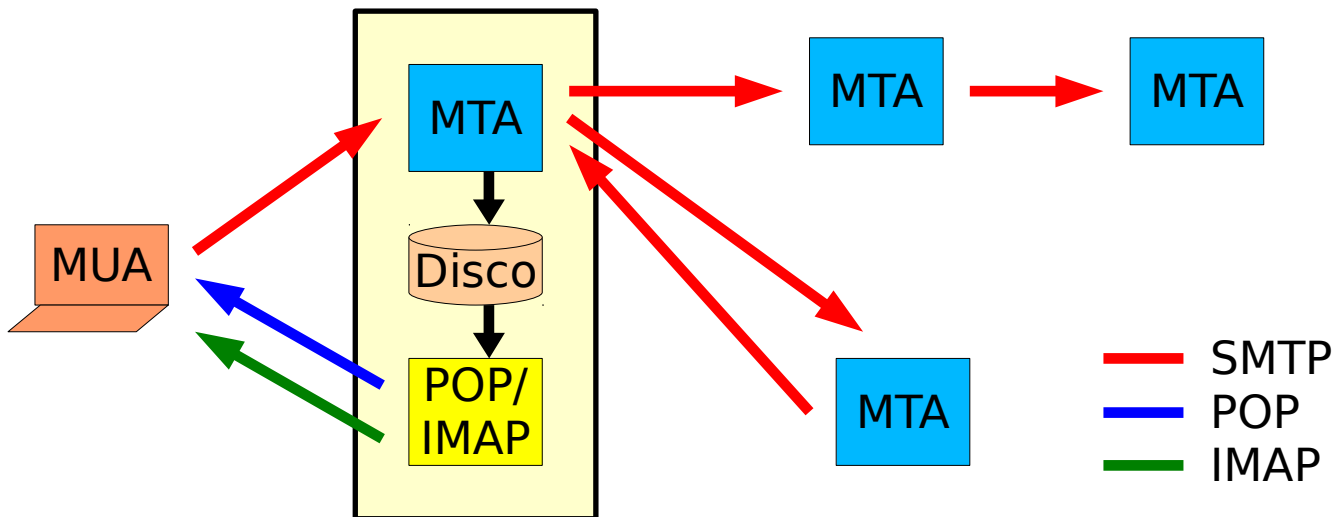
## Elementos del sistema de correo

---

- Servidor de nombres (DNS)
  - Indica qué ordenador (dirección IP) gestiona los buzones de un dominio.
- Agente de transporte de correo (MTA)
  - también “servidor de correo saliente”
  - recibe mensajes de correo para ser enviados a su destino
- Servidores POP/IMAP
  - permiten descargar el correo desde el servidor (MTA) donde se almacenan
- Agente de usuario de correo (MUA)
  - también “cliente de correo”
  - envía, descarga y muestra mensajes al usuario

# Operación del correo electrónico

---



# Operación del correo electrónico

---

- Reenvío (relay) de correo por parte del MTA
  - necesario controlar el reenvío indiscriminado para prevenir el spam
    - reenvío por rangos de IP o dominios
    - reenvío para usuarios autenticados
- Cifrado de las comunicaciones (SSL, TLS)
  - protege datos de usuario (usuario, clave)
  - protege contenido de mensajes
- Coordinación con DNS
  - el dominio de correo debe estar en el DNS como nombre de host o entrada MX (**M**ail **eX**changer)
    - \$ host **-t MX** us.es

# Configuración de clientes

---

- Servidor de correo saliente (SMTP)
  - nombre/ip del MTA
  - puerto (*smtp 25/tcp, smtps 465/tcp*)
  - seguridad: **Ninguna**, SSL, **TLS**
  - autenticación: **Ninguna**, **PLAIN**, LOGIN, ...
- Servidor entrante (POP/IMAP)
  - nombre/ip del servidor POP/IMAP
  - puerto (*pop3 110, pop3s 995, imap 143, imaps 993*)
  - seguridad: ~~Ninguna~~, SSL, TLS
  - autenticación: **PLAIN**, LOGIN, ...

## POSTFIX: Configuración básica MTA

---

- Parámetros
  - Entrega directa o a través de un *smarthost*
  - Dominio para el que se gestiona el correo
  - Control del relay
  - Cifrado de las conexiones (TLS)
  - Puerto (estándar: 25)
- Ejemplo
  - Entrega directa: servidor de internet independiente
  - Dominio: nombre del ordenador
  - Relay para subred local
  - Sin cifrado
  - Puerto 25

# Configuración básica MTA

---

- MTA's disponibles en Ubuntu: **postfix**, exim, ...
  - Instalar y dejar configuración por defecto.
- Configuración de postfix. Asistente de configuración:  
**# dpkg-reconfigure -p low postfix**
  - Tipo: sitio de Internet
  - Nombre del sistema de correo: nombre del host
  - Recipiente de correo para superusuario: curso
  - Dominios de destino final: por defecto (debe incluir nombre del sistema de correo)
  - Transacciones síncronas: no
  - Reenvío de correo: añadir bloque 10.1.12.0/22 (opcional)
  - Límite de buzones de correo: elegir
  - Extensiones de dirección local: por defecto
  - Protocolos: por defecto (todos)

# Configuración básica MTA

---

- Comprobación MTA
  - Enviar/recibir **correo local** con mutt o mailx (formato mbox)
  - Comprobar /var/log/mail.\*
  - Comprobar buzones de correo en:
    - /var/mail o /var/spool/mail (mbox)
    - ~/Maildir/ (maildir)
  - Comprobar con clientes remotos o con telnet/netcat al puerto 25: “HELO pc-xxx” o “EHLO pc-xxx”; “QUIT”.
  - Comprobar envío con TLS (activo por defecto)
- Gestión de la **cola** de mensajes
  - \$ mailq | \$ postqueue -p : lista cola de mensajes
  - # postsuper: borra mensajes de la cola, etc.
    - Ej:# postsuper -d 7E7C03B02A

# Ejemplo Protocolo SMTP

---

```
ostua@kyke:~$ netcat localhost smtp
220 kyke ESMTP Postfix (Ubuntu)
ehlo kyke
250-kyke
250-SIZE 52428800
250-STARTTLS
250 HELP
mail from: ostua@dte.us.es
250 2.1.0 OK
rcpt to: destinatario@gmail.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
esto es una prueba
fin
.
250 2.0.0 Ok: queued as 2907E2202D2
quit
221 2.0.0 Bye
```

## Alias de correo local y .forward

---

- Podemos redirigir correos locales a uno o varios usuarios y/o emails externos.
- **/etc/aliases:**

```
postmaster: root
```

```
root: ostua ostua@dte.us.es
```

– Al hacer cambios hay que invocar “# newaliases”

- Fichero “**.forward**” en el HOME de un usuario (debe ser accesible en lectura por el usuario “postfix”)
- Ejemplo ~/.forward que reenvia el correo a 2 emails:

```
email1@gmail.com
```

```
email2@us.es
```

– Si se añade el propio usuario (sin @) se deja copia local también.

# DOVECOT: Servicios POP e IMAP

---

- **dovecot**: servidor con soporte POP e IMAP
  - # apt-get install dovecot-imapd dovecot-pop3d
- Configuración por defecto:
  - válida para la mayoría de los casos
  - protocolos: pop3, pop3s, imap, imaps
  - seguridad: TLS (pop3, imap) y SSL (pop3s, imaps)
  - autenticación: PLAIN
  - no permite conexiones remotas sin seguridad
  - IMAP: carpetas de correo en \$HOME/Mail

## Servicios POP e IMAP

---

- Archivo de configuración:
  - `/etc/dovecot/dovecot.conf` y `/etc/dovecot/conf.d`
  - extensos comentarios sobre las opciones
  - valores por defecto aparecen como comentarios
  - comando “doveconf”.
- Posibles cambios en la configuración
  - limitar protocolos a pop3 e imap (eliminar pop3s e imaps). Seguridad sigue disponible por TLS.
  - comprobar con “\$ doveconf protocols”
    - “protocols = imap pop3” en dovecot.conf
  - añadir autenticación tipo LOGIN (inicio de sesión): necesaria para algunas versiones de MS-Outlook(TM).
    - `auth default {`
    - `mechanisms = plain login`
    - ...

# Ejemplo Protocolo POP3

---

```
ostua@teclix:~$ netcat localhost pop3
+OK Dovecot ready.
user ostua
+OK
pass cursolinux
+OK Logged in.
list
+OK 10975 messages:
.....
10974 3016
10975 9049
.
retr 10881
+OK 852 octets
Delivery-date: Wed, 15 May 2013 07:53:49 +0200
...
dele 10881
+OK Marked to be deleted.
quit
+OK Logging out, messages deleted.
```

## Autenticación de salida

---

- Consiste en permitir relay en el MTA cuando el usuario se identifica con una contraseña.
- Mecanismo más flexible que el control por IP
- Configuración segura habitual
  - seguridad: TLS
  - autenticación: PLAIN
- El MTA necesita usar algún complemento que proporcione mecanismos de autenticación
- Configuración
  - configurar dovecot para que proporcione mecanismo de autenticación SASL para aplicaciones externas
  - configurar postfix para que use SASL proporcionado por dovecot



# Autenticación de salida

---

- Configuración de dovecot (dovecot.conf)

```
auth default {
    ...
    mechanisms = plain login
    ...
    socket listen {
        client {
            # Assuming the default Postfix $queue_directory setting
            path = /var/spool/postfix/private/auth
            mode = 0660
            # Assuming the default Postfix user and group
            user = postfix
            group = postfix
        }
    }
}
```

- Configuración de postfix (main.cf)

```
...
smtpd_sasl_type = dovecot
# Can be an absolute path, or relative to $queue_directory
smtpd_sasl_path = private/auth
# and the common settings to enable SASL:
smtpd_sasl_auth_enable = yes
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination
```

## Ubuntu: mail-stack-delivery

---

- Paquete **mail-stack-delivery**
  - # apt-get install mail-stack-delivery
- (Paquete **dovecot-postfix** en versiones anteriores)
- Proporcionan:
  - Postfix (SMTP)
  - Dovecot (POP3/POP3S + IMAP/IMAPS)
  - Integración postfix+dovecot
  - Formato maildir
  - Autenticación de salida SASL

# Otras opciones de configuración

---

- SMTP en puerto alternativo (ej: 10000+25)
  - /etc/postfix/master.cf

```
...
smtp      inet  n       -       -       -       -       smtpd
10025     inet  n       -       -       -       -       smtpd
...
```

- POP e IMAP en puertos alternativos (ej: 10000+x)
  - /etc/dovecot/dovecot.conf

```
...
protocol imap {
  listen = *:10143
  ssl_listen = *:10993
  ...
}

protocol pop3 {
  listen = *:10110
  ssl_listen = *:10995
  ...
}
```

## Maildir

---

- Buzones en formato Maildir (recomendado!)
  - Árbol de directorios “Maildir/” en el HOME, y cada email en un fichero diferente. Más escalable y menos posibilidades de corrupción.
  - /etc/postfix/main.cf
    - añadir “home\_mailbox = Maildir/”
    - comentar “# mail\_spool\_directory”
  - /etc/dovecot/dovecot.conf
    - mail\_location = maildir:~/Maildir

# mbox

---

- Buzones en formato mbox (el clásico)
  - Un fichero de buzón por usuario que contiene todos los emails. Poco escalable y posibilidad de corrupción!
  - /etc/postfix/main.cf
    - añadir “mail\_spool\_directory = /var/mail”
    - comentar “# home\_mailbox”
  - /etc/dovecot/dovecot.conf
    - mail\_location = mbox:~/mail:INBOX=/var/mail/%u

## Virtual domains

---

- Se pueden tener varios dominios virtuales usando el mismo servidor de correo.
- El servidor aceptará usuarios en varios dominios
  - [user1@domain1.com](#)
  - [user2@domain1.com](#)
  - [user3@domain2.com](#)
- Según queramos que los usuarios reciban correo en cualquiera de los dominios o no, la solución se implementará de forma distinta.

# Correo local o Virtual

---

- Postfix distingue entre 3 tipos de dominios:
  - Local domains: aquellos que son entregados a usuarios del sistema Linux
  - Virtual alias domains: alias con [user@domain1.com](#) , [user2@domain1.com](#), [user3@domain3.com](#), ...
  - Virtual mailbox domains: se recoge correo para dominios completos @domain1.com, @domain2.com
- Se pueden guardar los emails en carpetas con el “nombre de usuario” y el “dominio” para distinguirlos, cuando no existen los usuarios en el sistema.

# Antivirus y Antispam

---

- Hay que añadir en el MTA llamadas a los procesadores apropiados que comprueben el contenido del mensaje, lo modifiquen y decidan si sigue su curso o se borra.
- Los paquetes más populares:
  - Para virus tenemos **amavisd-new**
  - Para spam es **spamassassin**
-

# Webmail

---

- Son aplicaciones que se instalan en un servidor web y acceden al correo por IMAP(s), mostrando el mismo en un formato web.
- Algunos paquetes populares:
  - **squirrelmail**
  - **roundcube**

## Integración LDAP o mySQL

---

- La búsqueda de alias y dom.virtuales se pueden redirigir a un directorio LDAP o una tabla mySQL.
- Por ejemplo, mySQL, en main.cf:
  - alias\_maps = mysql:/etc/postfix/mysql-aliases.cf
- Que contendrá:
  - user = dbusuario
  - password = dbcontraseña
  - dbname = customer\_database
  - query = SELECT forw\_addr FROM mxaliases WHERE alias='%s' AND status='paid'
- Man 5 mysql\_table