

# 0



**IRONTEC**  
INTERNET Y SISTEMAS SOBRE GNU/LINUX

## Sistemas de Correo en GNU/Linux

### **Servidores de Correo con Filtros Antivirus y Antispam**



1 - 203

Iker Sagasti Markina  
<iker@irontec.com>

# O



## Sistemas de Correo en GNU/Linux

### **Contenido**

---

# Contenido

**IRONTEC**  
INTERNET Y SISTEMAS SOBRE GNU/LINUX

**2 - 203**

*Iker Sagasti Markina*  
<iker@irontec.com>



## Sistemas de Correo en GNU/Linux

### **Contenido**

---

- Introducción al correo electrónico
- Servidor de Correo Saliente: Postfix
- Servidor de Correo Entrante
  - IMAP: Courier-Imap
  - POP: Courier-Pop
- Interfaz para filtrar contenidos: Amavisd-new
  - Antivirus: Clamav
  - Antispam: SpamAssassin
- Gestión de Buzones de Usuario
  - Reparto: Courier-maildrop
  - Cliente: Mutt y Mozilla-Thunderbird

# 0



## Sistemas de Correo en GNU/Linux

### **Contenido**

---

- Monitorización del Servidor
  - Mailgraph y Couriergraph
  - Pflogsumm
- Gestión de listas de distribución: Mailman
- Servicio de Webmail: Squirrelmail
- Generación de certificados y CA: Openssl

1



Sistemas de Correo en GNU/Linux

## **Introducción**

---

# Introducción

**IRONTEC**  
INTERNET Y SISTEMAS SOBRE GNU/LINUX

**5 - 203**

*Iker Sagasti Markina*  
<iker@irontec.com>

# 1



## Sistemas de Correo en GNU/Linux

### **Contenido**

---

- Historia.
- Funcionamiento Correo Electrónico.
- Protocolo de envío de correos: SMTP.
- Protocolo de recepción de correos: IMAP y POP.
- Mailboxes: Mbox y Maildir.
- SPAM: Listas Negras.

# 1



## Sistemas de Correo en GNU/Linux

### **Historia – Acontecimientos [I]**

---

- **1514:** Correo Mayor de las Indias. Servicio entre las colonias americanas y España.
- **1844:** Samuel F. Morse primer telegrama de la historia. “What hath God wrought!”
- **1876:** Antonio Meucci utiliza por primera vez teléfono. “Mr Watson, come here, I want u”
- **1971:** Ray Tomlinson primer e-mail a través de red distribuida: ARPANET. “Testing 1-2-3”
- **1972:** Se escoge el símbolo @ para denotar “en”.
- **1975:** Primera lista de correo. “MsgGroup”.
- **1976:** Reina Isabel II primer jefe de estado en enviar email.
- **1977:** RFC733 y RFC822. Especificaciones correo electrónico.

# 1



## Sistemas de Correo en GNU/Linux

### **Historia – Acontecimientos [II]**

- **1978:** DEC envía el primer correo comercial no solicitado. “DECSYSTEM-20 FAMILY”.
- **1979:** Kevin MacKenzie propone romper el hielo. ;-).
- **1982:** Simple Mail Transfer Protocol (SMTP).
- **1985:** Cadenas de email.
- **1988:** Roberto Morris envía primer virus de tipo gusano.
- **1989:** Primer intercambio de correo electrónico entre proveedores comerciales de correo
- **1991:** Linus presenta el SO Linux a la comunidad a través de email.
- **1994:** Primer hoax o virus social. “Good times”. Post Office Protocol (RFC 1725).
- **2003:** Alan Ralsky recibe de su propia medicina.

# 1



## Sistemas de Correo en GNU/Linux

### **Historia – Evolucion**

---

Coste:

- **1850:** Telegrama 20p.
  - 18,44 francos (varios jornales)
- **1875:** Telegrama 20p.
  - 0,50 francos (1 kg. pan)
- **1976:** Email
  - 4 dólares
- **2002:** SPAM. Pérdidas en empresas europeas
  - 2.500 millones de euros :-0

# 1



## Sistemas de Correo en GNU/Linux

### **Historia – Evolucion**

---

Tiempo

- **Palomas Mensajeras**
  - 200 km: 2 horas
- **Telégrafo Óptico**
  - 5.000 km: 2 minutos
- **Email**
  - 40.000 km: 2 segundos

# 1



## Sistemas de Correo en GNU/Linux

### **Historia – Evolucion**

---

#### SPAM

- **1978**
  - $\approx 0\%$
- **2001**
  - 10%
- **2004**
  - 60%

# 1



## Sistemas de Correo en GNU/Linux

### **Historia – Evolucion**

---

#### Virus

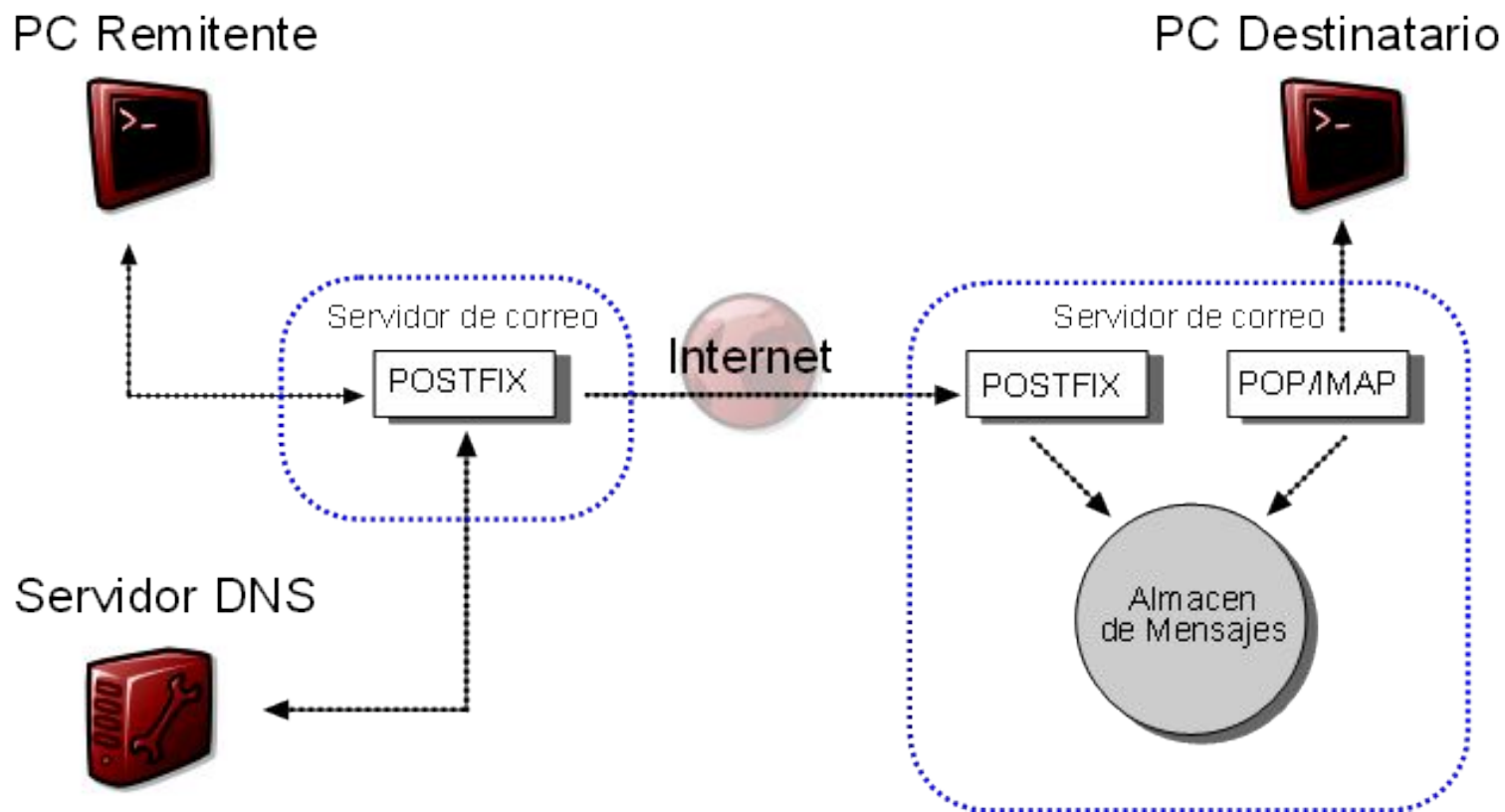
- **1988**
  - 3 horas – 10% de los servidores infectados
- **2003**
  - SQL Slammer
  - 3 horas – 125.000 equipos (mayoria en 5 primeros minutos)

# 1



## Sistemas de Correo en GNU/Linux

### Correo – Diagrama



# 1



## Sistemas de Correo en GNU/Linux

### Correo – Formato

---

- RFC 822. Nuevo estandar: RFC 2822

```
Return-Path: <txipi@txipinet.com>
X-Original-To: aktor@aktornet.ath.cx
Delivered-To: aktor@aktornet.ath.cx
Received: from txipinet.com (unknown [213.96.147.10])
  by aktornet.ath.cx (Postfix) with ESMTTP id 73E70B99F
  for <aktor@aktornet.ath.cx>; Mon, 26 Jul 2002 19:44:03
+0200 (CEST)
Received: by txipinet.com (Postfix, from userid 33)
  id 7517289914; Mon, 26 Jul 2002 19:40:34 +0200 (CEST)
From: txipi <txipi@txipinet.com>
To: aktor <aktor@aktornet.ath.cx>
Subject: Bilbowireless
X-Mailer: PHP/4.1.2
Message-Id: <20040726174650.CFE7B301CC@txipinet.com>
Date: Mon, 26 Jul 2002 19:46:50 +0200 (CEST)
```

Hola aktor,

Nos enlazamos?

--

Agur

txipi

# 1



## Sistemas de Correo en GNU/Linux

### **SMTP (Simple Mail Transfer Protocol)**

---

- Protocolo estandar para enviar correos entre servidores.
- Protocolo simple pero muy inseguro. Cabeceras spoofeables. SPAM.
- Requiere de un servidor DNS que resuelva el host MX o A del destinatario.
- Solo soporta caracteres ascii de 7 bits. ¿ñ?
- La gran mayoría de los MUA envían correo a los MTA por medio de SMTP.

# 1



## Sistemas de Correo en GNU/Linux

### **SMTP (Simple Mail Transfer Protocol)**

---

- Diversos servidores SMTP: Postfix, Qmail, Exim, Sendmail, Microsoft Exchange...
- Puertos well-known definidos: SMTP 25/tcp y SSMTP 465/tcp.
- Creado en 1982. RFC 821. Múltiples RFC's.



## Sistemas de Correo en GNU/Linux

### **SMTP – Definiciones**

---

#### **HELO / EHLO**

- El servidor emisor comunica al receptor quien es
  - Facilmente “spoofeable”
  - A menudo mal configurado

#### **Sender**

- Dirección del emisor

**MAIL FROM: <iker@irontec.com>**

- No confundir con la cabecera From:

#### **Recipient**

- Dirección del destinatario

**RCPT TO: <aktor@aktornet.ath.cx>**

- No confundir con las cabeceras To: y Cc:

#### **Client**

- IP de la máquina que envía el correo

# 1



## Sistemas de Correo en GNU/Linux

### **SMTP – Secuencia de Comandos Protocolo**

```
$ telnet aktornet.ath.cx 25
Trying 80.35.230.140...
Connected to Asterix.
Escape character is '^]'.
220 aktornet.ath.cx ESMTP Postfix
helo ironmail.irontec.com
250 aktornet.ath.cx
mail from:<iker@irontec.com>
250 Ok
rcpt to:<aktor@aktornet.ath.cx>
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
From: Iker Sagasti Markina <iker@irontec.com>
Subject: Esto es el asunto de un correo

Esto es el cuerpo de un correo
.
250 Ok: queued as 4F979B2D3
quit
221 Bye
Connection closed by foreign host.
```

# 1



## Sistemas de Correo en GNU/Linux

### **SMTP – Open Relay**

---

```
$ telnet aktornet.ath.cx 25
Trying 80.35.230.140...
Connected to Asterix.
Escape character is '^]'.
220 aktornet.ath.cx ESMTP Postfix
helo mail.irontec.com
250 aktornet.ath.cx
mail from:<iker@irontec.com>
250 Ok
rcpt to:<aktor@enpresadigitala.com>
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Esto puede ser un spam. No seas un open-relay o
aparecerás en listas RBL.
.
250 Ok: queued as 4F979B2D3
quit
221 Bye
Connection closed by foreign host.
```

# 1



## Sistemas de Correo en GNU/Linux

### **ESMTP (Enhanced Simple Mail Transfer Protocol)**

- Extensión del protocolo SMTP para adaptarse a las nuevas necesidades.
- Varias extensiones: 8BITMIME, DSN, STARTTLS, AUTH ...
- Permiten características adicionales como: reducir ancho de banda, reducir la latencia, recuperación mejorada de errores.
- Para iniciar una conexión ESMTP se utiliza el comando EHLO.
- RFC 1869.

# 1



## Sistemas de Correo en GNU/Linux

### **ESMTP – Secuencia Comandos Protocolo**

```
$ telnet aktornet.ath.cx 25
Trying 80.35.230.140...
Connected to Asterix.
Escape character is '^]'.
220 aktornet.ath.cx ESMTP Postfix
ehlo mail.irontec.com
250-aktornet.ath.cx
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250 8BITMIME
mail from: <iker@irontec.com>
250 Ok
rcpt to: <aktor@aktornet.ath.cx>
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
```

# 1



## Sistemas de Correo en GNU/Linux

### **MIME (Multiple Internet Mail Extensions)**

- Extensiones del Correo de Internet para Múltiples propósitos. Caracteres ascii de 8 bits.
- Define la representación estándar para cuerpos de correos complejos.
- Aparece como solución a:
  - Codificación de caracteres en diferentes idiomas. ñ (0xf1), Ñ (0xd1).
  - Contenido binario de 8 bits como: imágenes, sonidos, programas...

# 1



## Sistemas de Correo en GNU/Linux

### **MIME (Multiple Internet Mail Extensions)**

- La transformación de 7 a 8 bits la realiza el MUA habitualmente.
- Para codificar datos binarios se utiliza el formato base64.  $\approx$  33% más de tamaño.
- Cabeceras para definir el tipo de contenido MIME.

# 1



## Sistemas de Correo en GNU/Linux

### MIME - Ejemplo

```
Mime-Version: 1.0
Content-Type: multipart/mixed;

boundary="Multipart=_Tue__27_Jul_2004_01_26_41_+0200_G2cYEnhBTt8gwhnt"

--Multipart=_Tue__27_Jul_2004_01_26_41_+0200_G2cYEnhBTt8gwhnt
Content-Type: application/x-gtar;
  name="scripts.iptables.tgz"
Content-Disposition: attachment;
  filename="scripts.iptables.tgz"
Content-Transfer-Encoding: base64

H4sIAB2TBUEAA+1cX0/bSBDnlUh8hwGqNkiE2E5Mr1Q9yQVzRBdILgG16qmqlngBU8freh
3anvpl
+3gP9x1u1n+C49hJCCGQ1oOE7d31zOzO7sxxZw2865qOx8srD0gSUK1VxVWuqVL8GtGKLO
FPRZYr
[...]
Dm8Lz7RVKMQ+OR+87LjsgnLh0q2phCvnd38/FD+a8RZcBmgH/Vg32PSkSS8k98tTvSsk/w
xOI6ec
csopp5xyWmr6H+b3+QoAUAAA

--Multipart=_Tue__27_Jul_2004_01_26_41_+0200_G2cYEnhBTt8gwhnt--
```

# 1



Sistemas de Correo en GNU/Linux

## **Introducción – Recepcion Correo**

---

# Introducción Recepcion Correo

25 - 203

*Iker Sagasti Markina*  
<iker@irontec.com>

# 1



## Sistemas de Correo en GNU/Linux

### **POP (Post Office Protocol)**

---

- Protocolo de recepción de correo.
- Diseñado para acceder a los correos de modo off-line. Clientes estáticos y sin conexión.
- Poco pesado para la máquina servidora. Conexión, descarga y desconexión.
- Protocolo simple: 13 comandos que pueden responder con +OK o -ERR.
- Comportamiento defecto: descargar los mensajes y borrarlos del servidor.
- Puetos well-known definidos: POP3 110/tcp y POP3S 995/tcp.

# 1



## Sistemas de Correo en GNU/Linux

### **POP – Secuencia Comando Protocolo**

---

```
$ telnet mail.ironotec.com 110
Trying 82.194.66.125...
Connected to mail.ironotec.com.
Escape character is '^]'.
+OK POP3 mail [cpop 16.2] at [82.194.66.125]
user iker@ironotec.com
+OK Need a password
pass *****
+OK You have 509 messages totaling 34295635 octets
from /home/ironwebs/mail/ironotec.com/iker/inbox
(full load - partial cache outdated/corrupted v0)
stat
+OK 509 34295053
Tralara
-ERR Command not implemented
```

# 1



## Sistemas de Correo en GNU/Linux

### **IMAP (Internet Message Access Protocol)**

- Protocolo de recepción de correos.
- Método acceso correo almacenados en almacén de correo remoto como si fuese local.
- Mensajes almacenados pueden ser accedidos de múltiples puntos sin moverlos.
- Protocolo soporta crear, modificar y/o eliminar buzones.

# 1



## Sistemas de Correo en GNU/Linux

### **IMAP (Internet Message Access Protocol)**

- Ofrece soporte para diferentes modos de acceso: online, offline, desconectado.
- Protocolo complejo: 24 comandos, 5 respuestas(OK, NO, BAD, PREAUTH, BYE)
- Puertos well-known definidos: IMAP 143/tcp y IMAPS 993/tcp.
- Creado en 1986. Univ. Stanford. Múltiples RFC's. Actual: RFC 3501. Version 4.

# 1



## Sistemas de Correo en GNU/Linux

# IMAP – Secuencia Comandos Protocolo

```
$ telnet mail.irontec.com 143
Trying 82.194.66.125...
Connected to mail.irontec.com.
Escape character is '^]'.
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=LOGIN]
mail.irontec.com I MAP4rev1 2003.339-cpanel at Tue, 27 Jul 2004
03:38:14 +0200 (CEST)
1 CAPABILITY
* CAPABILITY IMAP4REV1 IDLE NAMESPACE MAILBOX-REFERRALS BINARY
UNSELECT SCAN SORT T THREAD=REFERENCES
THREAD=ORDEREDSUBJECT MULTIAPPEND LOGIN-REFERRALS AUTH=LOGIN
1 OK CAPABILITY completed
2 LOGIN iker@irontec.com *****
2 OK [CAPABILITY IMAP4REV1 IDLE NAMESPACE MAILBOX-REFERRALS
BINARY UNSELECT SCAN SORT THREAD=REFERENCES
THREAD=ORDEREDSUBJECT MULTIAPPEND] User iker@irontec.com
authenticated
3 NAMESPACE
* NAMESPACE ((" " "/")("#mhinbox" NIL)("mh/" "/")) ((" " "/"))
(("shared/" "/") ("ftp/" "/")("#news." ".")("#public/"
"/"))
3 OK NAMESPACE completed
SELECT INBOX.Sent
SELECT BAD Command unrecognized: INBOX.SENT
4 SELECT INBOX.Sent
* 1 EXISTS
* 0 RECENT
```

# 1



## Sistemas de Correo en GNU/Linux

### **IMAP vs POP**

---

#### Ventajas POP

- Protocolo muy simple. Fácil implementación.
- Actualmente hay más clientes que lo soportan.
- Consume menos recursos de la máquina servidora.

# 1



## Sistemas de Correo en GNU/Linux

### **IMAP vs POP**

---

#### Ventajas IMAP

- Puede manipular correos con distintos flags. Definibles por usuario.
- Puede acceder y manipular múltiples buzones.
- Puede almacenar correos tan bien como los recoge.
- Permite actualizaciones concurrentes y acceso a buzones compartidos.
- Diseñado para optimizar el acceso online, especialmente en accesos de baja velocidad.

1



Sistemas de Correo en GNU/Linux

## **Introducción – Mailbox**

---

# Introducción Buzones (Mailbox)

**IRONTEC**  
INTERNET Y SISTEMAS SOBRE GNU/LINUX

**33 - 203**

*Iker Sagasti Markina*  
<iker@irontec.com>



## Sistemas de Correo en GNU/Linux

### **Mailbox – mbox**

- Es el método tradicional de almacenar correos en servidores tipo UNIX.
- Los correos según van llegando se van concatenando en un único archivo.
- Para indicar fin y comienzo de mail:

- Cada correo empieza por **From:**

```
From aktor@aktornet.ath.cx Fri Feb 27 09:27:55 2004
```

- Y acaba por línea en blanco

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA # fin de archivo adjunto
-----=NEOMAIL_ATT_0.0743188935603065-- # fin de indicador adjunto
# Línea en blanco
From gorka@irontec.com Fri Feb 27 11:56:54 2004 # From: sig. mail
```

# 1



## Sistemas de Correo en GNU/Linux

### **Mailbox – mbox**

---

- Solo un proceso puede abrir el archivo mbox en modo lectura/escritura.
- Acceso concurrente requiere mecanismo de bloqueo.
- Durante la actualización del archivo mbox, todo el resto deben esperar.
- Por defecto el archivo es:
  - `/var/spool/mail/usuario`

# 1



## Sistemas de Correo en GNU/Linux

### **Mailbox – Maildir**

---

- Implementados inicialmente por el servidor Qmail para mejorar los mbox.
- Cada mensaje en un archivo individual.
- Mensaje en formato RFC 822.
  - Comienza con la cabecera Return-Path:
  - Seguido de la cabecera Delibered-To:  

```
Return-Path: <ironotec-bounces@aktornet.ath.cx>  
Delivered-To: aktor@aktornet.ath.cx  
Received: from aktornet.ath.cx (localhost [127.0.0.1])  
by AsteriX (Postfix) with ESMTTP  
id 9D81A2EAAD; Mon, 12 Jan 2004 21:48:47 +0100 (CET)
```
  - No puede acabar con línea en blanco.
- No es necesario bloquear los correos.



## Sistemas de Correo en GNU/Linux

### **Mailbox – Maildir**

---

- Hay un procedimiento definido de añadir nuevos correos al maildir.
- Un maildir se compone por 3 subdirectorios: tmp, cur, new.
- Existe una manera definida para nombrar a cada archivo.

```
1090878520.M967905P7992V0000000000000803I0001806F_0.AsteriX,S=2541  
1090878520.M967905P7992V0000000000000803I0001806F_0.AsteriX,S=2541:2,FS
```

```
new: time.MusecPpidVdevIino.host,S=cnt  
cur: time.MusecPpidVdevIino.host,S=cnt:2,info
```

cnt: tamaño de archivo. Sirve para optimizar el trabajo con cuotas.

info: estado del mail. 0 ó + flags. Orden alfabético.

F: marcado, R: Replied-To, T: Trashed, D: Draft, S: Seen

- Múltiples procesos pueden acceder al mismo tiempo a los maildirs

# 1



## Sistemas de Correo en GNU/Linux

### **Mailbox – Maildir**

---

#### Maildirmake

- Comando para crear maildirs.
- Crea automáticamente los 3 directorios:
  - new
  - cur
  - tmp
- Sintaxis

```
$ maildirmake [opciones] maildir
```



## Sistemas de Correo en GNU/Linux

### **Mailbox – Maildir**

---

#### Ejemplo

- Indicamos la cuota a aplicar sobre el maildir.

```
maildirmake -q cuota
```

- Crea un maildir “compatible”. Diferentes permisos.

```
maildirmake -S
```

- No crea un maildir, sino una carpeta dentro del maildir.

```
maildirmake -f folder:
```

```
~$ maldirmake -q 5000000S,1000C ./Maildir/
```

# 1



## Sistemas de Correo en GNU/Linux

### **Mailbox – mbox vs Maildir**

---

- Maildir lo soportan menos MUA's que mbox.
- Mbox muy poco óptimo para mailboxes grandes.
- Maildir, al ser múltiples archivos, suele ocupar más espacio en disco. Cluster Size.
- Maildir trabaja muy bien con NFS, que tiene grandes problemas históricos con bloqueos.
- `apt-get install mb2md ; -P`
- Todo lo anterior mencionado ;-)

# 1



## Sistemas de Correo en GNU/Linux

### **SPAM**

---

- Mensajes de correo comerciales no solicitados. También conocido como UBE o UCE.
- Debido a servidores de correo mal configurados, gusandos que infectan ordenadores, contraseñas de correo robadas...
- RBL: Realtime Blackhole List
- <http://rbls.org/>
  - Comprobar si una IP está en alguna lista de negra.

# 1



## Sistemas de Correo en GNU/Linux

### **SPAM – Terminos**

---

- Todo software antispam se puede equivocar
  - Falsos Negativos
    - Cuando el software antispam no es capaz de detectar un correo no solicitado.
  - Falsos Positivos
    - Son los más graves.
    - Cuando un correo legítimo es clasificado como spam.
- Un buen software antispam es el que no tiene falsos positivos y muy pocos falsos negativos.

# 1



## Sistemas de Correo en GNU/Linux

### **SPAM – DNS BlockList**

---

- DNS BlockList (DNSbl)
  - Comprueba la IP del cliente.
  - Hay que tener cuidado con las listas.
    - Si no está actualizada puede provocar perdidas
    - Dificil seguir un criterio “justo”
  - Listas recomendadas a fecha 01/01/05

[cbl.abuseat.org](http://cbl.abuseat.org)

[dul.dnsbl.sorbs.net](http://dul.dnsbl.sorbs.net)

[list.dsbl.org](http://list.dsbl.org)

[opm.blitzed.org](http://opm.blitzed.org)

[relays.ordb.org](http://relays.ordb.org)

[sbl.spamhaus.org](http://sbl.spamhaus.org)

[xbl.spamhaus.org](http://xbl.spamhaus.org)

# 1



## Sistemas de Correo en GNU/Linux

### **SPAM – Right-Hand Side BlockList**

---

- Right-Hand Side BlockList (RHSbl)
  - Comprueba el host y nombre de dominio
  - Listas recomendadas a fecha 01/01/05

[blackhole.securitysage.com](http://blackhole.securitysage.com)

[rhsbl.sorbs.net](http://rhsbl.sorbs.net)

1



Sistemas de Correo en GNU/Linux

## **Introducción**

---

Fin Introducción

# 2



Sistemas de Correo en GNU/Linux

## **Integración de Servicios**

---

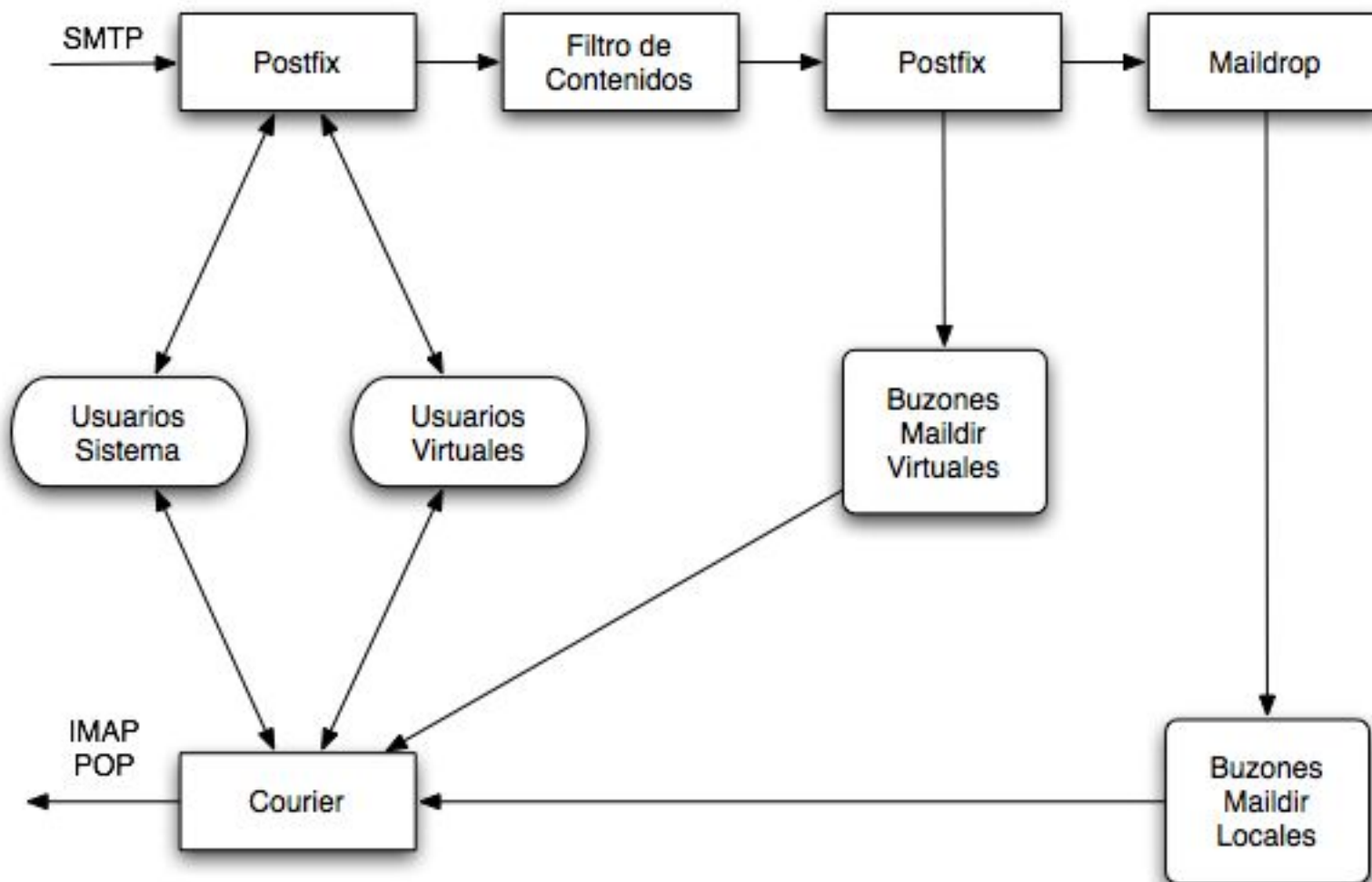
# Integración de Servicios Sistema Correo

# 2



## Sistemas de Correo en GNU/Linux

### Integración de Servicios



# 2

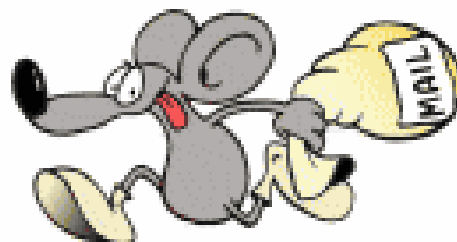


## Sistemas de Correo en GNU/Linux

### **Postfix**

---

# Postfix (SMTP Server)



**POSTFIX**

<http://www.postfix.org>

# 2



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Servidor de correo que funciona sobre sistemas tipo UNIX.
- Su intención fue la de sustituir a sendmail. Compatible para el resto de aplicaciones.
- Arquitectura y diseño muy modular.
- Fácil de administrar y configurar.
- Muy rápido. Fué diseñado pensando en el rendimiento. Evita saturar otros sistemas.
- Repartir correo de forma local puede repartir a almacén de correo o pasarlo a un MDA.
- Escrito en C. Wietse Zwietering Venema, IBM hacker.

# 2



## Sistemas de Correo en GNU/Linux

### **Características - Seguridad**

---

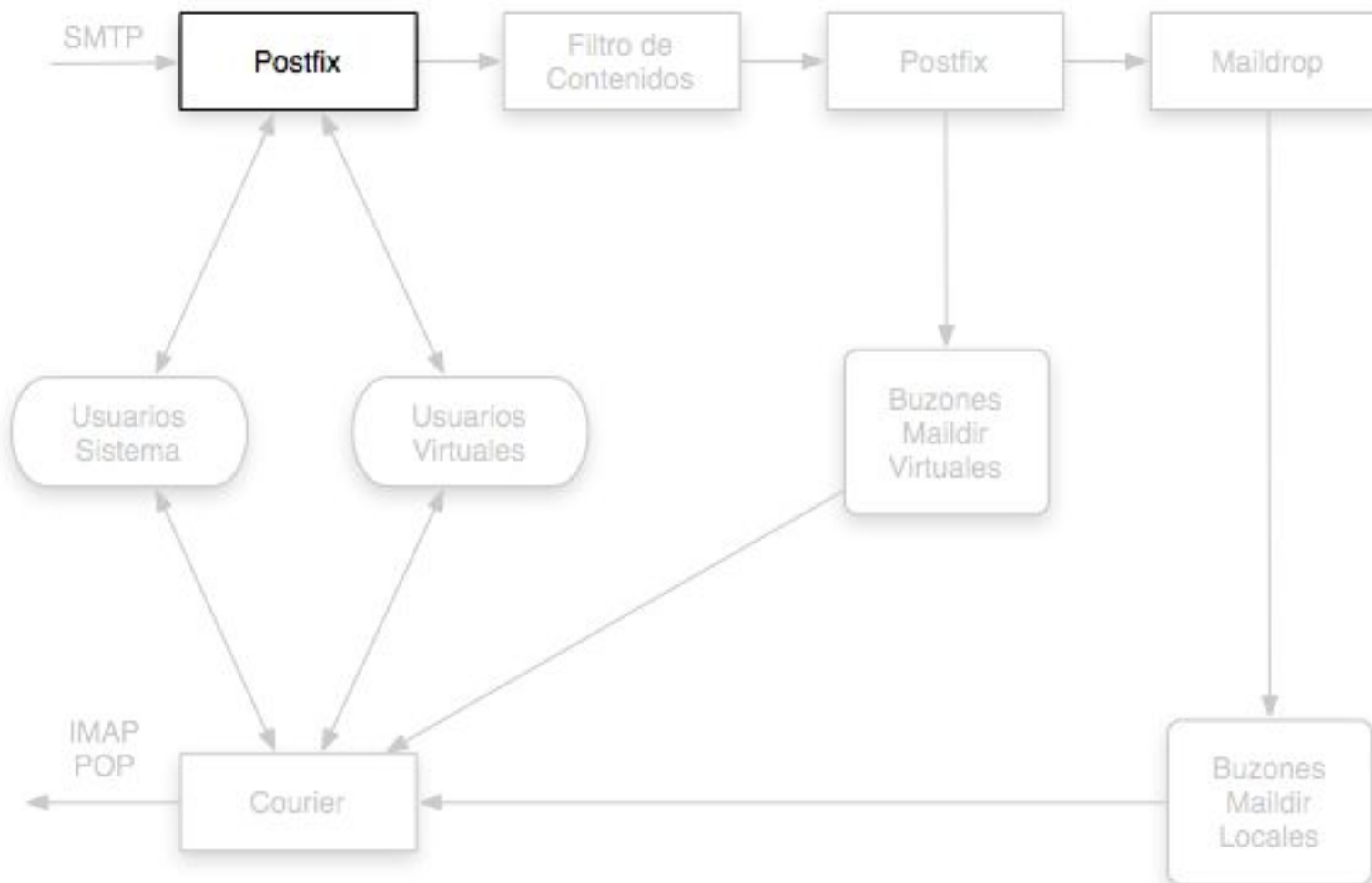
- Arquitectura modular: Cada proceso se ejecuta con privilegios mínimos para su tarea.
- Procesos que no se necesitan se deshabilitan: no se pueden explotar. Postfix GW.
- Los procesos se aíslan unos de otros. Muy poca comunicación entre procesos (IPC).
- Evita utilizar buffers de tamaño fijo, evitando que tengan éxito ataques buffer overflow
- Puede ejecutarse chrootado (/var/spool/postfix).
- Preparado para ataques DoS. Cantidad de memoria controlada.

# 2



## Sistemas de Correo en GNU/Linux

### Integración de Servicios

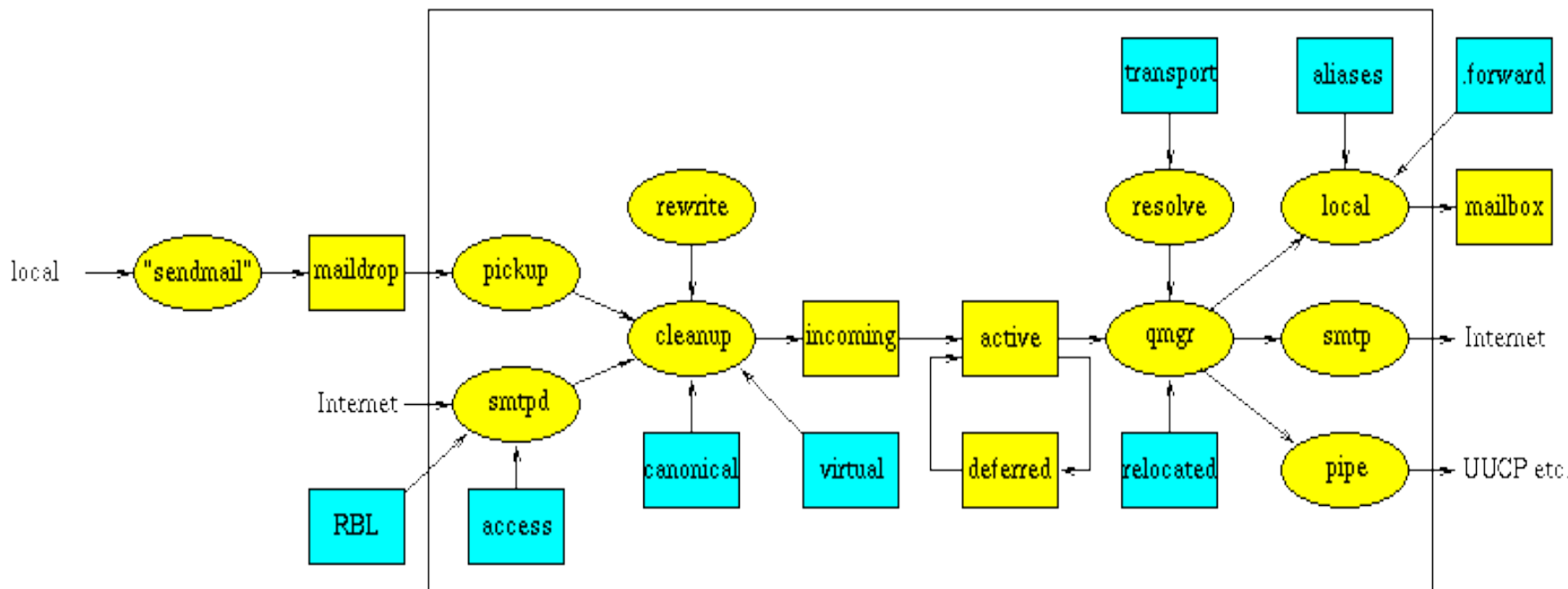


# 2



## Sistemas de Correo en GNU/Linux

### Arquitectura



# 2



## Sistemas de Correo en GNU/Linux

### **Arquitectura – Colas de Correo**

---

- Postfix basa su funcionamiento en cuatro colas: maildrop, incoming, active y deferred.
  - **Maildrop queue:** El correo que es generado y/o entregado localmente en el sistema es procesado por la cola Maildrop.
  - **Incoming queue:** Esta cola recibe correo de otros hosts, clientes o de la cola maildrop. Si llegan correos y Postfix no puede atenderlos se quedan esperando en esta cola.

# 2



## Sistemas de Correo en GNU/Linux

### **Arquitectura – Colas de Correo**

---

- **Active queue:** En esta cola están los mensajes en fase de encaminamiento. Espacio limitado.
- **Deferred queue:** En esta cola se almacenan los mensajes que no se han podido encaminar o están pendientes de reintentar su encaminamiento.

# 2



## Sistemas de Correo en GNU/Linux

### **Arquitectura – Procesos**

---

- Postfix gestiona las colas mediante procesos independientes.
  - **Pickup**: Recoge los correos que provienen de la cola maildrop y los pasa a cleanup.
  - **Smtpd**: Este proceso atiende, mediante protocolo SMTP, los correos de otros sistemas.
  - **Cleanup**: Analiza las cabeceras de los correos. Si ok, los deposita en la cola incoming.
  - **Qmgr**: Proceso encargado de tratar los correos que llegan a incoming, depositarlos en active y lanzar el proceso adecuado para su encaminamiento: local, smtp o pipe.

# 2



## Sistemas de Correo en GNU/Linux

### **Arquitectura – Procesos**

---

- **Local:** Proceso encargado de depositar el correo en el buzón.
- **Smtplib:** Proceso encargado de enviar el correo al host destino mediante protocolo SMTP.

# 2



## Sistemas de Correo en GNU/Linux

### **Arquitectura – Tablas**

---

- Las tablas, creadas por el administrador, sirven a los procesos para saber que tratamiento hay que dar a cada correo. Son 6 tablas aunque no son obligatorias.
  - **Access:** Sistemas a los que se acepta o rechaza los correos. La utiliza proceso smtpd.
  - **Aliases:** Define nombres alternativos a usuarios locales. Consulta el proceso local.
  - **Canonical:** Relación entre nombres alternativos y reales, locales o no. Proceso cleanup.

# 2



## Sistemas de Correo en GNU/Linux

### **Arquitectura – Tablas**

---

- **Relocated:** Devolver los mensajes que han cambiado de dirección. Proceso qmgr.
- **Transport:** Política de encaminamiento por dominios. Proceso trivial-rewrite.
- **Virtual:** Relación entre usuarios virtuales y reales. Proceso cleanup.

# 2



## Sistemas de Correo en GNU/Linux

### Arquitectura – Tablas

- Postfix soporta muy diversos soportes de backend para las tablas. Algunos de ellos:
  - **Hash:** El archivo generado es un hash. Disponible para sistemas con soporte BD db.
  - **MySQL:** Mapeo de las tablas de postfix a MySQL. Actualmente no es la mejor solución. Bastante sencilla de implementar.
  - **PostgreSQL:** Mapeo de las tablas de postfix a PostgreSQL. Dificultad mediana.
  - **LDAP:** Mapeo de las tablas de postfix a LDAP. Actualmente es la mejor solución aunque la más complicada de implementar, sobre todo contra Active Directory. No hay esquemas propios para LDAP.

# 2



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos el mta postfix.

```
# apt-get install postfix
```

- Instalamos comando para shell para enviar mails

```
# apt-get install mailx
```

# 2



## Sistemas de Correo en GNU/Linux

### **Configuración**

---

- En Debian, el instalador en ncurses nos ofrece varias opciones.
- Configuramos Postfix para que funcione como 'Internet Site' y configuramos nuestro dominio y los dominios para los cuales vamos a permitir recibir correo.
- Comprobamos que tenemos el demonio escuchando y los procesos ejecutándose.

# 2



## Sistemas de Correo en GNU/Linux

### Configuración

---

```
$ netstat -an | grep :25 | grep " LISTEN "  
tcp        0      0 0.0.0.0:25          0.0.0.0:*          LISTEN
```

```
$ ps aux  
root      1872  0.0  0.2 3004 1140 ? Ss  11:26  0:00 /usr/lib/postfix/master  
postfix  1876  0.0  0.2 3012 1104 ? S   11:26  0:00 pickup -l -t fifo -u -c  
postfix  1877  0.0  0.2 3044 1132 ? S   11:26  0:00 qmgr -l -t fifo -u -c
```

```
$ telnet localhost 25  
Trying 127.0.0.1...  
Connected to hq.irontec.com.  
Escape character is '^]'.  
220 hq.irontec.com ESMTP Postfix (Debian/GNU)
```

# 2



## Sistemas de Correo en GNU/Linux

### **Archivos de Configuración**

---

`main.cf` [ Debian: `/etc/postfix/main.cf` ]

- Archivo de configuración principal de postfix. La mayoría de los cambios aquí.

`master.cf` [ Debian: `/etc/postfix/master.cf` ]

- Archivo de configuración del demonio master. Servicios o transporte.

`aliases` [ Debian: `/etc/aliases` ]

- Archivo de alias. Equivalencia entre una dirección local ficticia y una dirección local real

# 2



## Sistemas de Correo en GNU/Linux

### **Archivos de Configuración**

---

#### `main.cf`

- Contiene unos pocos de todos los parámetros que controlan el comportamiento de Postfix.

`postconf -n`

- Los parámetros no especificados cogen su valor por defecto.

`postconf -d`

- Si no sabemos para que sirve un parámetro, mejor dejarlo con su valor por defecto.

# 2



## Sistemas de Correo en GNU/Linux

### Archivos de Configuración

`main.cf`

- Formato

`parámetro = valor`

- Línea en blanco, # comentario y espacios antes y después del = **no importan**.
- Cada parámetro 1 línea. Si siguiente línea empieza por ESPACIO, es que continúa.

```
smtpd_recipient_restrictions =  
    permit_mynetworks  
    permit_sasl_authenticated  
    reject_unauth_destination
```

- \$variable recibe el valor de otro parámetro.

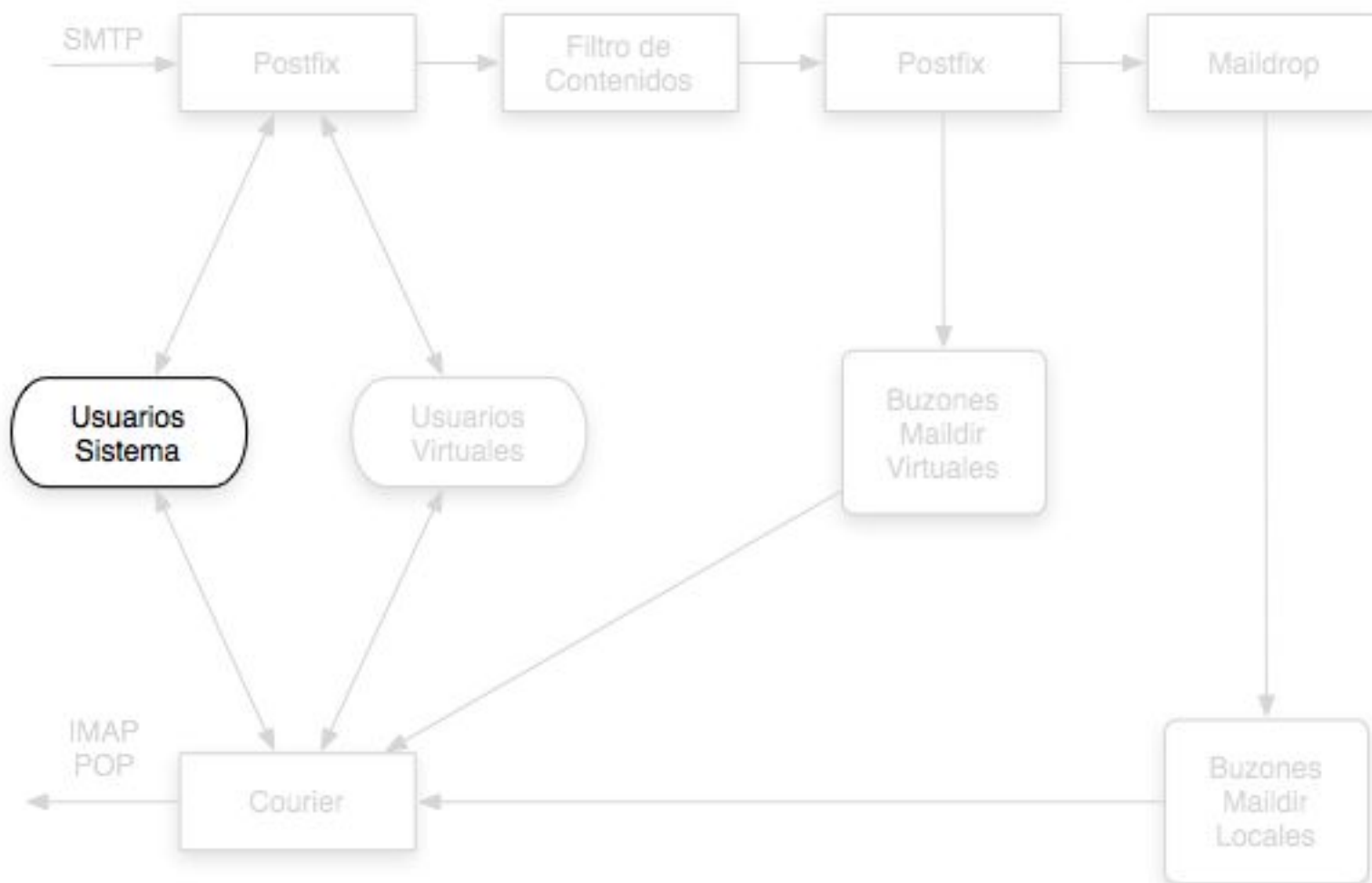
```
(mydestination = $myhostname)
```

# 2



## Sistemas de Correo en GNU/Linux

### Usuarios de Sistema



# 2



## Sistemas de Correo en GNU/Linux

### Archivos de Configuración – main.cf

```
# GID para Postfix para gestión de correo y de colas.  
# Grupo dedicado!  
setgid_group = postdrop  
  
# Texto que acompaña a la respuesta 220 de bienvenida  
smtpd_banner = $myhostname Microsoft ESMTTP MAIL Service ;)  
  
# Reescribir usuario@host a usuario@host.$mydomain. Esto es  
trabajo del MUA.  
append_dot_mydomain = no  
  
# Nombre de la máquina. FQDN.  
myhostname = mail.irontec.com.  
  
# Dominio principal  
mydomain = irontec.com  
  
# Dominio para añadir cuando mail solo indica usuario.  
# /etc/mailname = irontec.com  
myorigin = /etc/mailname
```

# 2



## Sistemas de Correo en GNU/Linux

### Archivos de Configuración – main.cf

```
# Dominios que voy a considerar como locales,  
# además localhost para programas.  
mydestination = irontec.com, localhost, localhost.$mydomain  
  
# Redes a las que permito hacer relay (enviar mails a  
# través este mta). ¿red local?  
mynetworks = 127.0.0.0/8  
  
# Directorios de trabajo de postfix.  
# En Debian no hacen falta.  
command_directory = /usr/sbin  
daemon_directory = /usr/lib/postfix  
program_directory = /usr/lib/postfix  
  
# Archivo para los alias.  
# Para actualizarlos comando newaliases.  
alias_maps = hash:/etc/aliases  
alias_database = hash:/etc/aliases
```

# 2



## Sistemas de Correo en GNU/Linux

### Archivos de Configuración – main.cf

```
# Sin límite de correo.  
# Si ponemos límite ojo con 33% tamaño MIME.  
mailbox_size_limit = 0  
  
# Delimitador de usuario @ y +.  
recipient_delimiter = +  
  
# Cambiamos el formato de los mailboxes a Maildir.  
# ~/Maildir/. IMPORTANTE / final  
home_mailbox = Maildir/
```

# 2



## Sistemas de Correo en GNU/Linux

### Archivos de Configuración – main.cf

- Algunas opciones orientativas. No tomarlas como definitivas.

```
# Directorios de trabajo de postfix. En Debian no hacen falta.
```

```
smtpd_helo_required = yes
```

```
# Restricciones al comando HELO/EHLO
```

```
# Hay mucho software mal configurado en Internet!!
```

```
smtpd_helo_restrictions = reject_invalid_hostname,  
reject_non_fqdn_hostname,  
reject_unknown_hostname,  
permit
```

```
# Forzar a que las direcciones cumplan el RFC 821
```

```
# mail from: <iker@irontec.com>
```

```
# rcpt to: <aktor@aktornet.ath.cx>
```

```
# Hay mucho software mal configurado en Internet!!
```

```
strict_rfc821_envelopes = yes
```

70 - 203

# 2



## Sistemas de Correo en GNU/Linux

### Archivos de Configuración – main.cf

```
# Comprobaciones antes de filtro de contenidos.  
Mejora rendimiento. Archivo existir.
```

```
mime_header_checks =  
    regexp:/etc/postfix/mime_header_checks
```

```
# Dominios virtuales con usuarios de sistema.  
Correo usuario@hq.irontec.com
```

```
virtual_alias_domains = hq.irontec.com  
virtual_alias_maps = hash:/etc/postfix/virtual
```

# 2



## Sistemas de Correo en GNU/Linux

### **Proceso de filtrado**

---

- Posftix permite realizar una serie de tareas de filtrado de acuerdo al siguiente orden:
  - Restricciones SMTPD
    - Estados de Restricción
      - `smtpd_client_restrictions`
      - `smtpd_helo_restrictions`
      - `smtpd_sender_restrictions`
      - `smtpd_recipient_restrictions`
      - `smtpd_data_restrictions`
    - Restricciones
    - Listas de acceso (mapas)
  - Comprobaciones de Cabeceras/Cuerpo del mail
  - Filtros de Contenidos

# 2



## Sistemas de Correo en GNU/Linux

### Comandos

---

- Algunos de los comandos más interesantes de Postfix:
  - **mailq**: lista el contenido de la cola de correo. Muestra el ID de cola, tamaño del correo, hora llegada, remitente y destinatario/s. Si no se ha podido entregar, muestra la razón. Enlace simbólico a sendmail (compatibilidad).
  - **newaliases**: actualiza la base de datos de los alias (/etc/aliases). Enlace simbólico a sendmail (compatibilidad).
  - **postsuper**: se encarga de realizar operaciones de mantenimiento

# 2



## Sistemas de Correo en GNU/Linux

### Comandos

---

- **postqueue**: comando que sirve de interfaz para la gestión de las colas.
- **postmap**: crea, actualiza o consulta una o más tablas de postfix.
- **postconf**: muestra los valores actuales de los parámetros de postfix.

# 2



## Sistemas de Correo en GNU/Linux

### **Registros**

---

`mail.log` [Debian: `/var/log/mail.log`]

- Fichero donde se registran todas las acciones del servidor postfix.

`mail.err` [Debian: `/var/log/mail.err`]

- Fichero donde se registran los errores que se producen en postfix.

`mail.info` [Debian: `/var/log/mail.info`]

- Fichero donde se registran todas las acciones del servidor postfix.

# 2



Sistemas de Correo en GNU/Linux

## **Postfix-TLS**

---

# Postfix-TLS

# 2



## Sistemas de Correo en GNU/Linux

### **Postfix-TLS**

---

- Transport Security Layer.
- Se construye a partir de SSL 3.0. Muy similar. A veces se le llama SSL 3.1
- Mejora la comunicación TCP añadiendo cifrado e integridad en los correos.
- No protege el contenido de los mails. Para ello PGP o S/MIME.
- Necesita un par de claves pública y privada. Autoridad Certificadora (CA).
- RFC 2487 y 3207. STARTTLS.
- En Postfix el parche lo hizo Kutz Jänicke.

# 2



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos el soporte para tls en postfix

```
# apt-get install postfix-tls
```

- Instalamos soporte para SSL (Secure Socket Layer)

```
# apt-get install openssl
```

- Creamos los certificados ssl.

```
# openssl req -new -x509 -nodes -out smtpd.pem  
-keyout smtpd.pem -days 3650
```

# 2



## Sistemas de Correo en GNU/Linux

### **Instalación - main.cf**

---

- Añadimos las siguientes líneas al main.cf

```
# tls
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/postfix/ssl/smtpd.pem
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.pem
smtpd_tls_CAfile = /etc/postfix/ssl/smtpd.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
```

# 2



Sistemas de Correo en GNU/Linux

## **Postfix-SASL**

---

# Postfix-SASL

# 2



## Sistemas de Correo en GNU/Linux

### **Postfix-SASL**

---

- Simple Authentication and Security Layer.
- Método de autenticación para protocolos orientados a la conexión.
- En sistemas de correo se utiliza para permitir hacer relay.
- Integrado en postfix. No es necesario utilizar librerías externas (Cyrus SASL Library).
- Permite distintos tipos de autenticación: ANONYMOUS, CRAM-MD5, DIGEST-MD5, GSSAPI, KERBEROS\_V4, OTP, PLAIN, or LOGIN.
- RFC 2222 y 2554. AUTH.

# 2



## Sistemas de Correo en GNU/Linux

### Instalación

- Instalamos soporte para sasl

```
# apt-get install postfix-tls
```

- Instalamos librerías para implementar la API de SASL

```
# apt-get install libsasl2 libsasl2-modules
```

- Instalamos herramientas para administración de usuarios

```
# apt-get install sasl2-bin
```

- Comprobamos que el demonio smtpd soporta sasl.

```
$ ldd /usr/lib/postfix/smtpd
```

```
libsasl2.so.2 => /usr/lib/libsasl2.so.2  
(0x401a6000)
```

82\_203

# 2



## Sistemas de Correo en GNU/Linux

### **Instalación - main.cf**

---

- Añadimos las siguientes líneas al main.cf

```
# sasl
smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = $myhostname
smtpd_recipient_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_unauth_destination
smtpd_sasl_security_options = noanonymous
```

# 2



## Sistemas de Correo en GNU/Linux

### **Instalación - pwcheck**

---

- Existen varios métodos gestionar las contraseñas.
  - **saslauth**: Demonio Cyrus SASL contra cuentas UNIX.
  - **auxprop**: Archivo independiente de usuarios y contraseñas.
- Escogemos auxprop en archivo smtpd.conf [ /etc/postfix/sasl/smtpd.conf ]
- Escogemos los métodos de autenticación que queremos permitir.

```
pwcheck_method: auxprop  
mech_list: plain login
```

# 2



## Sistemas de Correo en GNU/Linux

### **Instalación - pwcheck**

---

- Paramos el demonio de Cyrus saslauthd (/etc/default/saslauthd).

**START=no**

# 2



## Sistemas de Correo en GNU/Linux

### **Instalación - sasl2**

- Creamos las contraseñas para los usuarios.  
Contraseñas independientes de /etc/shadow

```
# saslpasswd2 -c -f /etc/sasl2 -u `postconf -h  
myhostname` aktor
```

Password:

Again (for verification):

```
# saslpasswd2 -d -f /etc/sasl2 -u `postconf -h  
myhostname` aktor
```

- Como Postfix está trabajando en modo chroot es necesario enlazar el archivo de contraseñas al correspondiente en el chroot.

```
# touch /var/spool/postfix/etc/sasl2  
# chown root.postfix /var/spool/postfix/etc/sasl2  
# chmod 640 /var/spool/postfix/etc/sasl2  
# cat /etc/sasl2 > /var/spool/postfix/etc/sasl2
```



# Courier IMAP (IMAP Server)

*Courier*  
**IMAP**

<http://www.courier-mta.org/imap/>

# 3



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Es un servidor que da acceso IMAP a los Maildirs. Está diseñado para ello.
- Servidor IMAP incluido en Courier Mail Server. Configurado en solitario puede trabajar con otros MTA's que reparten a Maildirs.
- Soporta varias extensiones al formato Maildir básico como carpetas y cuotas por soft.
- Incluye módulos de autenticación abstractos. Passwd, PAM, MySQL, PostgreSQL, LDAP...
- Ofrece IMAP sobre SSL. Soporte IPv6.

# 3



## Sistemas de Correo en GNU/Linux

### **Características**

---

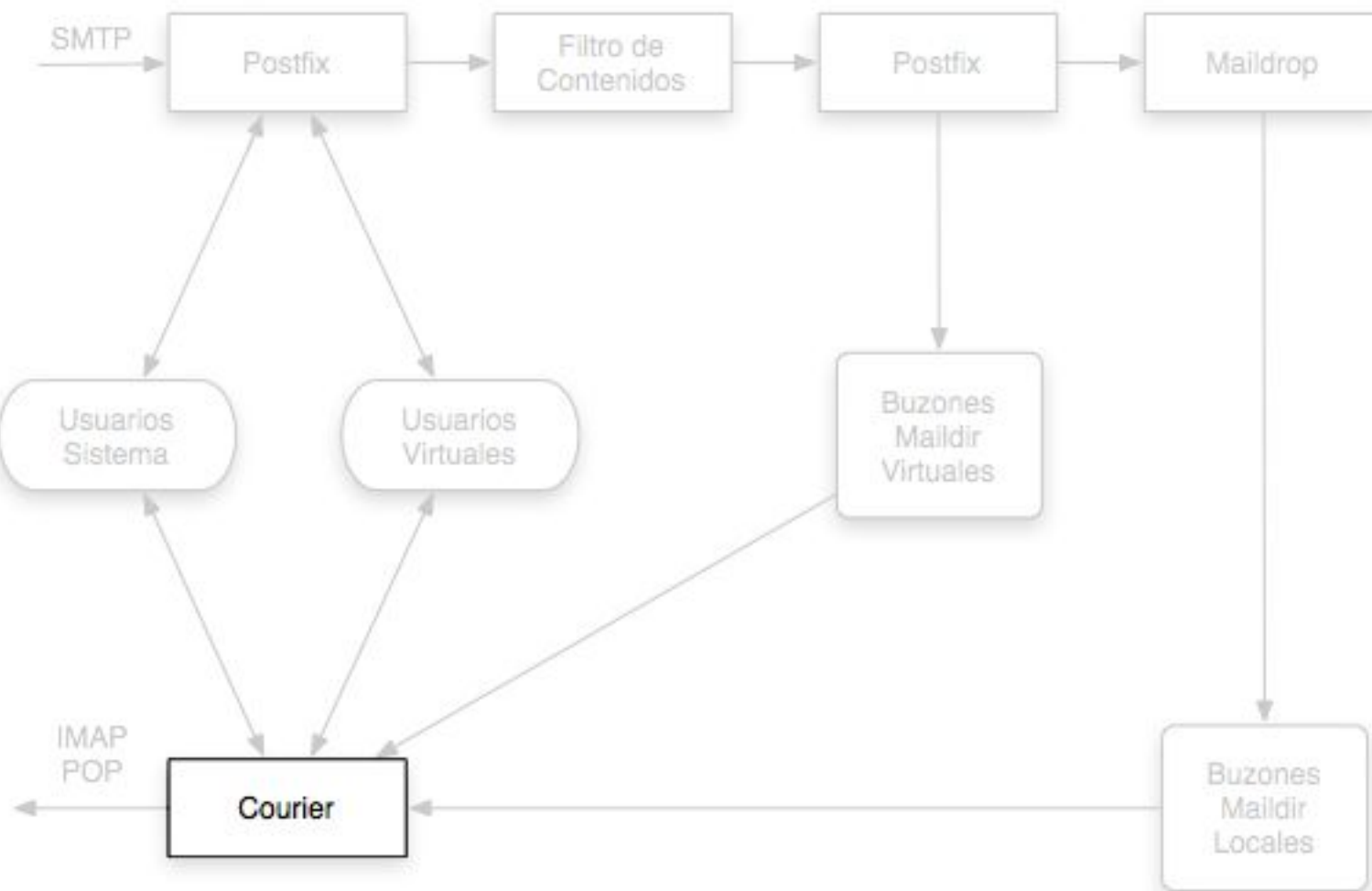
- Soporta carpetas compartidas entre grupos de usuarios.
- Permite limitar el nº de accesos de IMAP y numero máximo de accesos desde la misma IP.
- Escrito en C.

# 3



## Sistemas de Correo en GNU/Linux

### Arquitectura



90 - 203

Iker Sagasti Markina  
<iker@irontec.com>

# 3



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos los demonios para imap e imap-ssl de la suite de courier.

```
# apt-get install courier-imap courier-imap-ssl
```

- Instalamos los demonios y librerías genéricas de courier.

```
# apt-get install courier-authdaemon courier-base  
courier-ssl
```

# 3



## Sistemas de Correo en GNU/Linux

### Archivo de Configuración SSL

```
imapd.cnf [ Debian: /etc/courier/imapd.cnf ]
```

```
[ req ]  
default_bits = 1024  
encrypt_key = yes  
distinguished_name = req_dn  
x509_extensions = cert_type  
prompt = no
```

```
[ req_dn ]  
C=ES  
ST=Bizkaia  
L=Bilbao  
O=Irontec - Internet y Sistemas sobre GNU/Linux  
OU=Sistemas  
CN=mail.irontec.com  
emailAddress=sistemas@irontec.com
```

# 3



## Sistemas de Correo en GNU/Linux

### **Certificado Digital**

---

- Generamos la clave privada  

```
# openssl genrsa -out mail.irontec.com.key 1024
```
- Generamos la solicitud de certificado firmado  

```
# openssl req -new -key mail.irontec.com.key -config  
imapd.cnf -out mail.irontec.com.csr
```
- Generamos un certificado firmado mediante una CA  

```
# openssl ca -out mail.irontec.com.crt -in  
mail.irontec.com.csr
```

# 3



## Sistemas de Correo en GNU/Linux

### **Configuración SSL**

---

- El certificado de Courier tiene que estar formado por:
  - Clave privada del servidor
  - Certificado firmado por una CA
    - Unicamente desde -----BEGIN CERTIFICATE-----
      - Editamos y eliminamos el resto
  - Parámetros DH

```
# cat mail.irontec.com.key mail.irontec.com.crt >  
mail.irontec.com.pem
```

```
# openssl gendh >> mail.irontec.com.pem
```

# 3



## Sistemas de Correo en GNU/Linux

### Configuración SSL

```
# cat www.irontec.com.pem
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAABgQDWP7WzRg7DNpXgF94YsqPr84p08sAWcM6jXdG1QQZhuWBtyoWU
0DnpLndcjV5At6IdQ7ZqSi6XbE1jEONyIZ3Ruimrd2+gks8a9NkQoI2YLjTTR5dL
EAZxasb3AkeEA3dsqgh7cBIItGaC7PYve0vch4gMYTiOR1NHzQHv4uojdAxvCGxdrV
qEYEUBnNGcYy1tbSzLFKt7Npz6RORpB4lwJBAL7eSyORtWJ1RT4WnceIOWf6Kkaa
a4NEJttVYYBw+8muVQgnnM/MbjlzRUcDm9HL82sd9rZXAvh2dj30oWTTUYUCQQCh
OiQTOe/00W5SSipmptNPz8Ytd1887aILieUJkPk84+CMcshOxPeW+YMq3wVBhNrA
6c95+CHvjFAKGULVXypzAj9VpUkgGwDmCFayOs4zwa5MN6B2G4NN6EsNDu/SWcY/
E/skSXjRI7RhcR3cle7KDqaQJJAi/TOFhV43OWC1q1Q=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDrDCCAxWgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBkDELMAkGA1UEBhMCRVMx
EDA0BgNVBAgtTB0JpemthaWEXDzANBgNVBAcTBkJPBjBzEQMA4GA1UEChMHSHXJv
hvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydG1maWNhdGUwHQYDVR0OBBYE
w6tWudMrm8QFoYGWpIGTMIGQMqswCQYDVQGEwJFuzEQMA4GA1UECBMHQml6a2Fp
YTEPMA0GA1UEBxMGQmlsYmFvMRAwDgYDVQQKEwdJcm9udGVjMREwDwYDVQQLEWhT
aXN0ZW1hczeUUMBIGAlUEAxMLaXJvbnR1Yy5jb20xIzAhBgkqhkiG9w0BCQEFHNp
c3RlbWFzZGlyb250ZWMuY29tggaHSHOIQtatpswDQYJKoZIhvcNAQEEBQADgYEA
M1S8cmkUC/nE5gnpiEWg+lYcHuJsNs6uBTNn7PdUiRqZOTCcucqIpIV1iwe6OxsX
Yz3DQe3JCXcf+3BSgtt9hrrTTNOgoEZLEPlTHUV3dVZnm0wNlMuobfM0p6BhS+m2
NWFMQKpe79rWcgShkLeJfz1IzDWRchzj4205Fpe+VMO=
-----END CERTIFICATE-----
-----BEGIN DH PARAMETERS-----
MEYCQQDTT1zESN4Dzbp9mL0bIdbbs/CafrR2Q0RvWumpPYQX4jjwKk3mEttinZ4H
wzMDbuS8a5EgRTRk67TPq0H/uBIDAgEC
-----END DH PARAMETERS-----
```



# Courier POP (POP Server)

<http://www.courier-mta.org/imap/>

# 3



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos los demonios para pop e pop-ssl de la suite de courier.

```
# apt-get install courier-pop courier-pop-ssl
```

- Instalamos los demonios y librerías genéricas de courier (en caso de no tenerlas ya)

```
# apt-get install courier-authdaemon courier-base  
courier-ssl
```

# 4



Sistemas de Correo en GNU/Linux

## **Amavisd-new**

# Amavisd-new (Filtro Contenidos)



<http://www.ijs.si/software/amavisd>

# 4



## Sistemas de Correo en GNU/Linux

### **Características**

---

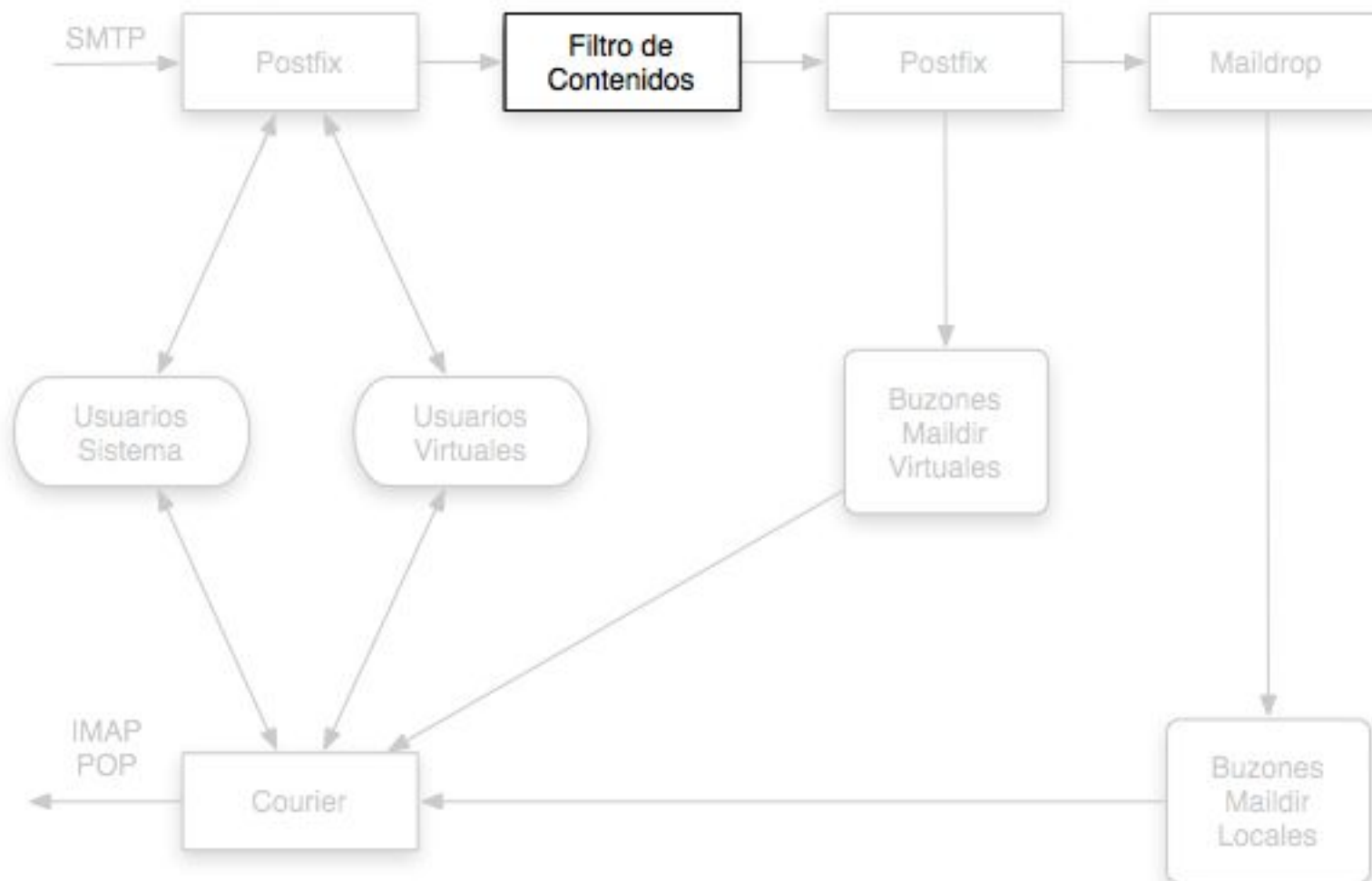
- Es una interfaz entre el MTA y los filtros de contenidos.
- Interfaz para MTA y línea de comandos.
- Capaz de comunicarse con el MTA vía (E)SMTP o LMTP, o utilizando programas auxiliares
- Cuando se integra con Mail::SpamAssassin (SA), solo llama a SA una única vez.
- Evolución mejorada de amavisd.
- Interfaz para una gran cantidad de filtros de contenidos (spam, virus, listas...)
- Escrito en Perl.

# 4



## Sistemas de Correo en GNU/Linux

### Arquitectura



100 - 203

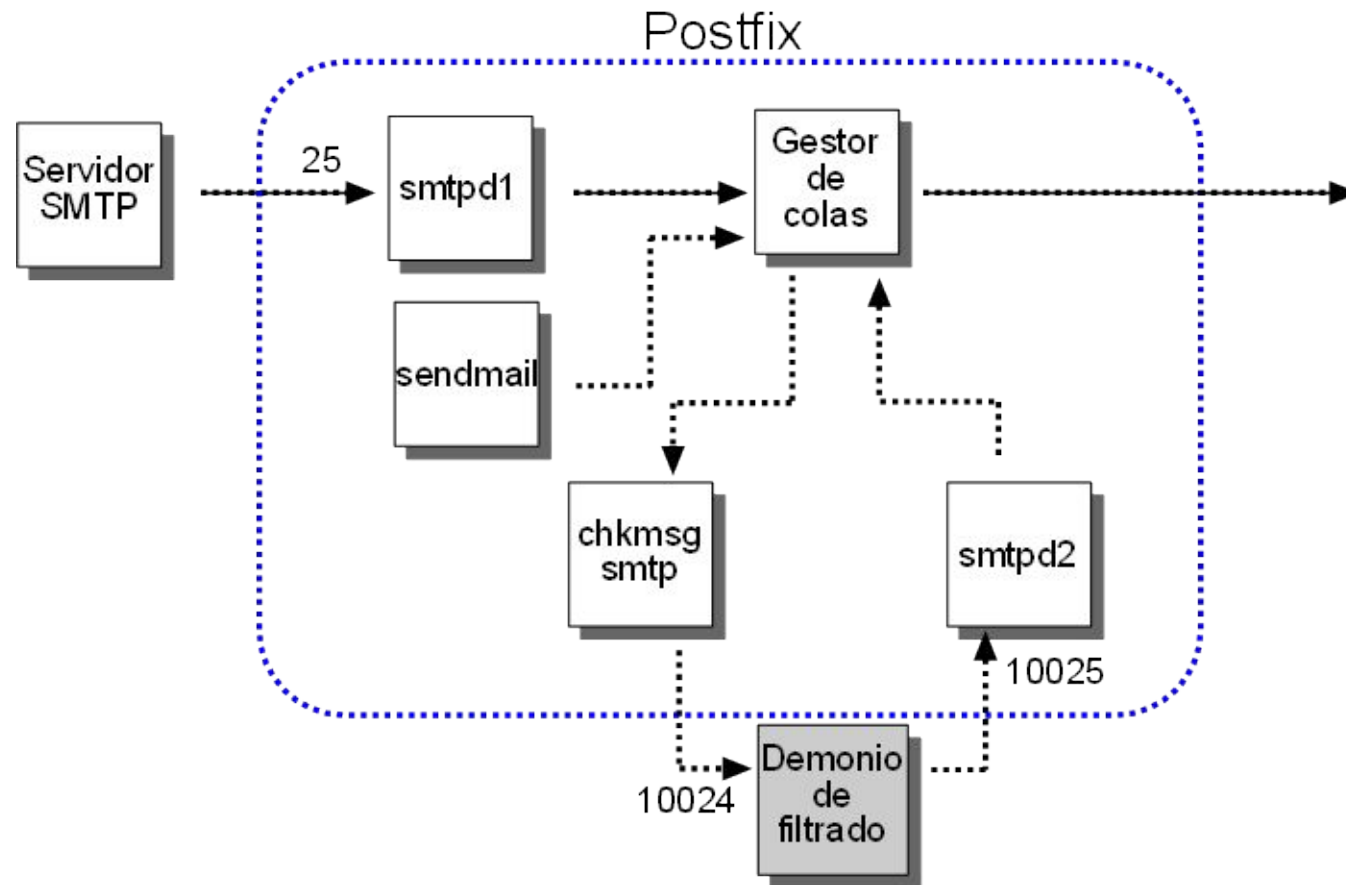
Iker Sagasti Markina  
<iker@irontec.com>

# 4



## Sistemas de Correo en GNU/Linux

### Diagrama



# 4



## Sistemas de Correo en GNU/Linux

### **Funcionamiento Filtro Contenidos**

---

1. El correo llega a nuestro MTA en el puerto 25, procedente de un MUA o MTA.
2. El demonio principal smtpd con los parámetros definidos en main.cf gestiona el correo.
3. Si no es rechazado, el correo se transporta a amavisd-new al puerto 10024.
4. Para ello definimos en master.cf un nuevo cliente smtp secundario.
5. El correo es inyectado a amavisd-new por el nuevo cliente smtp definido.

# 4



## Sistemas de Correo en GNU/Linux

### **Funcionamiento Filtro Contenidos**

---

6. Amavisd-new procesa el mensaje con filtros de contenidos configurados (virus y spam)
7. Si no es rechazado, amavis reinyecta el correo a 2º demonio smtpd en el puerto 10025
7. Definimos en master.cf nuevo demonio smtpd. Solo acceso localhost por seguridad
8. El 2º demonio smtpd se encarga de entregar correo en el buzón correspondiente. MDA.

# 4



## Sistemas de Correo en GNU/Linux

### Integración con Postfix - main.cf

```
main.cf [Debian: /etc/postfix/main.cf]
```

```
# Pasamos los correos recibidos en 0.0.0.0:25 al  
puerto 1024 de localhost mediante el transporte  
definido como smtp-amavis
```

```
content_filter = smtp-amavis:[localhost]:1024
```

# 4



## Sistemas de Correo en GNU/Linux

### **Integración con Postfix - master.cf**

- Definimos un nuevo cliente smtp que será el encargado de inyectar los mails a amavisd.
- Como hemos definido en main.cf (smtp-amavis:[localhost]:10024), cuando un correo llegue al puerto 25 será procesado por el demonio smtpd principal y después será transportado a un servicio local que escucha en el puerto 10024 (amavisd).

# 4



## Sistemas de Correo en GNU/Linux

### Integración con Postfix - master.cf

```
master.cf [Debian: /etc/postfix/master.cf]
```

```
# Cliente smtp encargado de reinyectar el correo a  
amavisd-new.
```

```
smtp-amavis unix - - y - 2 smtp  
    -o smtp_data_done_timeout=1200  
    -o disable_dns_lookups=yes
```

# 4



## Sistemas de Correo en GNU/Linux

### Integración con Postfix - master.cf

```
# Añadimos otro demonio smtp (smtpd)
# para la reinyección de correos de amavisd
127.0.0.1:10025 inet n - - smtpd
    -o content_filter=
    -o mynetworks=127.0.0.0/8
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_client_restrictions=
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=
        permit_mynetworks,
        reject
    -o strict_rfc821_envelopes=yes
```

# 4



## Sistemas de Correo en GNU/Linux

### Archivos de Configuración

```
amavisd.conf [ Debian: /etc/amavis/amavisd.conf ]
```

- Archivo general de configuración de la interfaz a los filtros de contenidos.

```
# Definimos el dominio principal del MTA.  
$mydomain = 'aktornet.ath.cx';
```

```
# Inyectar el correo filtrado a una segunda  
# instancia de Postfix en localhost:10025.  
$forward_method = 'smtp:127.0.0.1:10025';
```

```
# Donde enviar las notificaciones generadas  
$notify_method = $forward_method;
```

```
# Nos interesan los logs en /var/log/amavis.log.  
# Mailgraph  
$DO_SYSLOG = 0;  
$LOGFILE = "/var/log/mail.log";
```

# 4



## Sistemas de Correo en GNU/Linux

# Archivos de Configuración

---

```
# Avisos de llegada de virus
$virus_admin = "aktor\@aktornet.ath.cx";

# Añadimos una cabecera a los correos que hemos
filtrado
$X_HEADER_LINE = "por AMAVIS + CLAMAV en $mydomain";
```

# 4



Sistemas de Correo en GNU/Linux

## **Clamav**

---

# Clamav (Anti-Virus)



<http://www.clamav.net>

# 4



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Es un escaner de virus GPL y mantenido por la comunidad.
- Interfaz para MTA (clamd) y línea de comandos (clamscan).
- Demonio rápido (algoritmo Aho-Corasic mutado) y multi-hilo.
- Interfaz enviar nuevas firmas de virus [<http://clamav.catt.com/cgi-bin/sendvirus.cgi>].
- Actualización periódica vía Internet (freshclam).
- Detección de más de 30.000 viruses, gusanos y troyanos.

# 4



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Soporta mbox, Maildir y mails en modo raw.
- Escrito en C. POSIX.
- Lo usan: SourceForge, DynDNS, HispaNetwork, Multiples Universidades (Deusto), Irontec ;-)

# 4



## Sistemas de Correo en GNU/Linux

### Situación Actual – Tiempos de Respuesta

- Mutación de Mydoom con compresor MEW
- Reacción de las “casas” antivirus

# Fuente: Hispasec

ClamAV	16.02.2005	23:02	::	Worm.Mydoom.M-2
Sophos	17.02.2005	00:02	::	W32/MyDoom-O
TrendMicro	17.02.2005	01:11	::	WORM_MYDOOM.M
F-Prot	17.02.2005	01:48	::	W32/Mydoom.AY@mm
McAfee	17.02.2005	01:53	::	W32/Mydoom.bb@MM!zip
eTrust-Iris	17.02.2005	02:35	::	Win32/Mydoom.AU!Worm
Symantec	17.02.2005	03:30	::	W32.Mydoom.AX@mm
eTrust-Vet	17.02.2005	06:35	::	Win32.Mydoom.AU!ZIP
Antivir	17.02.2005	07:11	::	Worm/MyDoom.BB
DrWeb	17.02.2005	08:10	::	Win32.HLLW.MyBot
BitDefender	17.02.2005	08:54	::	Win32.Mydoom.AQ@mm
Panda	17.02.2005	08:54	::	W32/Mydoom.AO.worm
Norman	17.02.2005	09:25	::	MyDoom.AQ@mm
AVG	17.02.2005	11:10	::	I-Worm/Mydoom.AP

# 4



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos el software antivirus para línea de comandos, como demonio

```
# apt-get install clamav clamav-base clamav-daemon
```

- Instalamos actualizador de base de datos de virus

(acceso permanente a Internet)

```
# apt-get install clamav-freshclam
```

(acceso NO permanente Inet)

```
# apt-get install clamav-data clamav-getfiles
```

- El usuario clamav necesita pertenecer al grupo amavis

```
# adduser clamav amavis
```

# 4



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos los descompresores para los archivos comprimidos.

```
# apt-get install lha arj unrar zoo nomarch lzop  
arc unzoo
```

- Descarga de virus de prueba (solo prueba ;)

```
# wget -r -nH --cut-dirs 1  
http://www.irontec.com/~aktor/files/virii/
```

# 4



## Sistemas de Correo en GNU/Linux

### Sintaxis

---

```
$ clamscan [opciones] [archivo/directorio/-]
```

- Escanea directorios de forma recursiva.

```
clamscan -r
```

- Muestra solo los archivos infectados.

```
clamscan -i
```

- Habilita el soporte para escanear buzones mbox. Maildir por defecto.

```
clamscan -mbox
```

- Carga BD de virus del archivo o todos .db y .db2 del directorio

```
clamscan -d ARCH/DIR
```

116 - 203

# 4



## Sistemas de Correo en GNU/Linux

### **Sintaxis**

---

- Guarda el resultado del escaneo en el archivo indicado.

```
clamscan -l ARCHIVO
```

- Escanea el archivo\_virus. IPC.

```
cat archivo_virus | clamscan -
```

# 4



## Sistemas de Correo en GNU/Linux

### Ejemplo – Sin Infecciones

(PIV 2,0 Ghz Celeron - 512 MB RAM)

```
$ clamscan /home/aktor/Maildir/.irontec/cur
```

```
----- SCAN SUMMARY -----
```

```
Known viruses: 31015  
Scanned directories: 1  
Scanned files: 213  
Infected files: 152  
Data scanned: 9.48 MB  
I/O buffer size: 131072 bytes  
Time: 5.642 sec (0 m 5 s)
```

```
$ htop
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	COMMAND
16210	aktor	15	0	7408	7408	1208	R	83.8	1.4	clamscan

# 4



## Sistemas de Correo en GNU/Linux

### Ejemplo – Con Infecciones - EICAR

```
Eicar: Eicar Anti-Virus Test File (www.eicar.org). NO GPL!!!
```

```
$ wget -O - http://www.eicar.org/download/eicar.com | clamscan -  
$ wget -O - http://www.eicar.org/download/eicar_com.zip | clamscan -
```

```
$ clamscan -ri --tgz virusmails/  
/var/lib/amavis/virusmails//virus-20040330-201255-13796-05: Eicar-Test-  
Signature FOUND
```

```
/var/lib/amavis/virusmails//virus-20040401-143048-24910-05:  
Trojan.URLspoofer.gen.2 FOUND
```

```
/var/lib/amavis/virusmails//virus-20040423-042237-02619-09:  
Exploit.HTML.Bagle.Gen-4-eml FOUND
```

```
/var/lib/amavis/virusmails//virus-20040426-175605-24493-05:  
Worm.Bagle.H-zippwd-1 FOUND
```

```
----- SCAN SUMMARY -----
```

```
Known viruses: 22925
```

```
Scanned directories: 1
```

```
Scanned files: 522
```

```
Infected files: 4
```

```
Data scanned: 14.06 Mb
```

```
I/O buffer size: 131072 bytes
```

```
Time: 38.784 sec (0 m 38 s)
```

```
# Cabeceras añadidas al mail puesto en cuarentena
```

```
X-Amavis-Alert: INFECTED, message contains virus: Worm.Bagle.Gen-zippwd,  
Worm.Bagle.H-zippwd-1
```

**119 - 203**

*Iker Sagasti Markina*  
<iker@irontec.com>

# 4



## Sistemas de Correo en GNU/Linux

### **Daemon**

---

- Demonio (clamd) que se inicia al arrancar el sistema.
- Modo de ejecución ideal para integrarlo con MTA's o con interfaces a MTA's.

```
root 311 0.0 5.3 17476 13832 ? Ss Jul04 0:00 /usr/sbin/clamd
root 313 0.0 5.3 17476 13832 ? S Jul04 0:01 /usr/sbin/clamd
root 314 0.0 5.3 17476 13832 ? S Jul04 2:35 /usr/sbin/clamd
```

- Archivo de Configuración del demonio del antivirus Clam (clamd)

```
clamav.conf [Debian: /etc/clamav/clamd.conf]
```

# 4



## Sistemas de Correo en GNU/Linux

### Integración con amavisd-new

- Comprobamos que la directiva LocalSocket del fichero '/etc/clamav/clamd.conf' tiene el mismo valor que '/var/run/clamd.ctl':
  - Clamav

```
LocalSocket /var/run/clamav/clamd.ctl
```

- Amavisd-new

```
### http://clamav.elektrapro.com/  
['Clam Antivirus-clamd',  
  \&ask_daemon, ["CONTSCAN {} \n",  
  '/var/run/clamav/clamd.ctl'],  
  ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^  
  qr/\bOK$/, qr/\bFOUND$/,  
  qr/^. *?: (?!Infected Archive)(.*) FOUND$/ ],
```

# 4



## Sistemas de Correo en GNU/Linux

### **Actualizaciones**

---

- Hay 2 maneras para actualizar la base de datos:
  - **Clamav-freshclam:** Herramienta para actualizar la base de datos desde internet.
    - Mirror principal. Se encarga de buscar por los mirrors oficiales.
      - [database.clamav.net](http://database.clamav.net)
  - **Clamav-data:** No se actualiza la BD desde instalación. Para actualizar: clamav-getfiles

# 4



## Sistemas de Correo en GNU/Linux

### **Freshclam**

---

- Herramienta de clamav para actualizar la BD de los virus automáticamente desde Inet.
- Descarga la base de datos de Internet y comprueba consistencia: MD5 sum.
- Funciona de 2 maneras:
  - Interactivo: desde línea de comandos.  
Periodicidad mediante cron.

```
0 8 * * * /usr/bin/freshclam --quiet -l /var/log/clam-update.log
```

# 4



## Sistemas de Correo en GNU/Linux

### **Freshclam**

---

- Demonio: trabaja de manera autónoma, silenciosa.

```
clamav 26558 0.0 0.3 2412 884 ?          Ss   Jul25   0:01  
/usr/bin/freshclam --daemon --checks 5 --quiet --log /  
var/log/clamav-freshclam.log --datadir /var/lib/clamav/
```

- Ж Cuando el proceso es iniciado por root dropea los privilegios (a usuario clamav por defecto)

# 4



## Sistemas de Correo en GNU/Linux

### **Freshclam – Archivos de Configuración**

- `/etc/clamav/freshclam.conf`

```
# Número de actualizaciones diarias  
Checks 24
```

- Archivo que recoge el resultado de las descargas de la base de datos de virus.

- `/var/log/clamav/freshclam.log`

```
-----  
ClamAV update process started at Sun Feb 20 06:26:37 2005  
main.cvd is up to date (version: 29, sigs: 29086, f-level: 3, builder: tomek)  
daily.cvd is up to date (version: 714, sigs: 1195, f-level: 4, builder: tkojm)  
-----  
ClamAV update process started at Sun Feb 20 13:26:37 2005  
main.cvd is up to date (version: 29, sigs: 29086, f-level: 3, builder: tomek)  
daily.cvd updated (version: 715, sigs: 1921, f-level: 4, builder: ccordes)  
Database updated (31007 signatures) from db.local.clamav.net (IP:  
64.186.250.53)  
Clamd successfully notified about the update.
```

# 4



Sistemas de Correo en GNU/Linux

## **SpamAssassin**

# SpamAssassin (Anti-spam)



<http://spamassassin.apache.org/>

# 4



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Es un filtro para correos que se utiliza para identificar el SPAM (UBE o UCE).
- Realiza una serie de pruebas sobre el correo para comprobar si es spam o no.
- Utiliza análisis bayesianos. Los usuarios pueden entrenarle para que aprenda.
- Soporta gran cantidad de listas negras (mail-abuse.org, ordb.org, ...)
- Diseñado para ser llamado por los archivos .mailfilter o .forward del MDA de un usuario, aunque puede ser integrado junto al MTA.
- Resulta muy pesado para la máquina en el que está instalado.
- Escrito en Perl.

# 4



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos el software demonio y cliente anti spam.

```
# apt-get install spamassassin spamc
```

# 4



## Sistemas de Correo en GNU/Linux

### Configuración

- `amavisd.conf` [ Debian: `/etc/amavisd/amavisd.conf` ]
- Integramos spamassassin junto con amavisd.  
# para que deje pasar los mails luego los filtraremos  
# con maildrop.  
`$final_spam_destiny = D_PASS;`  
`$sa_tag_level_deflt = 0.0;`  
`$sa_tag2_level_deflt = 5.0;`  
`$sa_kill_level_deflt = $sa_tag2_level_deflt;`
- Y comentamos la línea para que amavis utilice spamassassin:  
`# @bypass_spam_checks_acl = qw( . );`
- Para que corra como demonio hay que modificar el archivo `'/etc/default/spamassassin'`

`ENABLED=1`

129 - 203

# 4



## Sistemas de Correo en GNU/Linux

### **Ejemplo – GTUBE**

- Mail de prueba. SpamAssassin le otorga 1000.0 puntos.

```
Subject: Test spam mail (GTUBE)
Message-ID: <GTUBE1.1010101@example.net>
Date: Wed, 23 Jul 2003 23:30:00 +0200
From: Sender <sender@example.net>
To: Recipient <recipient@example.net>
Precedence: junk
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
```

```
This is the GTUBE, the
Generic
Test for
Unsolicited
Bulk
Email
```

# 4



## Sistemas de Correo en GNU/Linux

### Aprendizaje

- Comando para el aprendizaje del SpamAssassin.

```
$ sa-learn [opciones] archivo/s
```

- Aprende los correos del directorio ham como NO spam.

```
sa-learn --ham ham
```

- Aprende el correo X como spam.

```
sa-learn --spam ~/Maildir/spam/X
```

- Olvida el correo archivo que le hicimos aprender.

```
sa-learn --forget archivo
```

# 4



## Sistemas de Correo en GNU/Linux

### Aprendizaje

---

- Los correos entrantes están en formato mbox.

```
sa-learn --mbox
```

- Muestra el contenido de las BD bayesianas.

```
sa-learn --dump [all|data|magic]
```



# Courier Maildrop (Mail Delivery Agent)

<http://www.courier-mta.org/maildrop/>

# 5



## Sistemas de Correo en GNU/Linux

### **Características**

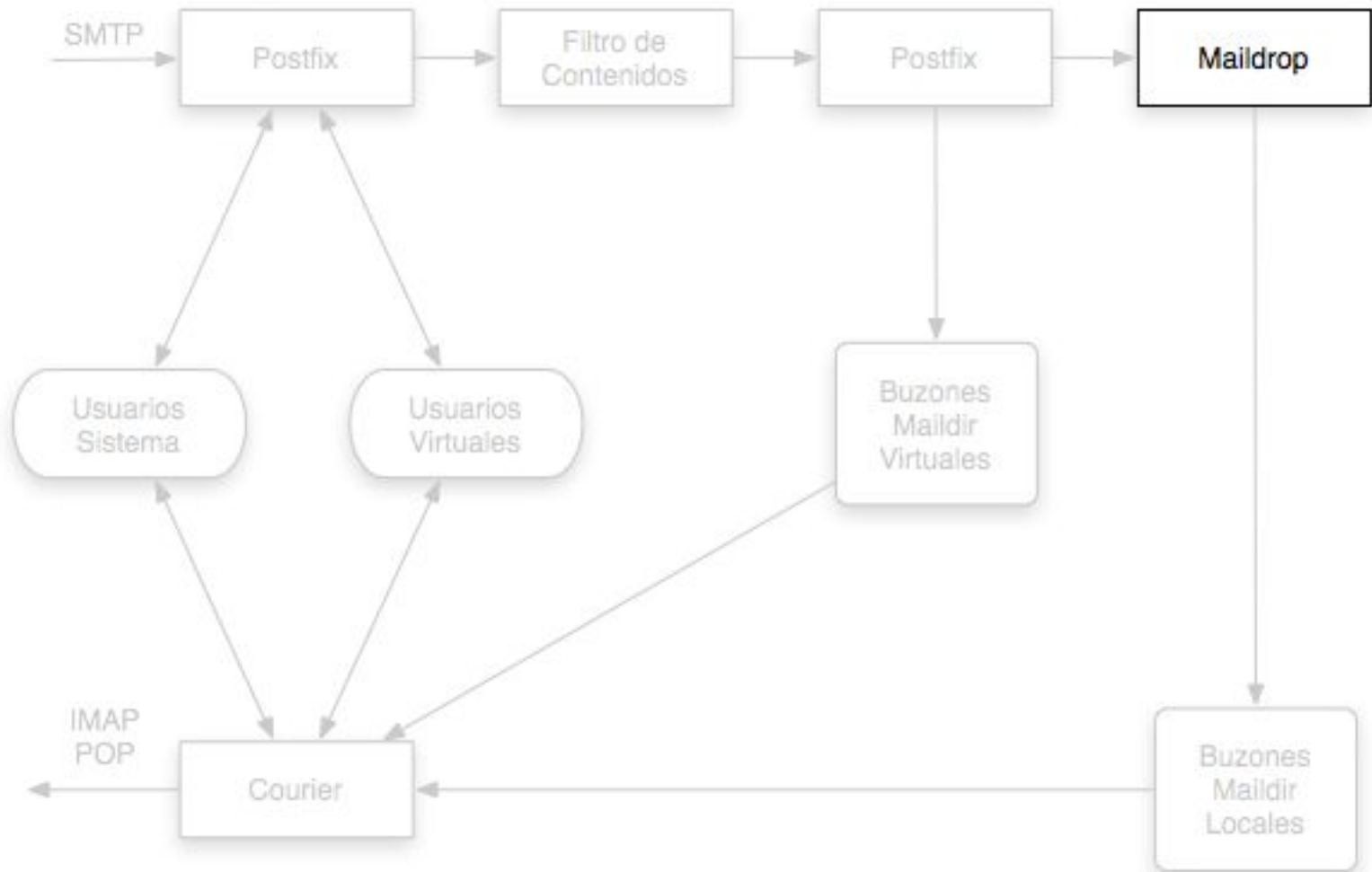
---

- Es un MDA (Agente de Reparto de Correo) con capacidad de filtrado.
- Es un software de la suite de courier (<http://www.courier-mta.org>).
- Sustituye al software de reparto de correo local.
- Capacidad para trabajar con buzones tipo mbox y maildir.
- Escrito en C++.
- Double Precision Inc.



## Sistemas de Correo en GNU/Linux

### **Arquitectura**



135 - 203

Iker Sagasti Markina  
<iker@irontec.com>



## Sistemas de Correo en GNU/Linux

### **Courier Maildrop vs Procmail**

---

- Maildrop, a diferencia de Procmail, utiliza un lenguaje estructurado.
- El binario de maildrop es más grande que el de procmail, sin embargo, utiliza los recursos de forma más eficiente.
  - Maildrop no guarda un mensaje de 10 MB en memoria.
  - Lo salva a un fichero temporal y lo filtra directamente.



### **Courier Maildrop vs Procmail**

---

- Si el archivo de configuración tiene errores:
  - a) Si error en instrucciones: No realiza la instrucción.
  - b) Si error en sintaxis: No reparte el correo y lo deja en la cola.

# 5



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos el Mail Delivery Agent (MDA) que va a sustituir al que trae Postfix.

```
# apt-get install courier-maildrop
```

# 5



## Sistemas de Correo en GNU/Linux

### **Archivos de Configuración**

---

- Archivo de configuración general. Todos los usuarios comparten los filtros definidos.

`/etc/courier/maildroprc`

- Archivo de configuración local para cada usuario. Cada usuario define sus propios filtros.

`$HOME/.mailfilter`



## Sistemas de Correo en GNU/Linux

# Archivos de Configuración

---

- Permisos de los archivos
  - Mails filtrados tienen que pertenecer al mismo usuario y NO tener permiso de grupo o resto.

```
-rw----- 1 aktor aktor 3,9K 2003-04-28 13:11  
1051528262.681_1.Asterix:2,S
```

- Archivos de configuración local (\$HOME/.mailfilter) permisos 600.

```
-rw----- 1 aktor aktor 1923 2004-07-23 19:38  
/home/aktor/.mailfilter
```



## Sistemas de Correo en GNU/Linux

### **Sintaxis**

---

- También conocida como maildropfilter.
- Muy similar a Perl, aunque diferente!
- Es un “lenguaje” de programación.
  - Variables
  - Estructuras de Control
  - Expresiones regulares
  - Ejecución de comandos
- Muy potente



## Sistemas de Correo en GNU/Linux

### Sintaxis

---

- Estructuras de control para filtrar por cabeceras o cuerpo del mensaje. Regexp.

```
if ( /^Subject: eghost/ )  
{  
    ...juego de  
    instrucciones...  
}
```

- Si las instrucciones son largas mejor utilizar include (solo se procesan cuando se cumple la condición)

```
if ( /^Content-Type: application\/octet-stream;/:b && /^  
name=".*\.(pif|scr)"/:b )  
{  
    log "----- VIRIII"  
    to "/dev/null"  
}
```

# 5



## Sistemas de Correo en GNU/Linux

### Sintaxis

---

```
if ( /^List-Id: Lista de eside-ghost/ ) {  
  to "Maildir/.eghost"  
  xfilter "reformail -A'X-Sender: $SENDER'"  
}
```

# 5



## Sistemas de Correo en GNU/Linux

### Integración con Postfix

```
main.cf [Debian: /etc/postfix/main.cf]
```

```
# maildrop
```

```
mailbox_command = /usr/bin/maildrop -d $USER -f $SENDER
```

- Los parámetros del maildrop permiten pasar los valores a maildrop para su posterior uso.

```
import SENDER
```

```
if ( /^List-Id: prueba.ironotec.com/ )
```

```
{
```

```
    log "[prueba] $SENDER"
```

```
}
```

# 5



## Sistemas de Correo en GNU/Linux

### Auto-aprendizaje junto con SpamAssassin

```
/etc/courier/maildroprc

# Si la puntuación es 5.0 o mayor lo movemos
# a la carpeta de spam y lo aprendemos.
if (/^X-Spam-Level: \*\*\*\*/)
{
  cc "|/usr/bin/sa-learn --spam"
  to "Maildir/.Spam"
}
# Si la puntuación es 2.0 o mayor lo movemos
# a la carpeta de posible spam.
if (/^X-Spam-Level: \*\*/)
{
  to "Maildir/.PosibleSpam"
}
# El resto lo aprendemos como correo NO spam
# y lo dejamos en nuestro INBOX.
cc "|/usr/bin/sa-learn --ham"
to "Maildir"
```



## Sistemas de Correo en GNU/Linux

### **Mailbot**

---

- Utilidad para autoresponder correos
- Personalizable para cada usuario o cuenta de correo mediante los archivos:
  - `/etc/courier/maildroprc`
  - `$HOME/.mailfilter`
- Se envia auto-respuesta excepto en los casos en que el mensaje original tenga:
  - Cabeceras:
    - Precedence: bulk
    - Precedence: junk
  - Tipo contenido MIME:
    - multipart/report



## Sistemas de Correo en GNU/Linux

### **Mailbot**

---

- Ejemplo:

```
if (/^To: soporte@irontec.com/:h)
{
    cc "| mailbot -t /etc/courier/mailbot/soporte \
-s 'Atenderemos su petición lo antes posible'
-A 'From: Irontec.com - SOPORTE<soporte@irontec.com>' \
/usr/bin/sendmail -t -f ''"
}
```

# -t: contenido de la respuesta en texto plano

# -s: asunto o subject de la respuesta

# -A: cabecera añadida al correo respuesta



## Mutt

---

# Mutt (Mail User Agent)



<http://www.mutt.org>



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Es un navegador de archivos especializado en navegación de emails en modo consola.
- Soporta multiples métodos de almacenamiento y acceso: mbox, mh, Mairdir, IMAP, NFS.
- Funciona mediante teclas de acceso rápido.
- Cliente muy pequeño y eficiente (631K lincado dinámicamente).
- Soporte PGP y MIME excelente.
- Muy configurable.
- Gran soporte para listas de correo.
- No habla SMTP. Necesita MTA (Mail Transport Agent) o MSA (Mail Sender Agent).

# 5



## Sistemas de Correo en GNU/Linux

### **Archivos de Configuración**

---

- Archivo de configuración global a todos los usuarios.  
`/etc/Mutttrc`
- Archivo de configuración personal de cada usuario.  
`~/.mutt/mutttrc` o `~/.muttrc`
- Archivo global para la definición del manejo de los MIME type de tipo no-texto.  
`/etc/mailcap`
- Archivo personal para la definición del manejo de los MIME type de tipo no-texto.  
`- ~/.mailcap`



## Sistemas de Correo en GNU/Linux

### **Sintaxis - muttrc**

---

```
# Definir dirección 'From:' por defecto
set from="Iker Sagasti Markina <iker@irontec.com>"
# Caracteres en castellano + Euro
set charset="iso-8859-15"
set locale="es_ES"
# Listas de correo suscritas. Reply-To-List
subscribe eside-ghost@deusto.es hacklab-
leioa@sindominio.net
# Definir el directorio donde están los mailboxes
set folder="~/Maildir"
# Definir el directorio donde se añadirán los
archivos leídos del '$spoolfile'
set mbox="~/Maildir"
# Definir el tipo de mailbox
set mbox_type=Maildir
# Definir donde están los mails entrantes
set spoolfile="~/Maildir/"
# Ordena los mensajes por hilos. In-Reply-To.
set sort=threads
```



## Sistemas de Correo en GNU/Linux

### **Sintaxis - muttrc**

---

```
# Color del texto y fondo de cabecera
color header brightblue black ^Subject:
# Definir macro
macro index <f2> "!/bin/date\n" "Mostrar la hora"
# Mailboxes donde checkear mail
mailboxes Maildir/.irontec Maildir/.eghost
# Mostrar solo determinadas cabeceras
# al leer los mails.
ignore *
unignore date from to cc x-mailer user-agent subject
# Pitido al llegar nuevo mail
set beep_new=yes
# Copia de los mensajes salientes
set record="~/Maildir/.Enviado/"
# Anteponer -- a la firma y añadir la firma
set sig_dashes
set signature="~/signature"
```



## Sistemas de Correo en GNU/Linux

### Parámetros

---

```
$ mutt [parámetros]
```

- Muestra listado con buzones de correo. Modo browser.

```
mutt -y
```

- Abre el buzón indicado.

```
mutt -f maildir_directory
```

```
$ mutt -f imaps://dns.servidor.imap/
```

```
$ mutt -f ~/Maildir/.eghost/
```

- Abre el buzón en modo solo lectura.

```
mutt -R
```

- Ignora los archivos de configuración de mutt.

```
mutt -n
```

# 5



## Sistemas de Correo en GNU/Linux

### **Integración GPG**

---

```
$HOME/.muttrc
```

```
# Verifica automaticamente mensajes entrantes
```

```
set pgp_verify_sig=yes
```

```
# Al recibir msg firmado, la respuesta tb se firma
```

```
set pgp_replysign
```

```
# Envia todos los mails firmados
```

```
set pgp_autosign=yes
```

```
# Adicionalmente se puede añadir una cabecera:
```

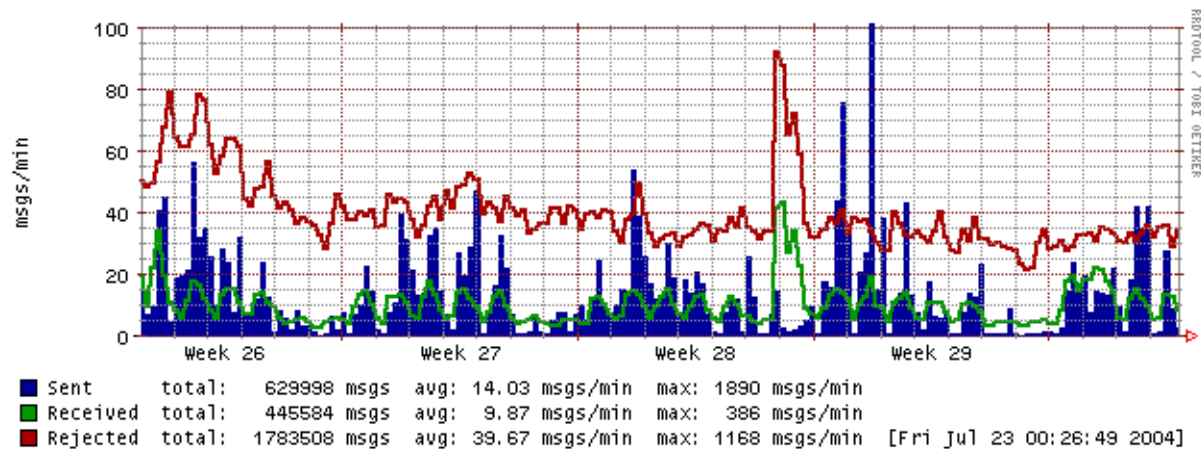
```
my_hdr X-GPG-key: http://aktornet.ath.cx/aktor.asc
```



## Sistemas de Correo en GNU/Linux

### **Mailgraph**

# Mailgraph (Visor de Logs)



<http://people.ee.ethz.ch/~dws/software/mailgraph>

# 6



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Es un frontend RRDTOol para visualizar las estadísticas de Postfix.
- Genera gráficos diarios, semanales, mensuales y anuales de los mails recibidos, enviados, rebotados, rejeitados, con spam y con virus.
- Necesita apache con soporte para cgi's.
- <http://mi.dominio.tld/cgi-bin/mailgraph.cgi>
- Escrito en Perl.
- David Schweikert <dws@ee.ethz.ch>
- Traducido al castellano por Iker Sagasti Markina <iker@irontec.com>.  
<http://www.irontec.com/~aktor/files/mailgraph.es.cgi>

# 6



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos el gestor de listas.  
`# apt-get install mailgraph`
- Instalamos servidor web (si es que no está ya instalado)  
`# apt-get install apache`

# 6



## Sistemas de Correo en GNU/Linux

### **Archivos de Configuración**

---

- Es necesario indicar el archivo donde se registran los logs para que mailgraph lo parsee.

```
mailgraph [Debian: /etc/default/mailgraph]
```

```
MAIL_LOG=/var/log/mail.log
```

- Si estamos utilizando AMAVIS, para evitar que cuente por duplicado el número de mensajes enviados o recibidos (debido a la realimentación de amavis) tenemos que indicarle al demonio que no contabilice los mails provenientes de 'localhost'.

# 6



## Sistemas de Correo en GNU/Linux

### **Archivos de Configuración**

---

```
/etc/init.d/mailgraph
```

```
start-stop-daemon -S -q -b -p $PID_FILE -x $DAEMON --  
-l $MAIL_LOG -d --daemon-rrd=$RRD_DIR -ignore-localhost  
^^^^^^^^^^^^^^^^^^^^
```

- Nos aseguramos \$MAIL\_LOG registra todos los sucesos. Necesario que AMAVIS loggee sobre él, sino perderemos toda la información relativa a los SPAM y VIRUSES.

# 6



# Pflogsumm (Visor de Logs)

[http://jimsun.linxnet.com/postfix\\_contrib.html](http://jimsun.linxnet.com/postfix_contrib.html)

# 6



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Es una herramienta para generar informes del correo que gestiona un MTA tipo Postfix.
- Genera informes muy completos sobre la cantidad de correos enviados y recibidos, por día, por hora, por remitente, por destinatario, errores... ordenados según diferentes criterios.
- Escrito en Perl 5.0

# 6



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos el visor de logs.

```
# apt-get install pflogsumm
```

# 6



## Sistemas de Correo en GNU/Linux

### **Modo de Uso**

---

```
# /usr/sbin/pflogsumm [opciones] [archivo]
```

- Mostrar el histórico de los correos enviados ayer

```
# pflogsumm -d yesterday /var/log/mail.log
```

- Mostrar el histórico de los correos enviados hoy

```
# pflogsumm -d today /var/log/mail.log
```

- Mostrar el histórico de los correos enviados durante esta semana (por defecto los log rotan cada semana)

```
# pflogsumm /var/log/mail.log
```

# 6



## Sistemas de Correo en GNU/Linux

### **Automatizar la generación de informes**

- A menudo puede resultar interesante la generación de informes de forma automática. Si encima los recibimos por email todavía mejor ;-)
- Utilizaremos la herramienta cron
- Envío de informe diario

```
# Script que enviará diariamente a las 7:00 am
# a la cuenta de postmaster un correo con el asunto:
# "estadísticas diarias de <nombre_host>" y con el
# resumen generado por pflogsumm como cuerpo del mismo
0 7 * * * /usr/sbin/pflogsumm -d yesterday
/var/log/mail.log 2>&1 | /usr/bin/mailx -s
"estadísticas diarias de $(uname -n)" postmaster
```

# 7



Sistemas de Correo en GNU/Linux

## **Mailman**

---

# Mailman (Gestor de Listas de Correo)



<http://www.gnu.org/software/mailman/>

# 7



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Es un software que ayuda a gestionar listas de discusión (listas de correo).
- Administración mediante interfaz web muy intuitiva. Creación y eliminación de listas.
- Posibilidad de moderadores y administración preferencias de cada usuario.
- Soporta filtrado por MIME type, expresiones regulares, direcciones de correo...
- Soporte para autorespondedores y plantillas personalizables.
- Soporte para dominios virtuales

# 7



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Soporte multi-lenguaje. Traducido al euskera por librezale.org.
- Escrito en Python, con un poco de código C para la seguridad.

# 7



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos el gestor de listas.

```
# apt-get install mailman
```

# 7



## Sistemas de Correo en GNU/Linux

### **Configuración**

---

- Es necesario crear la lista del sitio: mailman (encargada de labores administrativas).

```
# newlist mailman
```

```
Indique la dirección de correo de la persona que  
gestionará la lista: aktor@aktornet.ath.cx
```

```
Clave inicial de mailman:
```

```
Para terminar de crear su lista de distribución,  
tiene que editar el fichero /etc/aliases (o equivalente)  
añadiendo las siguientes líneas y ejecutando  
posiblemente el  
programa `newaliases':
```

# 7



## Sistemas de Correo en GNU/Linux

### Configuración

---

```
## lista de distribución mailman
mailman: "/var/lib/mailman/mail/mailman post mailman"
mailman-admin: "/var/lib/mailman/mail/mailman admin mailman"
mailman-bounces: "/var/lib/mailman/mail/mailman bounces mailman"
mailman-confirm: "/var/lib/mailman/mail/mailman confirm mailman"
mailman-join: "/var/lib/mailman/mail/mailman join mailman"
mailman-leave: "/var/lib/mailman/mail/mailman leave mailman"
mailman-owner: "/var/lib/mailman/mail/mailman owner mailman"
mailman-request: "/var/lib/mailman/mail/mailman request mailman"
mailman-subscribe: "/var/lib/mailman/mail/mailman subscribe mailman"
mailman-unsubscribe: "/var/lib/mailman/mail/mailman unsubscribe mailman"
```

# 7



## Sistemas de Correo en GNU/Linux

### **Creación Nueva Lista**

---

- Creamos una lista de correo y seguimos las instrucciones de lo que nos pide.

```
# newlist eghost
```

```
Indique la dirección de correo de la persona que  
gestionará la lista: txipi@sindominio.net
```

```
Clave inicial de eghost:
```

```
Para terminar de crear su lista de distribución,  
tiene que editar el fichero /etc/aliases (o  
equivalente)
```

```
añadiendo las siguientes líneas y ejecutando  
posiblemente el  
programa `newaliases':
```

# 7



## Sistemas de Correo en GNU/Linux

### Creación Nueva Lista

---

```
## lista de distribución eghost
```

```
eghost:          "/var/lib/mailman/mail/mailman post eghost"  
eghost-admin:   "/var/lib/mailman/mail/mailman admin eghost"  
eghost-bounces: "/var/lib/mailman/mail/mailman bounces eghost"  
eghost-confirm: "/var/lib/mailman/mail/mailman confirm eghost"  
eghost-join:    "/var/lib/mailman/mail/mailman join eghost"  
eghost-leave:   "/var/lib/mailman/mail/mailman leave eghost"  
eghost-owner:   "/var/lib/mailman/mail/mailman owner eghost"  
eghost-request: "/var/lib/mailman/mail/mailman request eghost"  
eghost-subscribe: "/var/lib/mailman/mail/mailman subscribe eghost"  
eghost-unsubscribe: "/var/lib/mailman/mail/mailman unsubscribe eghost"
```

# 7



## Sistemas de Correo en GNU/Linux

### **Acceso Interfaz Web**

---

- Acceso a la interfaz web de configuración
  - Listado con todas las listas visibles públicamente alojadas en la máquina

`http(s)://dominio.maquina/cgi-bin/mailman/listinfo`

- Interfaz web pública de la lista eghost. Edición opciones de suscripción para usuarios.

`http(s)://dominio.maquina/cgi-bin/mailman/listinfo/eghost`

- Interfaz web privada para la lista eghost. Solo accesible por el/los administrador/es.

`http(s)://dominio.maquina/cgi-bin/mailman/admin/eghost`

# 7



## Sistemas de Correo en GNU/Linux

### **Acceso Interfaz Web**

---

- Interfaz web privada para gestionar los rebotes generados en la lista eghost.

`http\(s\)://dominio.maquina/cgi-bin/mailman/admindb/eghost`

# 7



## Sistemas de Correo en GNU/Linux

### Configuración

```
mm_cfg.py [Debian: /etc/mailman/mm_cfg.py]

# Lista de gestión de mailman
MAILMAN_SITE_LIST = 'mailman'
# Por defecto ¡https!
DEFAULT_URL_PATTERN = 'https://%s/cgi-bin/mailman'
PRIVATE_ARCHIVE_URL = '/cgi-bin/mailman/private'
IMAGE_LOGOS         = '/images/mailman/'

# Dominio por defecto para las nuevas listas.
DEFAULT_EMAIL_HOST = 'irontec.com'

# Host por defecto para la interfaz de administración
DEFAULT_URL_HOST   = 'www.irontec.com'

# Lenguaje por defecto del servidor
DEFAULT_SERVER_LANGUAGE = 'es'
```



# SquirrelMail (Web Mail)



<http://www.squirrelmail.org>

# 8



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Es un software que permite leer el correo mediante un navegador web.
- Utiliza los protocolos IMAP y SMTP embebidos.
- Dispone de una gran variedad de plugins.
- No requiere de Javascript.
- No requiere de MySQL.
- Cliente de correo altamente estable.
- Muy sencillo de configurar e instalar. Script PERL.
- Soporte multi-lenguaje.
- Escrito en HTML 4.0 y PHP4. Estándares.



## Sistemas de Correo en GNU/Linux

### **Opciones Básicas**

---

- La interfaz web dispone de los siguientes menús:
  - Componer
    - Redactar y enviar mensajes con adjuntos
  - Direcciones
    - Libreta de direcciones.
  - Carpetas
    - Permite manipular las carpetas
  - Opciones
    - Ajustar las opciones de Squirrelmail
  - Buscar
    - Realizar un filtrado de los correos en base a un patron.

# 8



## Sistemas de Correo en GNU/Linux

### **Instalación**

---

- Instalamos el webmail

```
# apt-get install squirrelmail squirrelmail-locales
```

- Squirrelmail necesita un servidor web con soporte para php4

```
# apt-get install apache php4 libapache-mod-php4
```

# 8



## Sistemas de Correo en GNU/Linux

### **Archivos de Configuración**

---

- Incluimos las directivas para integrarlo con apache.
  - Insertamos la siguiente línea en el archivo `httpd.conf` de apache:

```
httpd.conf [ Debian: /etc/apache/httpd.conf ]
```

```
Include /etc/squirrelmail/apache.conf
```

# 8



## Sistemas de Correo en GNU/Linux

# Archivos de Configuración

---

```
# /usr/sbin/squirrelmail-configure
```

```
SquirrelMail Configuration : Read: config.php (1.4.0)
```

```
-----  
Main Menu --
```

1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

```
D. Set pre-defined settings for specific IMAP servers
```

```
C Turn color on
```

```
S Save data
```

```
Q Quit
```

```
Command >>
```

# 8



## Sistemas de Correo en GNU/Linux

### **Archivos de Configuración – Courier IMAP**

---

- Configuramos squirrelmail para integrarlo con courier-imap
  - Main Menu
    - Server Settings
      - Update IMAP Settings

8. `Server software : courier`

# 8



## Sistemas de Correo en GNU/Linux

### **Castellanizar**

---

- Necesita que el sistema tenga, al menos, soporte para locales 'es\_ES':
  - Importante!! Bug #269790
  - No es suficiente con 'es\_ES@euro'

```
# dpkg-reconfigure locales
```

```
es_ES ISO-8859-1
```

- Configuramos squirrelmail
  - Main Menu
    - Language Preferences
      - Default Language

```
es_ES
```
      - Default Charset

```
iso-8859-1
```

# 8



## Sistemas de Correo en GNU/Linux

### **Plugins**

---

- A fecha de hoy hay 194 plugins disponibles agrupados en 14 categorías.
- Disponibles en:
  - <http://www.squirrelmail.org/plugins.php>
- Descargar y descomprimir en:  
`/usr/share/squirrelmail/plugins`



## Sistemas de Correo en GNU/Linux

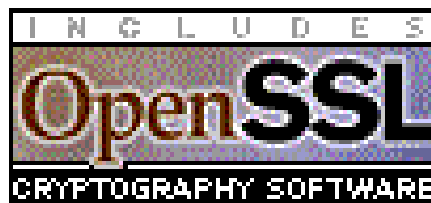
### **Plugins**

---

- A destacar:
  - View As HTML
    - Permite ver un email como HTML o como texto plano
  - Autocomplete
    - Busca en la agenda para autocompletar el destinatario
  - Calendars
    - Creación de calendarios publicos o limitados.
  - Dictionary
    - Comprueba la ortografía del texto redactado.
  - GPG
    - Soporte para firmas/cifrado GPG



# Openssl (Secure Socket Layer)



<http://www.openssl.org>

# 9



## Sistemas de Correo en GNU/Linux

### **Características**

---

- Herramienta que permite implementar los protocolos SSL v2/v3 y TLS v1.
- Gran variedad de librerías criptográficas.
- Muy robusto y funcional.
- Permite, entre otros, generar certificados digitales y entidades certificadoras.
- Desarrollado por Eric. A Young y Tim J.Hudson.



## Sistemas de Correo en GNU/Linux

### **Creación Certificados**

---

- Configuración de archivos
- Generar los archivos necesarios
  - Directorios necesarios
  - Archivos para registrar los certificados expedidos
  - CA
    - Clave privada
    - Certificado autofirmado
  - Servidor donde instalar el certificado
    - Clave privada
    - Solicitud de certificado para el servidor
    - Certificado del servidor firmado por el CA



## Sistemas de Correo en GNU/Linux

# Configuración de Archivos

---

```
openssl.cnf [Debian: /etc/ssl/openssl.cnf]

[ CA_default ]
# Directorio donde reside la CA q estamos creando
dir                = .
# Directorio para las listas de cert. revocados
crl_dir            = $dir/crl
# Base de datos con los certificados creados
database           = $dir/index.txt
# Directorio para alojar los nuevos certificados
new_certs_dir      = $dir/newcerts
# Certificado de la CA
certificate         = $dir/ironCA.crt.pem
# Número de serie
serial             = $dir/serial
# Clave Privada
private_key        = $dir/private/ironCA.key.pem
# Duración del certificado del servidor
default_days       = 3650
```



## Sistemas de Correo en GNU/Linux

### **Archivos Necesarios**

---

- Directorios Necesarios

```
# Directorio donde almacenaremos todos lo  
# relativo a los certificados  
# mkdir /etc/ssl/ironCA/
```

```
# Directorio para almacenar la KEY de la CA  
# mkdir /etc/ssl/ironCA/private
```

```
# Directorio para almacenar los nuevos certificados  
# mkdir /etc/ssl/ironCA/newcerts
```

```
# Directorio para almacenar los certificados revocados  
# mkdir /etc/ssl/ironCA/crl
```

# 9



## Sistemas de Correo en GNU/Linux

### **Archivos Necesarios**

---

- Archivos para registrar certificados expedidos

```
# Número de serie para el siguiente certificado
```

```
# echo "01" > /etc/ssl/ironCA/serial
```

```
# Registro de los certificados expedidos
```

```
# touch /etc/ssl/ironCA/index.txt
```



## Sistemas de Correo en GNU/Linux

### **Archivos Necesarios – CA**

---

- Generar la clave privada y el certificado autofirmado del CA

```
# openssl req -new -x509 -keyout private/ironCA.key.pem  
-out ironCA.crt.pem
```

```
Generating a 1024 bit RSA private key
```

```
.....+++  
+++
```

```
.....+++++
```

```
writing new private key to 'private/ironCA.key.pem'
```

```
Enter PEM pass phrase:
```

```
Verifying - Enter PEM pass phrase:
```

```
phrase is too short, needs to be at least 4 chars
```

```
Enter PEM pass phrase:
```

```
Verifying - Enter PEM pass phrase:
```

```
-----
```



## Sistemas de Correo en GNU/Linux

# Archivos Necesarios – CA

---

-----

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:**ES**  
State or Province Name (full name) [Some-State]:**Bizkaia**  
Locality Name (eg, city) []:**Bilbao**  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:  
**Irontec - Internet y Sistemas sobre GNU/Linux**  
Organizational Unit Name (eg, section) []:**Sistemas**  
Common Name (eg, YOUR name) []:**ca.irontec.com**  
Email Address []:**sistemas@irontec.com**



## Archivos Necesarios – Servidor

- Generar la clave privada y solicitud de certificado del servidor

```
# openssl req -new -nodes -keyout  
mail.irontec.com.key.pem -out mail.irontec.com.csr.pem
```

```
Generating a 1024 bit RSA private key
```

```
.....++++++  
.++++++
```

```
writing new private key to 'mail.irontec.com.key.pem'
```

```
-----
```

```
You are about to be asked to enter information that will be  
incorporated
```

```
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name  
or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
-----
```

# 9



## Sistemas de Correo en GNU/Linux

### Archivos Necesarios – Servidor

-----

```
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Bizkaia
Locality Name (eg, city) []:Bilbao
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Irontec
Organizational Unit Name (eg, section) []:Sistemas
Common Name (eg, YOUR name) []:mail.irontec.com
Email Address []:sistemas@irontec.com
```

Please enter the following 'extra' attributes  
to be sent with your certificate request

A challenge password []:

An optional company name []:



### Archivos Necesarios – Servidor

- Generar el certificado para el servidor firmado por la CA

```
# openssl ca -out mail.irontec.com.crt.pem -in  
mail.irontec.com.csr.pem
```

```
Using configuration from /usr/lib/ssl/openssl.cnf  
Enter pass phrase for ./private/ironCA.key.pem:  
Check that the request matches the signature  
Signature ok
```

Certificate Details:

Serial Number: 1 (0x1)

Validity

Not Before: Apr 23 20:27:55 2004 GMT

Not After : Apr 21 20:27:55 2014 GMT

Subject:

```
countryName           = ES  
stateOrProvinceName  = Bizkaia  
organizationName     = Irontec  
organizationalUnitName = Sistemas  
commonName           = mail.irontec.com  
emailAddress         = sistemas@irontec.com
```

**196 - 203**

*Iker Sagasti Markina*  
<iker@irontec.com>



## Sistemas de Correo en GNU/Linux

### Archivos Necesarios – Servidor

---

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

OpenSSL Generated Certificate

X509v3 Subject Key Identifier:

B2:E3:08:2D:97:93:6A:4E:09:1B:8D:56:6F:2E:D2:9D:61:27:82:26

X509v3 Authority Key Identifier:

keyid:66:C5:16:53:32:5A:2A:75:89:63:98:22:CA:2A:69:54:86:7A:C0:A0

DirName:/C=ES/ST=Bizkaia/L=Bilbao/O=Irontec/OU=Sistemas/CN=ca.iron  
tec.com/emailAddress=sistemas@irontec.com

serial:00

Certificate is to be certified until Feb 21 20:27:55 2015 GMT  
(3650 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated



## Sistemas de Correo en GNU/Linux

### **Comprobaciones**

---

- Comprobar que nos ha creado un listado similar de archivos y directorios

```
ironCA$ ls -RF
.:
crl/                index.txt.old      mail.irontec.com.csr.pem
private/
index.txt           ironCA.crt.pem    mail.irontec.com.key.pem
serial
index.txt.attr     mail.irontec.com.crt.pem  newcerts/
serial.old

./crl:

./newcerts:
01.pem

./private:
ironCA.key.pem
```



### **Comprobaciones**

---

- Examinar la clave secreta

```
openssl rsa -in ironCA.key.pem -text
```

- Examinar certificados

```
# openssl x509 -in ironCA.crt.pem -text [-noout]
```

- Comunicación correcta con servicios SSL

```
# openssl s_client -connect mail.irontec.com:993 -prexit
```



# Agradecimientos



## Sistemas de Correo en GNU/Linux

### **Agradecimientos**

---

- Irontec - <http://www.irontec.com/>
  - Por darme de comer.
- Eghost - <http://eghost.deusto.es/>
  - Por engancharme al software libre.
- Txipi, zgor, split y jabito
  - Por sus ánimos a seguir aprendiendo ;-)
- Mai:
  - Por aguantarme durante tanto tiempo.
- Fermat - <http://fermat.movimage.com/>
  - Por echarme una mano en todo esto.
- Vosotros:
  - Por aguantarme hasta aquí :-P.



# Copyright





## Sistemas de Correo en GNU/Linux

### **Licencia Copyleft**

---

- Este documento está protegido bajo la licencia Attribution-ShareAlike 2.0 de Creative Commons (<http://creativecommons.org/licenses/by-sa/2.0/>)

Copyright © 2004 Iker Sagasti Markina <iker@irontec.com>

Se permite la copia, modificación, distribución, uso comercial y realización de la obra, siempre y cuando se reconozca la autoría de la misma, a no sea ser que se obtenga permiso expreso del autor. El autor permite distribuir obras derivadas a esta sólo si mantienen la misma licencia que esta obra.

Esta nota no es la licencia completa de la obra, sino una traducción de la nota orientativa de la licencia original completa (jurídicamente válida).