

Práctica 2: Servicio de Correo Electrónico

Objetivo

El objetivo de esta práctica es poner en marcha un servicio de correo electrónico para los usuarios de una red. Se realizarán pruebas para verificar el correcto funcionamiento del servicio.

1. Introducción

El correo electrónico es un servicio de red muy utilizado por la mayoría de usuarios. Es una herramienta esencial en las comunicaciones profesionales y personales. Aunque menos frecuente, también lo utiliza el sistema operativo para comunicarse con los usuarios.

2. Agentes de transporte

Históricamente, **Sendmail** ha sido el agente de transporte de referencia por su versatilidad, aunque su complejidad de configuración es alta. Actualmente, **Postfix** y **Exim** son las alternativas más extendidas en entornos de producción debido a su arquitectura modular y mayor sencillez de administración.

3. Situación general: contexto de trabajo

Servicio de correo en unizar.es

Antes de abordar tanto la configuración como la verificación de funcionamiento de nuestro servidor hay que comprender cómo se controla la recepción y el envío de correo electrónico a nuestro dominio (**unizar.es**).

Los registros MX en la configuración DNS anuncian al exterior de nuestra red que los mensajes de correo dirigidos a usuarios del dominio **unizar.es** deben ser entregados al servidor **mx01.puc.rediris.es** o al **mx02.puc.rediris.es**. Esto no acaba con los intentos del exterior de conectarse al puerto 25 de otras máquinas, por esta razón el router de entrada a la Universidad de Zaragoza bloquea todo el tráfico entrante SMTP (puerto 25) excepto el dirigido al servidor de correo **relay.unizar.es**. De esta manera las reglas de detección de spam están centralizadas y se bloquea este tráfico de las máquinas externas a nivel de red -router- para evitar el spam.

En cuanto al envío de correo al exterior de la Universidad, solamente se permite iniciar el establecimiento de conexiones SMTP a las máquinas **smtp.unizar.es** y **smtpserver.unizar.es**. Por tanto, estas máquinas actúan como *smart hosts*, es decir, son las únicas máquinas que pueden enviar tráfico SMTP al exterior. De esta forma se impide el envío de spam desde máquinas internas infectadas por algún virus. La comunicación con **smtp.unizar.es** es a través de conexión SMTP autenticada y cifrada, mientras que con **smtpserver.unizar.es** es a través de conexión SMTP no autenticada y en claro.

A la vista de todo lo anterior, el puerto 25 de nuestro sistema no podrá recibir peticiones de conexión ni realizar envío de tráfico SMTP, por tanto nuestro servidor de correo no podrá recibir mensajes de servidores de correo externos a la Universidad de Zaragoza ni enviarlos. Sin embargo, el Servicio de Informática y Comunicaciones de la Universidad de Zaragoza (SICUZ) ha habilitado el puerto 25 para la subred del laboratorio L1.02 (155.210.154.0) para que desde sus máquinas pueda tanto recibirse mensajes desde el exterior de la red como enviarlos.

A no ser que haya cambiado recientemente la configuración de los filtros, no hay limitación a la hora de que los servidores de correo internos de la Universidad de Zaragoza puedan mandarse mensajes entre sí (aunque no lo hagan directamente sino a través de la máquina **relay.unizar.es**), con lo cual se podrían utilizar cuentas de usuario en **hendrix**, ... para enviar los mensajes de prueba a vuestros servidores de correo.

4. Enunciado

Instala las aplicaciones necesarias para proporcionar servicio de correo electrónico. El servicio deberá realizar funciones de agente de transporte (recepción/envío/encaminamiento de mensajes), agente de reparto (entrega en buzones locales) y agente de acceso (conexión de agentes de usuario remotos). Configúralo de forma que cumpla los siguientes requisitos:

- Prestar servicio de correo saliente a clientes ubicados en la red 155.210.154.0.
- Prestar servicio de correo entrante a los usuarios locales (lectura directa de correo) y a usuarios remotos (a través de cuentas pop o imap).
- Redirigir mensajes dirigidos a cuentas en servidores de la Universidad de Zaragoza.
- Filtrado básico de mensajes:
 - Remitentes y destinatarios vetados: rechazar o descartar mensajes provenientes de o dirigidos a determinadas direcciones de correo.

- Filtrado estático de contenido: rechazar o descartar mensajes que contengan determinadas cadenas de texto en el asunto o el cuerpo del mensaje.

En el apartado siguiente se lista una serie de pruebas que permiten verificar el cumplimiento de estos requisitos.

Ten presente que el sistema tiene instalado **exim**, y que instalar un segundo agente de transporte (*Mail Transfer Agent*, MTA) puede crear conflictos (por ejemplo, acceso al puerto 25). El documento “Preguntas frecuentes de las prácticas” (web de la asignatura) puede ayudarte en este punto y en otros que puedan surgir.

Se valorará la instalación desde las fuentes frente a la instalación desde paquetes mediante herramientas como **apt** o **aptitude**.

De manera **opcional** pueden instalarse otras aplicaciones que añadan funcionalidad al servicio de correo:

- Antivirus
- Acceso al buzón de correo a través de web (webmail)
- Gestor de listas de distribución
- Contestadores automáticos de mensajes
- Herramientas adicionales de administración del servidor de correo

Importante: antes de comenzar la práctica, lee atentamente el enunciado completo.

5. Pruebas

Una vez concluido el proceso de instalación y configuración del servidor de correo, debéis comprobar su funcionamiento. Se proporciona un script para automatizar las pruebas de verificación (**smtp.sh**). Seguidamente se detalla la batería de pruebas a realizar.

Pruebas MTA (servidor SMTP)

- Establecimiento de conexión: el servidor MTA deberá responder con el siguiente mensaje cuando establezca una conexión a petición de un cliente SMTP:

```
220 SMTP nombre_del_servidor: servidor de correo administrado por nombre_estudiante
```
- Servicio envío SMTP
 - Mensaje enviado por usuario local a una cuenta en un servidor externo, por ejemplo, **nip@unizar.es**. Este mensaje deberá enviarse al MTA correspondiente.
- Servicio recepción SMTP: todos los siguientes mensajes deberán aceptarse y enviarse a su destinatario:
 - Mensaje recibido desde una máquina en el exterior de la red (por ejemplo, hendrix) y que es dirigido a un usuario local (con cuenta en la máquina)
 - Mensaje recibido desde una máquina en el exterior de la red (por ejemplo, hendrix) y que es dirigido a una cuenta de un servidor de correo de la Universidad de Zaragoza (cuentas unizar.es, cuentas en hendrix, ...). Este mensaje deberá redireccionarse al servidor correspondiente.
- Prueba relay (servicio recepción SMTP): debe **rechazarse** la gestión del siguiente mensaje
 - Mensaje recibido desde el exterior de la red 155.210.154.0 (por ejemplo, hendrix) y que es dirigido a un usuario externo a la Universidad.
- Pruebas alias
 - Mensaje dirigido a un alias de usuario
 - Mensaje dirigido a un alias de lista
- Pruebas filtrado acceso (envío/recepción SMTP): todos estos mensajes deben rechazarse:
 - Mensaje proveniente de un dominio vetado
 - Mensaje enviado por un usuario vetado
 - Mensaje dirigido a un usuario vetado
 - Mensaje con la palabra Viagra en el campo del asunto (*subject*)
 - Mensaje con la palabra Viagra en el cuerpo

Pruebas servidor POP/IMAP (agente de acceso, *Mail Access Agent*, MAA)

- Consulta del buzón de un usuario que sí tiene acceso a shell en la máquina
- Consulta del buzón de un usuario que no tiene acceso a shell en la máquina

Otras pruebas

Si se han añadido funcionalidades adicionales (por ejemplo, WebMail, antivirus, antispam más completo), deben verificarse con las pruebas oportunas.

6. Memoria de la práctica

La memoria de la práctica, breve pero completa, deberá especificar:

- Agentes de transporte, acceso, reparto y aplicaciones adicionales instaladas
- Proceso de instalación: a partir de las fuentes, preinstalado, con dselect, apt ...
- Configuración: resaltar las modificaciones realizadas y explicarlas brevemente mediante comentarios en el propio fichero de configuración. Detallar especialmente los cambios realizados para superar las pruebas spam y la redirección de mensajes a servidores de correo de la Universidad de Zaragoza.
- Pruebas: no hace falta reseñar el detalle de las pruebas realizadas.

7. Material auxiliar, referencias ...

- Transparencias de la asignatura
- Características del servicio de correo en la Universidad de Zaragoza: es imprescindible entender la arquitectura de este sistema para poder configurar correctamente vuestro servidor de correo.

Referencias relativas a Exim

- Exim: <http://exim.org>
- En el sistema Debian del arranque remoto hay abundante información en el directorio
`/usr/share/doc/`

Referencias relativas a Postfix:

- PostFix: <http://www.postfix.org>
- Filtering E-Mail with Postfix and ProcMail: <http://online.securityfocus.com/infocus/1598>
- EnGarde Secure Linux Postfix HOWTO: <http://linuxsecurity.com/docs/HOWTO/Postfix-EnGarde-HOWTO.html>

Referencias relativas a Sendmail:

- Sendmail: <http://www.sendmail.org>
- Sendmail Configuration Files: <http://www.sendmail.org/m4/readme.html>

También puedes buscar documentación alternativa, hay multitud de tutoriales en la red.