ADMINISTRACIÓN DE REDES Y SISTEMAS

PRÁCTICAS DE LABORATORIO

Correo electrónico

El correo electrónico es uno de los servicios más usados en la Internet. En esta práctica se instala y configura una estafeta de correo con Postfix y Dovecot.

Requisitos previos

Tarea 1: Asegúrese de que todos los sistemas que va a usar en esta práctica tienen un nombre de máquina FQDN válido (`hostname -f`), es decir, un nombre con traducción en el DNS.

Tarea 2: Compruebe que todos los sistemas que va a usar en esta práctica pueden traducir nombres de DNS de su dominio (`xxx.mucs.es`) y de cualquier otro dominio de la Internet.

Instalación de Postfix

Tarea 3: Instale con `pkg` el paquete `postfix` en una máquina de la red interna. Después hay que ejecutar varios mandatos adicionales para desactivar Sendmail (estafeta de correo por defecto en FreeBSD) y habilitar Postfix. Para concretar, hay que hacer lo siguiente:

Instalar el paquete:

```
pkg install postfix
```

Deshabilitar Sendmail y habilitar Postfix:

```
service sendmail stop
sysrc postfix_enable="YES"
sysrc sendmail_enable="NONE"
mkdir /usr/local/etc/mail
install -m 0644 /usr/local/share/postfix/mailer.conf.postfix
/usr/local/etc/mail/mailer.conf      ← Ojo: esto es parte de la línea anterior
newaliases
```

Añadir a `/etc/periodic.conf` las líneas indicadas en el mensaje de instalación (esto cancela la ejecución de diversas tareas de mantenimiento periódico de Sendmail):

```
daily_clean_hoststat_enable="NO"
daily_status_mail_rejects_enable="NO"
daily_status_include_submit_mailq="NO"
daily_submit_queuerun="NO"
```

Tarea 4: Lance el servicio `postfix` y compruebe que no aparecen errores en `/var/log/maillog`.

Envío de mensajes locales

Tal como se instala de serie, Postfix funciona como estafeta local. Es capaz de enviar mensajes a cualquier destino y aceptar mensajes para usuarios locales. Las siguientes tareas se van a centrar en el envío de los mensajes.

Use el programa `mail` para leer y escribir mensajes. Es muy básico, pero de momento será suficiente. Otra opción interesante de explorar, aunque también sea rudimentaria, es usar `telnet` o `nc` para escribir directamente las órdenes necesarias del protocolo SMTP.

En la configuración de la estafeta que vamos a utilizar en esta práctica, los usuarios de correo serán los mismos que los usuarios del sistema operativo. Es decir, para crear la dirección de correo "pepe@midominio" habrá que crear el usuario "pepe" en la máquina donde se ejecuta la estafeta[1]. En otras configuraciones más avanzadas los usuarios pueden importarse de bases de datos externas, directorios LDAP, etc.

Tarea 5: Cree varias cuentas de usuario en la estafeta. A continuación, abra sesión con ellas y envíese mensajes de correo entre esos usuarios.

Es importante que en todas las pruebas que realice a lo largo de esta práctica revise los siguientes aspectos:

- Trazas que han aparecido en `/var/log/maillog`, tanto en el sistema de origen como en el de destino.
- Cabeceras completas del mensaje que se ha depositado en la cuenta de destino, especialmente las cabeceras `Received`.
- Si quiere ver la cola de mensajes pendientes utilice el mandato `postqueue -q`.
- Para reintentar el envío de los mensajes pendientes utilice el mandato `postqueue -f`.

NOTAS:

- Por el momento, el envío de mensajes a direcciones externas a su máquina no funcionará plenamente.
- Evite usar la cuenta "root" para hacer pruebas, pues en la configuración por defecto se trata de manera especial y puede que no funcione plenamente.

[1] Esto tiene el inconveniente de que el usuario "pepe" también podrá abrir sesión (mediante SSH o similar) en la máquina, salvo que se tomen medidas extra para evitarlo.

Envío de mensajes entre estafetas

Ahora se va a abordar la transmisión de mensajes entre sistemas. Arranque una segunda máquina de la red interna para hacer pruebas de envío de mensajes a su estafeta. En esa máquina se usará la estafeta por defecto que trae FreeBSD (Sendmail).
Verifique en primer lugar que el servicio de Sendmail está habilitado y en ejecución en esa máquina. Si no fuera así, podría activarlo de la siguiente manera:

```
sysrc sendmail_enable="YES"
service sendmail start
```

Tarea 6: Pruebe a enviar mensajes desde la segunda máquina a los usuarios de la primera máquina. Como en otras ocasiones, estudie los resultados y extraiga conclusiones.

Tarea 7: Configure su cortafuegos/NAT para redirigir los puertos del servicio de correo hacia la máquina donde ha instalado la estafeta Postfix. Verifique que puede enviar mensajes a los usuarios de su estafeta desde un tercer sistema que esté en la red externa[2].

Tarea 8: Con frecuencia se usan nombres de DNS obvios para apuntar a las máquinas que proporcionan diversos servicios. Configure su dominio de DNS para que el nombre smtp.xxx.mucs.es apunte a la estafeta.

Habrá observado que, hasta ahora, hay que indicar en la dirección de destino de los mensajes el nombre de la máquina concreta donde se ejecuta la estafeta. Ahora pasaremos a simplemente indicar el dominio (@xxx.mucs.es), al igual que se haría en el mundo real.

Tarea 9: Configure todo lo necesario para que su estafeta acepte mensajes dirigidos a su dominio (@xxx.mucs.es). Esto conllevará modificar el parámetro mydestination y añadir un registro MX a su DNS. Pruebe a enviar mensajes a sus usuarios tanto desde sistemas externos, como localmente desde la propia estafeta.

Tarea 10: Configure el parámetro myorigin de Postfix para que los mensajes generados localmente utilicen su dominio de correo (@xxx.mucs.es) y compruebe los resultados (esto solo afecta a mensajes generados por procesos locales, pero no sería necesario para mensajes recibidos de agentes de usuario en otros equipos).

Para hacer pruebas más completas en el laboratorio, puede enviar mensajes a eco@ars.lab.te.upm.es y al cabo de unos segundos recibirá una respuesta automática (si su dominio y estafeta están correctamente configurados para enviar y recibir mensajes de otros sistemas).

Tarea 11: Defina algunos alias (`/etc/mail/aliases`) que apunten a cuentas de su dominio. También puede definir alguno que apunte a cuentas externas. No olvide ejecutar el mandato `newaliases` cada vez que modifique el fichero de alias.

[2] Puede ser otra máquina suya de la red externa o una máquina de otro compañero de laboratorio.

Envío de mensajes desde una estafeta satélite

Ahora se va a abordar el caso de envío de mensajes desde una estafeta satélite, que se produce cuando una estafeta (o, en general, un cliente de correo) no puede o no debe conectarse directamente a los sistemas de destino, y en su lugar entrega los mensajes a una estafeta principal para que ésta los envíe a su destino final.

Tarea 12: Pruebe a enviar correos electrónicos desde su estafeta a alguna cuenta de Internet. Verá que los mensajes se quedan encolados en su estafeta[3].

Tarea 13: Configure el parámetro `relayhost` de su estafeta para que sea satélite de `cartero.ars.lab.te.upm.es`. Compruebe qué sucede ahora, tanto con mensajes enviados a la Internet, como con mensajes enviados a otros compañeros, a la cuenta de eco, y a cuentas de su propio dominio.

NOTA: dependiendo de la dirección de Internet a la que envíe los mensajes de prueba, quizá se depositen en la carpeta de correo no deseado o no sean aceptados por la estafeta de destino (en este último caso ni siquiera recibirá una notificación de rechazo). Todo esto es porque el envío se está realizando desde dominios no visibles en la Internet, y eso suele ser bastante sospechoso de spam para la mayoría de las estafetas reales.

Ahora vamos a hacer que nuestra estafeta actúe como estafeta principal para otros sistemas. Para hacer pruebas necesitará una segunda estafeta, que actuará como satélite de su estafeta principal.

Realice una de las dos siguientes tareas, a su elección:

Tarea 14: Si opta por instalar Postfix en la estafeta satélite, configure el parámetro relayhost para encaminar todo el correo a través de la estafeta principal.

Tarea 15: Si opta por utilizar Sendmail en la estafeta satélite, haga lo siguiente para encaminar todo el correo a través de la estafeta principal:

1. Cambie al directorio `/etc/mail` y ejecute el mandato `make`. Deberían aparecer unos ficheros nuevos con el nombre de la máquina.
2. Edite el fichero `MI_MÁQUINA.mc` (ojo: no es `MI_MÁQUINA.submit.mc`), busque la línea que define la variable `SMART_HOST`, quite la cadena `dnl` que tiene al inicio y ponga el nombre de su estafeta principal.
3. Ejecute el mandato `make` y después el mandato `make install`.
4. Reinicie el servicio de Sendmail: `service sendmail restart`.

Tarea 16: Desde la estafeta satélite, escriba un mensaje dirigido a una cuenta local de la estafeta principal y compruebe que se entrega sin problemas.

Tarea 17: Ahora escriba un mensaje dirigido a una cuenta externa y compruebe qué sucede. Observará que la estafeta principal no acepta encaminar el mensaje (da un error del tipo “relay access denied”).

Tarea 18: Configure la estafeta principal para que acepte encaminar mensajes externos desde la estafeta satélite (parámetro mynetworks).

[3] El cortafuegos del departamento no permite enviar correos directamente al exterior

Después de hacer las cuestiones de este apartado, puede quitar la opción `relayhost` de su estafeta principal. Observe que, si la mantiene y su estafeta principal es satélite de cartero.ars.lab.te.upm.es, los mensajes pasan por varios sistemas del laboratorio antes de llegar a su destino.

Acceso remoto a los buzones

En todas las actividades anteriores se han leído los mensajes recibidos en los buzones con programas que se ejecutaban localmente en la propia estafeta, pero lo habitual es que los agentes de usuario (MUA) sean remotos.

El formato de buzón mbox que utiliza Postfix en su configuración por defecto es insuficiente para usarlo en una estafeta de correo más avanzada, por lo que en primer lugar se cambiará dicho formato a Maildir.

Tarea 19: Configure el parámetro home_mailbox para usar el formato Maildir[4] en la estafeta principal. Después debe recargar Postfix.

Tarea 20: Con frecuencia se usan nombres de DNS obvios para apuntar a las máquinas que proporcionan diversos servicios. Configure su dominio para que el servidor de buzones esté apuntado por pop/imap.xxx.mucs.es.

Para acceder remotamente a los buzones mediante POP o IMAP se necesita instalar un paquete de software adicional. En esta práctica se usará Dovecot.

Tarea 21: Instale el paquete `dovecot` en la estafeta principal. Después copie los ficheros de `example-config` según se indica y habilite el paquete en `/etc/rc.conf`.

Tarea 22: En la configuración por defecto, Dovecot requiere instalar un certificado X.509 para el acceso cifrado mediante STARTTLS o mediante SSL. Genere una pareja de claves y un certificado autofirmado e instálelos en la ubicación esperada por Dovecot (consulte `/usr/local/etc/dovecot/conf.d/10-ssl.conf`).

Tarea 23: Arranque el servicio `dovecot` y compruebe que está operativo, por ejemplo así:

- Revise los mensajes de `/var/log/maillog`.
- Utilice `doveadm auth login` para autenticarse con una cuenta de prueba.
- Envíe un mensaje a una cuenta y compruebe que se deposita en su buzón.

Configuración de un agente de usuario avanzado

Ahora que ya tiene una estafeta accesible remotamente, tanto para enviar mensajes como para leer los mensajes recibidos, puede crear una cuenta de correo en un agente de usuario (MUA) avanzado. Como agente de usuario puede utilizar los programas Thunderbird, Outlook o similares de los ordenadores del laboratorio.

Desde el punto de vista de la estafeta de su dominio, el agente de usuario va a actuar como si fuera una estafeta satélite. Como ya se ha visto en el apartado anterior, por defecto las estafetas de correo no admiten cursar mensajes a destinos cualesquiera.

Tarea 24: Utilice el parámetro mynetworks para permitir el envío de mensajes a cualquier destino desde la máquina en la que ejecuta el agente de usuario. Esta opción no es la recomendada para aceptar mensajes de agentes de usuario, ya que lo más

[4] El programa `mail` no utiliza este formato, por lo que ya no podrá utilizarlo para leer mensajes.

adecuado es controlar el acceso por medio de autenticación; además, en el mundo real probablemente no se podrá determinar de antemano la dirección de red desde la que accederán los agentes de usuario. En un apartado posterior se aborda la autenticación de los clientes.

Tarea 25: Configure alguna de las cuentas de su estafeta en el agente de usuario y compruebe que puede enviar y recibir mensajes.

Autenticación SASL en la MTA (opcional)

Hasta ahora, todos los envíos de correo se han realizado sin autenticar al cliente. Entre estafetas, ese es el modo de funcionamiento más habitual. En cambio, cuando el cliente es un agente de usuario lo normal es que la estafeta requiera que el cliente se autentique, pues en otro caso no le dejará enviar mensajes a destinos externos.

Hemos visto que usando el parámetro mynetworks se puede permitir que determinados clientes envíen correos a cualquier destino, pero en general esa opción no es válida porque muchas veces la dirección IP de origen es insuficiente para establecer un control de acceso eficaz. En el mundo real, muchos de los clientes que se conectan a una estafeta acceden desde direcciones IP desconocidas a priori (sobre todo si son móviles, portátiles, acceden desde su casa o de viaje, etc.).

Un sistema mucho más adecuado es utilizar autenticación SASL para discernir entre clientes autenticados y clientes anónimos; a los primeros se les permitirá entregar correo para cualquier destino, pero a los segundos solo se les permitirá entregar correo destinado a la propia estafeta.

Postfix implementa la autenticación SASL apoyándose en un software externo. Una de las posibilidades es apoyarse en Dovecot, tal como se va a hacer en las siguientes actividades.

Para realizar estas actividades, lea Postfix SASL Howto, en particular Configuring SASL authentication in the Postfix SMTP server, y especialmente Configuring Dovecot SASL y Enabling SASL authentication and authorization in the Postfix SMTP server.

Tarea 26: Primero asegúrese de que la dirección IP del agente de usuario que ha usado en el apartado anterior NO está incluida dentro de mynetworks. Compruebe que si intenta enviar correos externos la estafeta NO los acepta.

Tarea 27: Configure a su estafeta para admitir autenticación SASL apoyándose en Dovecot. Configure el agente de usuario para que utilice autenticación con la estafeta. Compruebe que ahora sí puede enviar todo tipo de correos con el agente de usuario.

Cifrado TLS en la MTA (opcional)

Por defecto, Postfix no encripta las conexiones SMTP, ni entrantes ni salientes. En general, todas las estafetas trabajan inicialmente con conexiones no encriptadas y solo pasan a modo cifrado si alguna de las dos partes lo solicita. En algunos casos, las estafetas se pueden configurar para trabajar obligatoriamente con sesiones cifradas.

Para realizar las tareas de este apartado, consulte Postfix TLS Support.

Cuando se atiende a clientes que pueden autenticarse (como en el apartado anterior), es muy recomendable que la estafeta admita conexiones cifradas, pues por ellas circularán credenciales de autenticación al inicio de la sesión. De hecho, es probable que esos clientes estén configurados para requerir obligatoriamente cifrado de la sesión.

Tarea 28: Configure a su estafeta para que permita acceso cifrado a los clientes. Consulte SMTP Server specific settings.

También puede ser recomendable cifrar las sesiones salientes que realice Postfix. Esto dota de mayor seguridad al tránsito de mensajes externos, puesto que es más difícil que un nodo intermedio pueda examinar o incluso alterar el contenido de los mensajes salientes. En la práctica no todas las estafetas de Internet admiten sesiones cifradas, por lo que normalmente se utiliza una configuración de tipo "oportunista" (se cifrará la conexión si la estafeta de destino lo admite). Además, los certificados X.509 que presentan las estafetas externas no siempre son realmente adecuados y no es extraño encontrar certificados autofirmados, expirados o sin las capacidades suficientes, por lo que puede que sea necesario admitir certificados inválidos o que no se pueden comprobar, so pena de no poder transmitir mensajes destinados a estafetas configuradas incorrectamente.

Tarea 29: Configure a su estafeta para utilizar cifrado oportunista al enviar mensajes a otras estafetas. Consulte SMTP Client specific settings.

Integración de Postfix y Dovecot con LDAP (opcional)

En los apartados anteriores se ha usado la base de datos de usuarios locales de la estafeta para Postfix y Dovecot. Si los usuarios de la organización están definidos en un directorio LDAP será necesario que Postfix y Dovecot se integren con ese directorio.

Tarea 30: Configure Postfix para que reconozca a los usuarios de su directorio LDAP. Consulte Postfix LDAP Howto. No necesita recompilar Postfix, por lo que puede saltar el primer apartado (Building Postfix with LDAP support). En su lugar, tiene que desinstalar el paquete `postfix` e instalar el paquete `postfix-ldap-sasl`.

Tarea 31: Configure Dovecot para que reconozca a los usuarios de su directorio LDAP. Consulte el manual de Dovecot para LDAP.