El servidor de correo en el CAY

P. de Vicente

Informe Técnico IT-OAN/CAY 2002-5

Índice

1. Propósito del informe

Este informe describe la instalación, configuración y métodos de mantenimiento del sistema de correo implementado en el servidor de correo del Centro Astronómico de Yebes.

El CAY dispone de una subclase de la clase C que define al “oan.es”, y también dispone de un subdominio denominado “cay.oan.es”, definido en el DNS del OAN. En dicho DNS el servidor de correo primario para dicho subdominio es “zeus.cay.oan.es”, un Pentium III con GNU/Linux Debian 3.0, y 256 Mb de memoria RAM. Este informe describe el sistema de correo implementado en esta máquina.

2. El sistema de correo

Un sistema de correo es aquel que permite que los clientes de una red local intercambien correo entre sí y con el exterior. Habitualmente los usuarios disponen de un ordenador personal conectado a la red local con una aplicación cliente de correo con la que reciben, envian y gestionan sus mensajes. Dicho cliente transfiere los mensajes desde/hacia el servidor utilizando diferentes protocolos de transferencia, habitualmente SMTP de envio y POP3 de recepción.

Los mensajes procedentes del exterior entran directamente desde la máquina que los envia a la estafeta de correo definida en el DNS para dicho dominio. Habitualmente la negociación de la transferencia se hace mediante el protocolo Simple Mail Transport Protocol (SMTP). Una vez en el servidor los mensajes permanecen en un área común distribuidos por usuario hasta que los clientes de correo individuales los recogen de allí.

Los clientes de correo necesitan autentificarse ante el servidor, enviando un nombre de usuario y una contraseña que le permita acceder al archivo que contiene los mensajes de dicho usuario. Existen dos métodos básicos de autentificación,

- autentificación en claro, en la que el nombre del usuario y la contraseña se transmiten en claro,
- autentificación cifrada, en la que el nombre del usuario y la contraseña se envian cifradas a través de una capa de transporte seguro.

Existen además dos protocolos de transporte con distintas funcionalidades, POP3 e IMAP.

- El protocolo POP3 permite descargar los mensajes recibidos desde un cliente de correo, manteniendo una copia o borrando la copia del servidor. El almacenamiento de los mensajes se hace en el disco duro del ordenador personal de cada usuario.
- El protocolo IMAP permite gestionar el correo desde un cliente de correo local, pero manteniendo todas las carpetas y mensajes en el servidor.

El envio de mensajes desde los clientes de correo hasta el servidor se hace habitualmente empleando el protocolo SMTP. Existen dos modos de enviar los mensajes, sin autentificación y con autentificación. En el primero de los casos el cliente de correo envia su mensaje a la estafeta. En el segundo es necesario que el cliente de correo suministre un nombre de usuario y

una contraseña que le autentifiquen ante el servidor. Este, de acuerdo con la política de seguridad establecida, puede aceptar o no el reenvio del mensaje hacia su destino. La autentificación se puede hacer en claro o empleando una capa de transporte seguro en la que la información transferida se cifra.

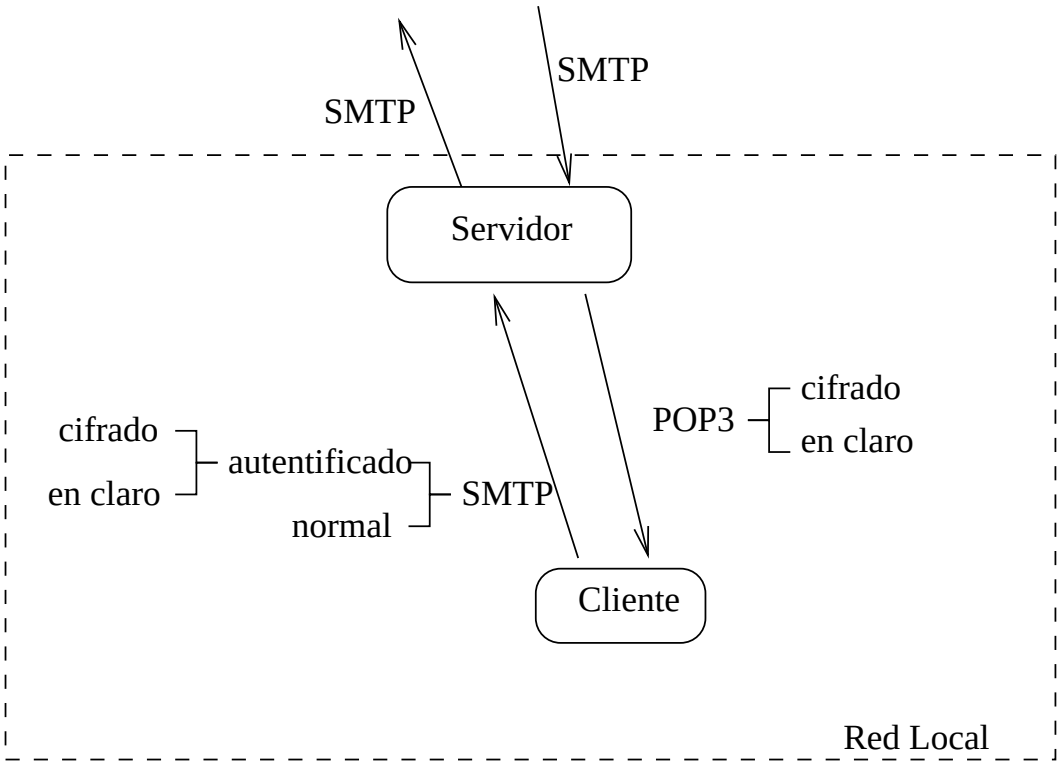

Figura 1: *Diagrama del flujo habitual de los mensajes de correo de/a una red local*

3. El correo en el CAY

3.1. El correo entrante

Los usuarios del Observatorio Astronómico Nacional (OAN) disponen de una dirección de correo del tipo “usuario@oan.es”, aunque por motivos históricos aquellos usuarios con su puesto de trabajo en el Centro Astronómico de Yebes (CAY) conservan todavía la dirección “usuario@cay.oan.es”, actualmente en desuso.

Los mensajes dirigidos a los usuarios del CAY con direcciones “@oan.es” se reciben en la estafeta principal del OAN: “conga.oan.es” y desde allí se redirigen a las direcciones “usuario@cay.oan.es”, de acuerdo con la lista de “aliases” (apodos o sinónimos) almacenada en “conga.oan.es”. “conga.oan.es” consulta en el DNS la estafeta del subdominio “cay.oan.es” y entrega los mensajes a dicha máquina.

Los mensajes dirigidos directamente a usuarios con direcciones “cay.oan.es” se reciben directamente en la estafeta de correo principal del subdominio “cay.oan.es”: “zeus.cay.oan.es”.

La figura 2 representa esquemáticamente la entrada y salida de mensajes hacia/desde el CAY.

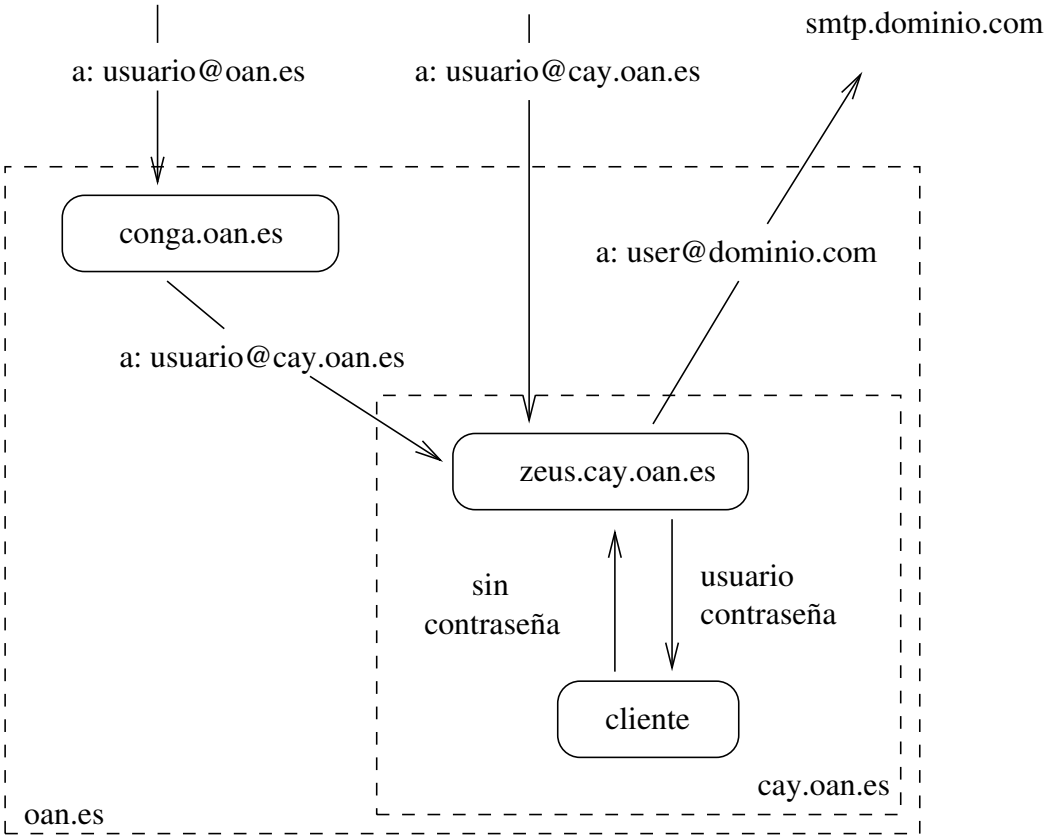

Figura 2: *Diagrama del flujo habitual de los mensajes de correo de/a una red local*

3.2. Las estafetas de correo del CAY

Para poder consultar las estafetas de correo disponibles para atender el correo del CAY y su prioridad se puede ejecutar la instrucción:

```
host -t mx cay.oan.es
```

que produce el siguiente resultado:

```
cay.oan.es              MX      300 mail.rediris.es
cay.oan.es              MX      100 zeus.cay.oan.es
cay.oan.es              MX      150 siva.cay.oan.es
cay.oan.es              MX      200 conga.oan.es
```

La estafeta de correo principal del subdominio “cay.oan.es” es “zeus.cay.oan.es”. La estafeta de correo secundaria es “siva.cay.oan.es”, y entra en marcha en caso de fallo del servidor primario. La estafeta terciaria es “conga.oan.es” y reside en la sede del OAN en Alcalá de Henares.

Entra en marcha en el caso en el que la línea punto a punto con Yebes sufra una avería. Finalmente la estafeta de correo de más baja prioridad es “mail.rediris.es” que recoge los mensajes dirigidos a “cay.oan.es” en caso de que ninguna de las máquinas anteriores se pueda hacer cargo de ellos.

3.3. El correo saliente

El correo es enviado desde los diferentes clientes, usualmente en PCs individuales, hacia el servidor. Una vez en el servidor, éste indaga, mediante una consulta al DNS, cuál es la estafeta de correo correspondiente al dominio del destinatario, y entrega el mensaje directamente a dicha máquina. En la figura 2 se muestra un ejemplo en el que un mensaje dirigido a “usuario@dominio.com” es enviado “smtp.dominio.com” que es la estafeta de correo de “dominio.com”.

Para evitar el uso malicioso de envio de correo, el router del OAN tiene filtrados los puertos SMTP de entrada y salida, restringiendo su uso a las máquinas autorizadas para realizar estas operaciones. Para obtener más detalles sobre esta política consultar el informe IT-OAN/CAY-.

4. Exim, un sendmail más sencillo

Exim es un MTA (Mail Transport Agent) en una máquina conectada a Internet, que recibe y envia correo desde y hacia el exterior y distribuye dicho correo localmente. La transferencia de los mensajes a/desde el exterior se hace mediante el protocolo SMTP. Esta aplicación no gestiona la entrega de mensajes mediante POP3 o IMAP.

Exim ha sido desarrollado por la Universidad de Cambridge, que proporciona prácticamente las mismas funcionalidades que *sendmail*, y que resulta más sencilla de configurar, y aunque no dispone de toda la potencia y flexibilidad de *sendmail*, cubre todas las necesidades del OAN y es más seguro que aquel.

La instalación de *Exim* se hace utilizando `apt-get`:

```
apt-get install exim eximon exim-doc exim-doc-html
```

- *eximon* es una utilidad auxiliar para monitorizar la cola de mensajes.
- *exim-doc* es un paquete con la documentación completa de *Exim* comprimida.
- *exim-doc-html* es un paquete con la documentación de *Exim* en formato HTML, lo que permite realizar consultas cómodamente utilizando un navegador.

Exim se puede instalar de modo que al arrancar el servidor de correo el proceso se inicie desde el superdemonio *inetd* o se inicie como demonio individual. El comportamiento predeterminado es que el proceso sea lanzado desde *inetd*. Esta opción se puede desactivar eliminando la entrada de *smtp* del archivo `etc/inetd.conf`. No es suficiente comentarla, sino que es necesario borrarla totalmente. Si la entrada se elimina, el archivo `/etc/init.d/exim` iniciará el demonio correspondiente.

Esta última opción de inicio puede resultar muy útil si se desea depurar la configuración de *Exim* y observar con detalle la negociación que establece *Exim* con otros agentes de transporte. El inicio de *Exim* en modo de depuración se hace del siguiente modo:

```
exim -d9
```

El número que sigue a la opción `-d` indica el nivel de depuración del demonio. 9 es el máximo valor, 10 ofrece detalles adicionales sobre la aplicación de reglas de filtrado y 11 permite observar las peticiones al DNS.

Durante la instalación de `Exim` se pone en marcha un procedimiento que hace una serie de preguntas sencillas para poder configurar el servidor de correo en la máquina sobre la que se realiza la instalación. Para poder acceder de nuevo a dicho procedimiento no es necesario instalar de nuevo el paquete, ya que basta introducir:

```
/usr/sbin/eximconfig
```

Aunque sencillo, este procedimiento de configuración carece de flexibilidad por lo que sólo es recomendable su uso para máquinas que no actuen como estafetas como correo. El mejor método de configuración es editar manualmente el archivo `/etc/exim/exim.conf`

5. Configuración de Exim

En el apéndice 1 se incluye el archivo de configuración para “zeus.cay.oan.es”. En esta sección analizaremos algunas de sus partes, en particular aquellas que nos parecen más relevantes. Algunas de las secciones no se discuten aquí porque sus valores son los predefinidos.

El archivo `/etc/exim/exim.conf` está dividido en diferentes secciones. En algunas de estas secciones el orden de los parámetros de configuración es relevante y en otros no, tal y como se indica en la cabecera de cada sección.

5.1. Sección principal (MAIN)

1. `qualify_domain = cay.oan.es`

   Esta opción sólo es de aplicación a los mensajes generados localmente (en circunstancias normales) e indica que en caso de que un mensaje contenga un remitente sin dominio se le añada automáticamente el que aquí se indica. De este modo se impide que los usuarios dejen su remite sólo con su nombre, y sin dominio.

2. `qualify_recipient = zeus.cay.oan.es`

   Esta opción sólo es de aplicación a los mensajes generados localmente (en circunstancias normales) e indica que en caso de que un mensaje contenga un destinatario sin dominio se le añada automáticamente el que aquí se indica. Por tanto los mensajes generados en “zeus.cay.oan.es” y dirigidos a un usuario, se les añade el sufijo: “zeus.cay.oan.es”, de modo que se entreguen localmente.

3. `local_domains = localhost:zeus.cay.oan.es:cay.oan.es:`

   Se indica cual es/son el/los dominio/s local/es aceptado/s para recibir los mensajes. Se pueden poner varios valores separados por ":". Si se dejara en blanco nunca se podrían entregar mensajes localmente en esta máquina. Por tanto al rellenar esta línea se indica que esta máquina acepta mensajes dirigidos a "zeus.cay.oan.es", a "cay.oan.es", y aquellos generados internamente.

4. `#relay_domains = *`
   `#relay_domains_include_local_mx = true`

   Estas opciones, al ir comentadas, impiden que "zeus.cay.oan.es" reenvie mensajes a otras máquinas, incluso si "zeus.cay.oan.es" estuviera en la sección MX de su DNS. Habitualmente y por motivos de seguridad (para evitar reenvios de mensajes basura) siempre están así.

5. `never_users = root`

   No se aceptan mensajes dirigidos a "root" o el uid que aquí figure. Esta es una medida de seguridad. Para recibir mensajes en esa cuenta se puede crear un alias que lo reciba, pero sin los privilegios de "root".

6. `host_lookup = *`

   Esta instrucción es costosa en términos de CPU ya que indica a *Exim* que haga una petición al DNS para encontrar el nombre de la máquina con la que está negociando. Este nombre luego figurará en los archivos de registro permitiendo su identificación más rápida.

7. `host_accept_relay = *oan.es`

   Esta instrucción permite que reenviemos mensajes a otras máquinas del dominio "oan.es". Es decir si entrara un mensaje dirigido a un usuario que no tiene cuenta en "zeus.cay.oan.es" pero que se sabe que si tiene en otra máquina del OAN se puede reenviar dicho mensaje. En el caso del CAY esta opción sólo tiene sentido si algún usuario del CAY responde a un mensaje desde su casa, empleando un método de autentificación segura a alguien del OAN. También figura probablemente por mantener la misma configuración que las estafetas del OAN en Alcalá de Henares y en Madrid, donde los reenvios de mensajes si son útiles.

8. `auth_always_advertise = false`

   Esta instrucción está disponible cuando `Exim` está compilado con soporte de autentificación. Habitualmente *Exim* anuncia los mecanismos de autentificación ante un comando EHLO. Al elegir la opción "false" *Exim* no anuncia que dispone de AUTH aunque está preparado para aceptarlo. Ciertos clientes de correo como Netscape precisan que se introduzca el usuario y la contraseña aunque realmente no sea necesario, porque la máquina desde la que se hace la negociación figura en una lista definida por el parámetro `host_accept_relay`. En el CAY, donde hay usuarios que emplean *Netscape*, esta

opción es imprescindible para impedir que *Netscape* solicite continuamente el nombre y la contraseña del usuario.

9. `tls_advertise_hosts = *`

   Esta opción es necesaria para anunciar al cliente la disponibilidad del comando START-TLS. Todas las máquinas reciben este anuncio. Todas las opciones con TLS (Seguridad en la capa de transporte), precisan que `Exim` esté compilado con soporte TLS.

   Para que `Exim` funcione como servidor con TLS, esto no es suficiente, son necesarias las siguientes dos opciones:

10. ```
    tls_certificate = /etc/exim/certificado
    tls_privatekey = /etc/exim/clave
    ```

    Estas opciones indican los archivos donde residen el certificado X509 y la clave privada asociado a él. Estos archivos deben ser leidos por el usuario de Exim. Sin el certificado los clientes de correo no funcionarán. Los archivos anteriores se generan empleando la siguiente instrucción:

    ```
    openssl req -x509 -newkey rsa:1024 -keyout clave
         -out certificado -days 9999 -nodes
    ```

11. `auth_over_tls_hosts = *`

    Esta directiva explicita que la autentificación se debe realizar iniciando una sesión TLS primero.

12. `host_auth_accept_relay = *`

    Esta instrucción sobresee la instrucción en la que se impide el reenvio de mensajes. Es decir si algún usuario se autentifica, puede emplear “zeus.cay.oan.es” para reenviar mensajes. Este es el caso típico de alguien que recibe los mensajes del OAN en su casa y desea contestar desde allí al remitente. Si no está autentificado “zeus.cay.oan.es” no permitirá la salida de ese mensaje, salvo que la directiva `host_accept_relay` explicite algo diferente.

13. `sender_address_relay = *oan.es`

    Esta instrucción indica que para que “zeus.cay,oan.es” reenvie un mensaje la dirección de remite debe contener la cadena “oan.es”. De lo contrario, incluso aunque el usuario esté autentificado, el mensaje no se reenviará. De este modo se impide que los usuarios pongan el remite de su casa y empleen “zeus.cay.oan.es” como enviador de mensajes.

5.2. Sección Reintentar (RETRY)

Esta sección contiene una instrucción que indica la frecuencia con la que se deben entregar los mensajes en caso de error temporal en la conexión o en la entrega de mensajes desde `zeus.cay.oan.es` hacia el exterior:
    ```

```
# Domain                Error       Retries
# ------                -----       -------

*                       *           F,2h,15m; G,16h,2h,1.5; F,4d,8h
```

Las letras F y G significan: F intentar en intervalos fijos, G en intervalos geométricos. Por tanto en caso de error en la conexión intentar: las dos primeras horas cada 15 minutos, las 16 horas siguentes en intervalos de 2 horas aumentando el intervalo en 1.5 veces. Es decir 2 horas, 2 x 1.5 = 3 horas, 6 horas, ... y luego durante los 4 siguientes días en intervalos fijos de 8 horas.

Esta regla es de aplicación para todos los dominios y para todo tipo de errores.

Las reglas se pueden refinar bastante, en función de los dominios y del tipo de error. Para más información consultar la documentación de `Exim`

5.3. Sección Reescribir (REWRITE)

Esta sección permite sobreescribir algunos de los campos de las cabeceras de los mensajes. Según la recomendación RFC 822, la dirección puede constar de los siguientes campos, que `Exim` identifica con las letras que figuran al lado:

sender	s
from	f
to	t
cc	c
bcc	b
reply-to	r
env-from	F
env-to	T

Los campos con “envelope” son direcciones de remite o destino que se han añadido a las cabeceras de los mensajes desde las estafetas de correo para redirigir los mensajes a la máquina adecuada.

En el caso del CAY existen 3 entradas:

1. ```
   *@zeus.cay.oan.es    ${lookup{$1}lsearch{/etc/email-addresses}\
                                    {$value}fail} frFs
   ```

   Esta instrucción indica que todos aquellos mensajes cuya cabecera contenga en el campo “from”, “reply”, “Sender” o “From envelope” se sustituyan por el nombre del mismo usuario con el formato que figura en el archivo `/etc/email-addresses`.

   En realidad en `zeus.cay.oan.es` dicho archivo esta vacío y por tanto la instrucción no es de aplicación. Sería de aplicación si alguien del OAN hubiese abandonado por ejemplo el centro y deseamos que en dichos campos de la cabecera figure otra dirección de remite.
   ```

2. `*@*oan.es  $1@oan.es  frFs`

   Esta instrucción es muy útil para hacer que los remites y las direcciones de envio de las usuarios que contengan algo del tipo “oan.es” se transformen en “oan.es”. Es decir un usuario que envie un mensaje con el remite “usuario@cay.oan.es” se le modifica dicho campo poniendo “usuario@oan.es”

3. `*@oan.es  $1@${qualify_domain}  X`

   Esta instrucción indica que sólo aquellos usuarios con cuenta en esta máquina pueden enviar correo fuera y recibirlo aquí.

5.4. Sección Autentificación (AUTHENTICATION)

Esta sección contiene información sobre la comprobación de los nombres de usuarios y sus contraseñas para poder autentificar a un usuario cuando es necesario. Existen dos métodos soportados por el servidor de correo: “plain” y “login”. En el primero el cliente de correo envia el nombre de usuario y la contraseña directamente, en el segundo el cliente envia dicha información una vez que el servidor se la demanda en forma de `Username:: : Password::`.

En ambos casos se comprueban los dos campos enviados con una tabla en el archivo `/etc/exim/passwd`.

```
plain:
driver = plaintext
public_name = PLAIN
server_condition = "${if crypteq{$2}{${extract{1}{:}{${lookup{$1}lsearch{/etc
/exim/passwd}{$value}{*:*}}}}}{1}{0}}"
server_set_id = $1
#
login:
driver = plaintext
public_name = LOGIN
server_prompts = "Username:: : Password::"
server_condition = "${if crypteq{$2}{${extract{1}{:}{${lookup{$1}lsearch{/etc
/exim/passwd}{$value}{*:*}}}}}{1}{0}}"
server_set_id = $1
```

El archivo `/etc/exim/passwd` contiene una serie de entradas del tipo: *usuario1:contraseña1cifrada*, donde la contraseña cifrada se puede conseguir empleando la siguiente instrucción:

```
perl -e "print crypt('contraseña','xy'),\"\n\";"
```

donde “contraseña” es una contraseña y “xy” son dos caracteres cualquesquiera. El resultado de esta instrucción es una contraseña cifrada que es la que se introduce en el archivo anterior.

6. Entrega del correo a los clientes

Cada usuario del CAY tiene la posibilidad de recibir y enviar su correo electrónico desde su máquina personal, que puede hacer funcionar en el sistema operativo que desee. También es posible gestionar el correo desde el servidor central, ya que todo el personal del CAY dispone de cuenta en el servidor central.

La entrega de correo en el CAY desde el servidor hacia los clientes se realiza mediante dos protocoloes diferentes, POP3 e IMAP. El protocolo POP3 permite descargar los mensajes recibidos desde un cliente de correo, manteniendo una copia o borrando la copia del servidor. La gestión y almacenamiento de los mensajes se hace localmente en el cliente de correo de cada usuario. El protocolo IMAP permite gestionar el correo desde un cliente de correo local, pero manteniendo todas las carpetas y mensajes en el servidor.

Los clientes de correo, utilizan un nombre de usuario y contraseña para poder acceder al servidor. Dado que las contraseñas se transmiten en claro y que ello es un posible riesgo de seguridad, se ha instalado en el servidor protocolos de transporte POP e IMAP seguros. La transferencia de información se hacen utilizando una capa de transporte seguro que cifra las comunicaciones entre el cliente y el servidor. Esta facilidad es opcional dentro de la red local del OAN y obligatoria si el acceso se hace desde el exterior del OAN, ya que el router tiene filtrados los puertos de acceso normales para POP e IMAP.

Los paquetes que permiten dicha funcionalidad son: `ipopd-ssl` y `uw-imapd-ssl`. Ambos paquetes suministran demonios POP3 e IMAP que funcionan con transmisión de información en claro y cifrada, dependiendo de lo que utilice el cliente de correo.

7. Configuración de los clientes de correo en un entorno seguro

Los clientes de correo en el CAY se dividen en dos tipos, aquellos que se ejecutan sobre MS-Windows, y aquellos que funcionan sobre Linux. Dentro de los primeros se emplean “Netscape” y “Microsoft-Outlook”. En el segundo caso se suele emplear “Kmail” y “Netscape”.

Las versiones 4.x de Netscape no funcionan adecuadamente con transporte seguro. Las versiones 6.x no han sido probadas todavía.

7.1. Configuración de Outlook en modo de transferencia seguro

Para poder recuperar el correo con POP3 y SSL en Outlook Express se deben seguir las siguientes instrucciones:

1. Pulsar sobre: Herramientas ->Cuentas...
2. Se abrirá una ventana con varias pestañas en la parte superior y un recuadro con fondo blanco con nombres de algunas cuentas de correo y de otras cosas más. Pulsar sobre el icono: Agregar... ->Correo

3. Rellenar el formulario:

   `Nombre`: un nombre identificativo
   `Dirección`: usuario@oan.es
   `Servidor de correo entrante`: POP3
   `Servidor de correo entrante (POP3)`: zeus.cay.oan.es
   `Servidor de correo saliente (SMTP)`: zeus.cay.oan.es

   `Iniciar sesion utilizando`:
   `Nombre de cuenta POP`: usuario
   `Contraseña`: contraseña_del_usuario
   `Nombre de correo de Internet`: zeus.cay.oan.es

   `Conectar por medio de la línea telefónica`
   Esta sección se debe rellenar dependiendo de la ubicación de la máquina cliente. Si está en la red local del OAN, no es necesario completar esta sección.

   Si la máquina está fuera del observatorio y el acceso es por línea telefónica completar los campos utilizando información sobe el modem y el proveedor de Internet que se utilice.

4. La ventana con múltiples pestañas y el recuadro blanco deben estar todavía en pantalla. Seleccionar "zeus.cay.oan.es" en el recuadro blanco y pulsar sobre `Modificar` o `Propiedades` (situado a la derecha de dicho recuadro):

5. Se abre una nueva ventana con 5 pestañas en la parte superior. Pulsar sobre la pestaña `Avanzada` y marcar la casilla que dice `Este servidor necesita una conexión segura (SSL)`, y seleccionar la casilla `Mantener una copia de los mensajes en el servidor` **sólamente** si el acceso se hace desde fuera del OAN.

6. Si se desea responder desde fuera del OAN se debe suministrar una contraseña al administrador del sistema, del modo explicado en la sección 5.4:

   a) Seleccionar en la ventana de las 5 pestañas en la parte superior, la pestaña `Servidores` y marcar la casilla `Mi servidor requiere autentificacion` y pulsar `Configuración`.

   b) Se abre una ventana, marcar la casilla `Iniciar sesión utilizando` y rellenar los campos `Nombre de cuenta` y `Contraseña` el nombre de usuario y la contraseña sin cifrar que se ha generado más arriba o si la contraseña coincide con la del servidor de correo entrante, marcar la casilla `Usar misma configuración que el servidor de correo entrante`.

El uso de Outlook Express empleando el modo seguro genera unos mensajes de error indicando que el servidor no tiene un certificado de seguridad. Se puede obviar el mensaje y continuar con la descarga de mensajes.

7.2. Configuración de Kmail en modo de transferencia seguro

Versión presente en KDE versiones 3.0.x

1. Pulsar sobre `Preferencias ->Configurar KMail...`
2. Pulsar sobre el icono `Red`
3. Seleccionar la pestaña `Recibiendo` y seleccionar la máquina "zeus.cay.oan.es", si ya estuviera definida, y pulsar `Modificar...` Si no lo estuviera, pulsar sobre `Añadir...` En este último caso seleccionar `POP3`.
4. Rellenar el formulario "Tipo de cuenta POP" con: `Nombre`: un nombre identificativo.
   `Usuario`: el nombre de usuario
   `Contraseña`: la contraseña
   `Servidor`: zeus.cay.oan.es
   `Puerto`: 995

   Seleccionar las opciones `Guardar contraseña` y las que se consideren adecuadas del resto de las existentes.
5. Pulsar sobre la pestaña `Extras` y en la sección `Cifrado` seleccionar la casilla: `Usar SSL para recibir el correo de forma segura` o pulsar sobre el botón `Comprueba que soporta el servidor`. Se seleccionará automáticamente el protocolo de transporte seguro, y el método de autentificación. .
6. Para enviar correo de modo seguro, seleccionar la pestaña `Enviando`
7. Seleccionar el perfil deseado con el que se hace la conexión SMTP, pulsar `Modificar`. Si la conexión se hace desde fuera del OAN:
   a) Seleccionar la opción `el servidor requiere autentificación` y rellenar los campos `Usuario` y `Contraseña`, donde la contraseña es aquella que se menciona en la sección 5.4.
   b) Pulsar sobre la pestaña `Seguridad` y pulsar sobre el botón `Comprueba que soporta el servidor`. Se debería activar la casilla TLS.

8. Gestión del servidor de correo

El servidor de correo está permanentemente en marcha de modo que si el sistema recibe una petición de negociación SMTP, este responde inmediatamente. Los mensajes salientes también son enviados inmediatamente. Sólo en aquellos casos en los que la negociación resulta fallida, debido por ejemplo a falta de conexión con la otra máquina negociadora, los mensajes quedan almacenados en una cola donde son procesados más tarde, con una periodicidad definida en el archivo de configuración `/etc/cron.d/exim`:

```
08,23,38,53 *     * * *     mail
if [ -x /usr/sbin/exim -a -f /etc/exim/exim.conf ];
then /usr/sbin/exim -q ; fi
```

Cada mensaje es luego procesado con la periodicidad que se haya establecido en el archivo de configuración `/etc/exim/exim.conf` (sección 4.2).

Exim guarda registro de su actividad en el directorio `/var/log/exim` donde se genera un informe en tiempo real para cada día. Sólo se conserva la información de los últimos 7 días, ya que los archivos de registro son reciclados periódicamente por una tarea a tal efecto.

Los mensajes en cola de espera quedan almacenados en el directorio `/var/spool/input` en dos archivos diferentes. Aquellos archivos cuyo nombre finaliza en H, contienen la cabecera del mensaje así como información de procesado del propio mensaje. Los archivos cuyo nombre finaliza en D contienen el cuerpo del mensaje. El directorio `/var/spool/msglog` contiene un mensaje de registro por cada mensaje fallido en su entrega y que figura en el directorio `/var/spool/input`.

Es posible obtener estadísticas de la actividad de *Exim* empleando la utilidad *eximstats*. De hecho es posible recibir por correo electrónico el informe de dicha actividad descomentando la entrada correspondiente en `/etc/cron.daily/exim`. En caso de ejecutarse interactivamente la instrucción adecuada es:

```
eximstats </var/log/exim/mainlog
```

eximstats extrae la información de los archivos de registro y genera un informe detallado de los mensajes enviados y recibidos, en el que se muestra el volumen de datos transferidos, el número de mensajes, el flujo entrante y saliente en función de la hora, el tiempo de espera en la cola, los mensajes reenviados, los destinos más frecuentes, los usuarios más utilizadores, etc....

8.1. Bases de datos

Para la gestión de los mensajes en cola existen 3 bases de datos en el directorio `/var/spool/db` que se pueden visualizar empleando los siguientes comandos:

```
exim_dumpdb /var/spool/exim retry
exim_dumpdb /var/spool/exim reject
exim_dumpdb /var/spool/exim wait-remote_smtp
```

Por ejemplo el primero de los comandos produce una salida de este tipo:

```
T:xuxa.gr.ssr.upm.es:138.4.37.12 110 77 Connection timed out
13-May-2002 11:43:46  27-Jun-2002 13:18:21  27-Jun-2002 21:18:21 *
T:mail2.dit.upm.es:138.4.2.8 110 77 Connection timed out
03-Jun-2002 09:55:15  06-Jun-2002 12:26:05  06-Jun-2002 20:26:05
```

El primer caracter se refiere al tipo de reintento que se debe hacer. Existen tres opciones, D (directing), R (routing) T(transport). El siguiente campo contiene la dirección local o la remota, seguida del número IP. Los siguientes campos contienen códigos de error y una descripción de

este. Los tres tiempos que figuran a continuación son el momento del primer error, el momento del último intento, y el momento estimado del siguiente intento. Si este último momento excede la hora y fecha actual la línea queda marcada con un asterisco final.

Para eliminar los registros de las bases de datos se emplea la instrucción

```
exim_tidydb -t 7d /var/spool/exim retry
```

donde en el ejemplo anterior indicamos que se eliminen todos aquellos mensajes con una antigüedad superior a 7 días. El valor predefinido, es decir si la instrucción anterior se ejecuta sin opciones, de limpieza es 30 días. Este comando se ejecuta cada día desde el archivo `/etc/cron.daily` por lo que en general no es necesario ejecutarlo a mano.

Se puede conocer cuando se procesará un cierto mensaje en cola empleando el comando:

```
exinext clarin.disam.upm.es
```

que produce una salida del tipo:

```
Deliver: clarin.disam.upm.es [138.100.76.2] error 110: Connection timed o
first failed: 28-Jun-2002 09:42:48
last tried:   28-Jun-2002 09:42:48
next try at:  28-Jun-2002 09:57:48
```

También se pueden editar/modificar mensajes individuales en la base de datos empleando la siguiente instrucción:

```
exim\_fixdb /var/spool/exim retry
```

Por ejemplo:

```
exim\_fixdb /var/spool/exim retry
> T:fenix.eui.upm.es:138.100.56.25
0 error number: 110 Connection timed out
1 extra data:   77
2 first failed: 14-Nov-2001 13:53:14
3 last try:     07-Dec-2001 22:21:04
4 next try:     08-Dec-2001 06:21:04
5 expired:      yes
> 4 011210:1100
0 error number: 110 Connection timed out
1 extra data:   77
2 first failed: 14-Nov-2001 13:53:14
3 last try:     07-Dec-2001 22:21:04
4 next try:     10-Dec-2001 11:00:00
5 expired:      yes
> CTRL-D
```

modifica la fecha del siguiente intento desde el 08-Dec-2001 a las 06:21:04 a 10-Dec-2001 a las 11:00:00.

En el resto de las bases de datos sólo es posible borrar mensajes y no modificarlos.

Este tipo de operaciones a veces no limpia totalmente los mensajes pendientes y en esos casos es conveniente examinar y corregir manualmente la cola.

8.2. La cola de mensajes

Para examinar la cola de mensajes se puede ejecutar la instrucción:

```
mailq
```

y si se desea un resumen organizado se puede emplear la instrucción:

```
mailq | exiqsumm
```

que produce una salida del tipo:

```
Count  Volume  Oldest  Newest  Domain
-----  ------  ------  ------  ------
3    28KB     34d     22d  hotmail.com
1    1740     35d     35d  miraaclebereast.net
2    31KB     39d     33d  mixmal.es
1   105KB     18d     18d  pccasting.com
1    3072      4d      4d  raginent.com
1    6041     18d     18d  trafficmagnet.net
1    2252     22d     22d  trutee.com
1    25KB     28d     28d  uol.com.ar
1    23KB      9d      9d  wxunicom.com
1    7577     25d     25d  yahoo.com.ar
2    2969     20d     16d  yahoo.es
```

La cola también se puede monitorizar gráficamente con la utilidad `eximon`. Situandose con el cursor sobre la lista y pulsando Mayúsculas + botón derecho del ratón aparece un menú de contexto que permite manipular los mensajes de la cola.

También es posible eliminar los mensajes manualmente del directorio `/var/spool/input`. Para ello se pueden ordenar temporalmente en orden inverso introduciendo:

```
ls -lrt
```

Los tres primeros números en hexadecimal que componen el nombre del mensaje identifican el día. Por tanto se pueden borrar del siguiente modo:

```
rm 16A*
cd ../msglog
rm 16A*
```

Se puede forzar el inicio de la ejecución de la cola, obviando las reglas temporales de reintentos, empleando la instrucción:

```
exim -qf
```

y se puede tratar de desatascar un mensaje particular empleando la instrucción:

```
exim -M 10hCET-0000Bf-00
```