

**Instituto Politécnico Nacional**

**Escuela Superior de Cómputo**

**Soto Ramos Manuel Alejandro**

Administración de Servicios en Red

**Manual de Instalación y Configuración - Servidor de Correo Electrónico / Antivirus / Listas de Correo.**

Grupo: 4CV4

**Jiménez Maruri Pedro**

**Romero Serrano Luis**

**Valencia Rodriguez Fernando**

# 

# Índice

[**Índice**](#_wfc3vv7ln5qf) **1**

[**Introducción**](#_7y8q9t7jxifk) **3**

[Servidores de salida y entrada.](#_kfi200zewzng) 3

[Funcionamiento.](#_diy5sajfe0ox) 4

[SMTP (Simple Mail Transfer Protocol)](#_bd3qgwkmzjc0) 4

[Pop3 (Post Office Protocol)](#_ud7nehs8g82r) 4

[IMAP (Internet Message Access Protocol)](#_hyrdxfcbkc5w) 4

[Ventajas.](#_bttvsf6wrz75) 5

[SMTP (Simple Mail Transfer Protocol)](#_9li8selato5h) 5

[Pop3 (Post Office Protocol)](#_21c8k7pxprma) 5

[IMAP (Internet Message Access Protocol)](#_ytaorftr05ra) 5

[**Herramientas**](#_8cludv93lsva) **5**

[**Requisitos previos**](#_ge7qpkeoqdh7) **7**

[Lea la documentación](#_rhe742ffenno) 7

[Registro y resolución de problemas](#_ajh2do4f9buh) 8

[Dónde obtener pistas para la resolución de problemas](#_evka9oac66rs) 8

[Linux, Apache, MySQL y PHP (LAMP) Stack](#_58txrfjeo8a3) 9

[Instalar paquetes de LAMP Stack](#_cpqjhn3yt24z) 9

[Preparar Apache](#_aotz7kv6rzrs) 9

[Paso 1: Configurar Global ServerName para que suprima los avisos de sintaxis](#_2dai05wpy9wh) 9

[Paso 2: Ajustar el cortafuegos](#_4j1017surubn) 10

[Cómo encontrar la dirección IP pública de su servidor](#_atjh7zbp7cqn) 11

[Paso 3: Compruebe su servidor web](#_9h86y5jj0bkn) 12

[Gestionar el proceso de Apache](#_nw7w4ib8tyxj) 14

[Familiaricese con los archivos y directorios importantes de Apache](#_9ktev8c9hzka) 14

[Contenido](#_5pads09v5c4d) 14

[Configuración del servidor](#_ti2pw4tme0hu) 14

[Registros del servidor](#_gb7421rcncy9) 15

[Preparar MySQL](#_o0tu0uj8b4qw) 15

[Preparar PHP](#_nz7bu7xbx51p) 17

[Instalar módulos PHP](#_700sqej9v6pa) 18

[Pruebe el procesamiento de PHP en su servidor web](#_yqr6ong6e5xy) 20

[**Instalación**](#_yx0f0w194smu) **22**

[Instalar paquetes](#_lnp0jscdsyzz) 22

[**Crear base de datos MySQL, Dominios Virtuales, Usuarios y Aliases**](#_ywcicix9ho8u) **23**

[Crear Usuario de MySQL para Postfix](#_idqi0ci5erb7) 23

[Crear tablas para los VirtualHosts](#_ubxxba5j7wxq) 24

[Dominios virtuales](#_86dgs5ttuzxk) 24

[Emails Virtuales](#_l2fggbgunie4) 25

[Alias virtuales](#_b8k4kkwmiond) 25

[**Configurar Postfix**](#_493qenrnqp2b) **25**

[Crear archivos para conectar con la base de datos](#_2r0nng6m8r31) 27

[Activar SSL](#_vm5f809gbsks) 28

[Configurar Relay](#_g7f9o8o2zjyw) 29

[Pruebas](#_way32flerzyf) 30

[Compruebe si los mensajes se envían a través del servidor SMTP de Gmail.](#_2o7x03jby0jx) 30

[Permitir Aplicaciones menos seguras en Gmail](#_o5jslfddax3) 30

[Solución de problemas](#_sikvxi521dzu) 31

[**Configurar Dovecot**](#_4b7lczuas38l) **31**

[¿A quién le pertenecen los correos?](#_dpus03gweg75) 32

[Verificar los permisos](#_jduuw8t4vtwk) 33

[Instalando certificados](#_4e89sxj0yq64) 37

[Pruebas](#_hoq0y0gcieeo) 39

[Postfix (SMTP)](#_869494io1f65) 39

[Dovecot (IMAP)](#_dap0qvd3q53e) 39

[Dovecot (IMAPS)](#_v31cxg5yje9r) 40

[**Configurar SpamAssassin**](#_vocxq77b382q) **41**

[Mover el spam a la carpeta Junk automáticamente](#_na1mfys41rpq) 43

[Borrar automáticamente spam después de 30 días](#_axp55ylsmv70) 45

[**Configurar ClamAV**](#_35y3ynba3y0s) **46**

[**Instalar RoundCube**](#_of1zwvl1gcp3) **48**

[Paso 1: Instalación de dependencias](#_ad84f0xfm201) 48

[Paso 2 - Descargar Roundcube](#_7awa93wqum4k) 50

[Paso 3 — Configurando Apache](#_xl74pjy3s1yf) 51

[Paso 4 — Configurando MySQL](#_eh8n7yvzbfv7) 53

[Paso 5 — Configurando Roundcube](#_ar5voj7moi8) 54

[Configuración general](#_oj1ddsjym6iv) 55

[Registro y depuración](#_orsbjkw515z7) 55

[Configuración de la base de datos](#_73t0jen5my1c) 55

[Configuración IMAP](#_7lrr6etzgic7) 56

[Configuración SMTP](#_l28mgwn85gin) 56

[Configuración de pantalla y preferencias de usuario](#_hhdru6ecbtkt) 57

[Plugins](#_v1s94ls18pnd) 57

[Paso 6 - Prueba de la configuración de Roundcube](#_uldpps7gr4p) 58

[Conclusión](#_r3ofxrf3tsz7) 58

[**Cuotas**](#_r2ef8modtnhs) **59**

[**Servidor de monitoreo - Monit**](#_ff1h98a7sijj) **60**

[Introducción](#_cppra5x730ii) 60

[Instalación.](#_7wqv5fa3ygpu) 60

[Configuración](#_iejfk9fddb1v) 61

[**Referencias**](#_xvjoktqo0xww) **62**

# **Introducción**

El correo electrónico es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante redes de comunicación electrónica sin importar la distancia que los separe. Por medio del correo electrónico se puede enviar texto, así como casi todo tipo de archivos digitales, aunque bien suelen existir limitaciones al tamaño de los archivos adjuntos.

Los sistemas de correo electrónico se basan en un modelo de almacenamiento y reenvío, de tal modo que no es necesario que ambos extremos se encuentren conectados simultáneamente. Para ello se emplea un servidor de correo que hace las funciones de intermediario, guardando temporalmente los mensajes antes de enviarse a sus destinatarios. En Internet, existen multitud de estos servidores, que incluyen a empresas, proveedores de servicios de internet y proveedores de correo tanto libres como de pago.

Un servidor de correo electrónico ofrece la posibilidad de trabajar con varios usuarios simultáneamente, conectados desde distintos dispositivos y compartiendo documentos. Permitiendo que la comunicación sea activa y eficiente de forma que se trabaja más fácilmente y con mayor interacción.

Otro punto clave para la elección de un servidor de correo es el soporte técnico. Es necesario contar con apoyo y asesoramiento del funcionamiento del servidor para que ante cualquier imprevisto o problema se solucione en el menor tiempo posible y el funcionamiento del email no se vea interrumpido.

## **Servidores de salida y entrada.**

* **SMTP (Simple Mail Transfer Protocol)**: El SMTP tomará tu correo electrónico y primero lo enviará a los servidores de correo de tu proveedor del servicio y de ahí a otra cuenta de correo electrónico que puede ser ajena a tu proveedor. Dado a que presenta algunas limitaciones en el procesamiento de la cola de mensajes recibidos en el servidor destino, se emplea para gestionar el correo saliente.

Su tarea específica es enviar el correo (correo saliente).

* **Pop3 (Post Office Protocol)**: Realiza el proceso de acceso al correo y lo descarga los mensajes de correo en la computadora (u otro dispositivo), donde quedan almacenados y organizados en las carpetas que se hayan creado. Esto implica que si en algún momento quieres acceder con más de un dispositivo al servidor, ya no encontrarás mensajes que hayas eliminado con anterioridad.

Su tarea específica es recibir el correo (correo entrante).

* **IMAP (Internet Message Access Protocol**): Está hecho para que la sincronización entre tu correo y el servidor sea constante, y una vez que un mensaje haya sido leído, modificado o eliminado de tu correo, este siga presente en el servidor. Con esto, se puede revisar y usar el correo desde distintos tipos de dispositivos como computadoras personales, Smartphone y Tablet, sin tener el temor de que estarás perdiendo tu información. Aunque se recomienda borrar periódicamente el contenido de la cuenta para no exceder el límite de espacio.

## **Funcionamiento.**

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

* El Servidor SMTP del emisor se comunica con un Servidor DNS (Sistema de Nombre de Dominio) y le pregunta si le puede brindar la dirección IP del SMTP del receptor.
* DNS responde con una o más direcciones IP.
* El Cliente de Correo se conecta con el Servidor SMTP y le comunica la dirección del remitente, la del destinatario y el cuerpo del mensaje.
* El SMTP toma la dirección del receptor (ejemplo, jesica.r@embluemail.com) y lo divide en dos partes: el nombre (jesica.r) y el sistema de nombres de dominio.
* El SMTP del receptor chequea en su base de datos si existe una cuenta con el nombre Jesica.r
* Si existe, acepta el email y lo deposita en el buzón de Jesica.r
* Luego, Jesica puede leer o descargar ese mensaje en su PC mediante POP o IMAP.

### **Pop3 *(Post Office Protocol)***

* En uno de sus métodos para leer emails, lee una colección de archivos de texto, una por cada cuenta de email. Cuando llega un mensaje, su función es la de adjuntarlo al final de los archivos del destinatario .
* Al chequear el email, el cliente de correo electrónico se conecta con el POP3, que requiere un nombre de cuenta y una contraseña. Una vez que te has logueado, el servidor abre los archivos de texto y permite su acceso.
* POP3 actúa como una interfaz entre el servidor de correo electrónico, los archivos de texto que contienen tus mensajes y tu PC.
* El correo vía POP3, una vez descargado y en la mayoría de los casos, es removido por defecto del servidor quedando alojado en la máquina del usuario.

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

* Posibilita que los mails queden alojados en el servidor realizando una sincronización del contenido en la PC del usuario.
* IMAP permite tener la casilla de correo sincronizada aún utilizando una diversidad de dispositivos. El mail no se descarga de manera literal en el dispositivo, sino que él mismo actúa directamente con el servidor para leerlos, modificarlos, o bien eliminarlo.

## **Ventajas.**

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

* Permite conectarse en cualquier sistema: No tiene restricciones, por lo tanto no importa que sistema operativo se use. Solo añadiendo los datos SMTP a tu cuenta Doppler Relay.
* Mejor entregabilidad: El envío está garantizado.
* Mayor velocidad de envío: Dedicado al 100% al envío de mensajes.
* Mejor gestión de recursos: Gestión de (bajas, rebotes, direcciones incorrectas y correos spam).
* Envíos automáticos: Se puede configurar para los envíos automáticos de mensajes.

### **Pop3 *(Post Office Protocol)***

* Poder utilizar un cliente de correo para descargarlos en un dispositivo u ordenador, y poder leerlos posteriormente, aún sin tener conexión a internet.
* No es necesario tener un gran espacio de almacenamiento en el servidor de correo, ya que al descargar los correos se borran del mismo.

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

* Comunicación bidireccional entre el servidor de correo y el cliente de correo electrónico, lo que permite que varios dispositivos trabajen con una misma cuenta viendo los cambios realizados por todos.
* Los correos están en todo momento en el servidor, por lo que se puede acceder a ellos desde cualquier lugar, teniendo un dispositivo con acceso a internet.
* En caso de una avería en el ordenador en el que esté configurado el buzón, o si por cualquier razón se elimina la cuenta, siempre es posible recuperar los correos.
* Al no descargarse los correos directamente en el dispositivo que accede al servidor de correo, no consume espacio local.
* Es posible gestionar carpetas locales y archivos desde el servidor.
* Permite la búsqueda de mensajes por medio de palabras clave.

## **Herramientas**

Hay una serie de funciones y utilidades que muchos usuarios de correos electrónicos podrían desconocer y que pueden facilitarles la gestión de sus correos.

* **Crear carpetas**: Para tener una mejor organización de los mensajes según las necesidades o asuntos correspondientes.
* **Reglas de mensajes**: Ayudan a redirigir los mensajes a lugares específicos, sin necesidad de hacerlo manualmente.
* **Localizar correos**: Buscador de correos electrónicos según su destinatario, asunto o palabras en los textos.
* **Mensaje con copia oculta**: Al enviar múltiples correos evita que los que lo reciban los mensajes perciban la lista de nombres y direcciones.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Software** | **Versión** | **Licencia** | **Lenguaje de programación** | **Sistema Operativos** | **Utilidad** |
| Postfix | 3.4.0 | Pública IBM | C | GNU/Linux / UNIX | Servidor de correo. |
| Dovecot | 2.3.4 | MIT & LGPL | C | GNU/Linux / UNIX | Servidor IMAP & POP3. |
| SpamAssasin | 3.4.2 | Apache 2.0 | Perl | Multiplataforma | Filtro de spam. |
| ClamAV | 0.100.1 | GPL | C & C++ | Multiplataforma | Antivirus. |
| Monit | 5.25 | AGPL | C | GNU/Linux / UNIX | Servidor de Monitoreo. |
| MySQL | 8.0.15 | GPL | C & C++ | Multiplataforma | Base de Datos |

# 

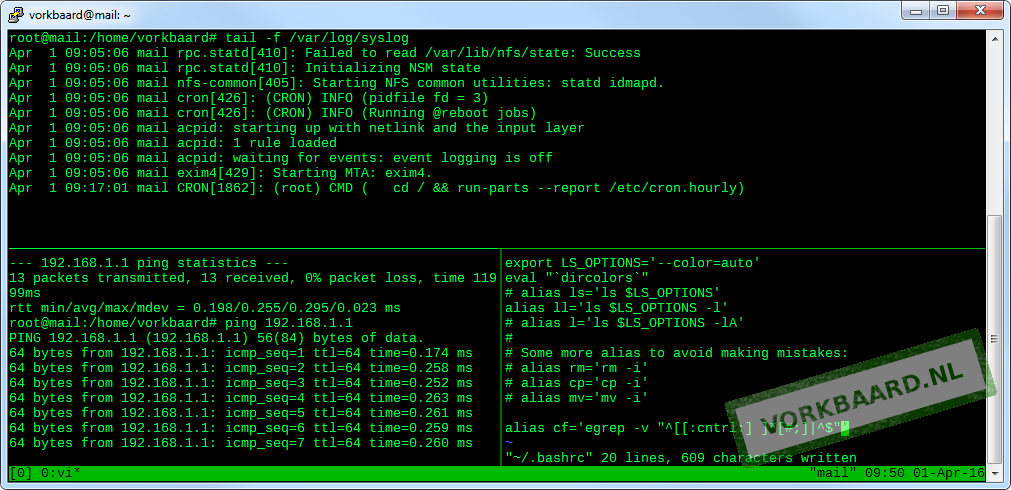
# **Requisitos previos**

## **Lea la documentación**

Si quiere entender los componentes, debería leer las sugerencias de lectura. Las páginas de manual son un buen lugar para empezar y la mayoría del software que usaremos tiene una excelente documentación en línea. No necesita aprenderlo todo de memoria. La lectura de la documentación antes de la instalación le dará una idea de lo que el software es capaz de hacer.

## **Registro y resolución de problemas**

Tmux permite ejecutar múltiples sesiones de terminal en una conexión SSH. El tercio inferior en la pantalla ejecuta el archivo de registro de correo y mantengo vigilada la configuración de Postfix con watch -d postconf -n en otro panel de tmux. Esta configuración permite una solución de problemas muy sencilla. Si no ha trabajado con tmux antes, es un buen momento para empezar. Su curva de aprendizaje valdrá mucho la pena.



Para instalarlo haga lo siguiente

sudo apt-get install tmux

Mas información de Tmux en: **https://en.wikipedia.org/wiki/Tmux** y

man tmux

### **Dónde obtener pistas para la resolución de problemas**

Los archivos de registro son el punto de partida para la resolución de problemas. Si las cosas no funcionan, revise sus registros. Por convención, los ficheros de registro van a **/var/log/** en los sistemas basado en Debian. Muchos programas le permiten establecer una ruta de archivo de registro personalizada, de modo que si no puede encontrar su archivo de registro, vea si puede encontrar su ubicación en los archivos de configuración del programa. Si no se ha creado un archivo de registro, compruebe si la cuenta que debe crearse o añadirse tiene permisos para hacerlo.

Es buena idea mantener los archivos de registro en funcionamiento mientras hace pruebas para poder ver qué está pasando. Para ello, haga

tail -f /var/log/mail.log

por ejemplo. Puede detenerlo con Ctrl + C.

Además, Postfix puede mostrarle estas cosas (desde la página de manual de postconf):

postconf -p Muestra los ajustes de los parámetros principales. Este es el valor por defecto. [Usar en conjunto con grep.]

postconf -n Muestra sólo los parámetros de configuración que tienen ajustes explícitos de name=value en **main.cf.** Especificar -nf para plegar las líneas largas para que sean legibles para el ser humano.

Dovecot tiene una característica similar (de la página de manual de doveconf):

* doveconf -a Muestra todos los ajustes con sus valores actualmente configurados.
* doveconf -d Muestra el valor por defecto del ajuste en lugar del configurado actualmente.
* doveconf -n Muestra sólo los ajustes con valores no predeterminados.

Tanto postconf como doveconf tienen más opciones; lea sus respectivas páginas de manual.

## **Linux, Apache, MySQL y PHP (LAMP) Stack**

Esta sección cubrirá la instalación de Apache, MySQL, PHP y SSL en tu servidor desde cero. Si ya tiene una pila LAMP en funcionamiento, vaya a la sección de Instalación de Paquetes.

### **Instalar paquetes de LAMP Stack**

Instale el metapaquete lamp-server^, que instala Apache, MySQL y PHP como dependencias:

sudo apt-get install lamp-server^

Durante el proceso de instalación, se le pedirá que elija una contraseña para el usuario MySQL root.

A continuación veremos una pequeñas preconfiguraciones de la pila LAMP.

## **Preparar Apache**

### **Paso 1: Configurar Global ServerName para que suprima los avisos de sintaxis**

A continuación, añadiremos una sola línea al archivo **/etc/apache2/apache2.conf** para suprimir un mensaje de advertencia. Si bien es inofensivo, si no establece **ServerName** globalmente, recibirá la siguiente advertencia cuando compruebe si hay errores de sintaxis en la configuración de Apache:

sudo apache2ctl configtest

**Output**  
 AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message  
 Syntax OK

Abra el archivo de configuración principal con su editor de texto:

sudo nano /etc/apache2/apache2.conf

Dentro, en la parte inferior del archivo, agregue una directiva **ServerName**, apuntando a su nombre de dominio primario. Si no tiene un nombre de dominio asociado con su servidor, puede utilizar la dirección IP pública de su servidor:

Si no conoce la dirección IP de su servidor, vaya a la siguiente sección sobre cómo encontrar la dirección IP pública de su servidor para encontrarla.

**/etc/apache2/apache2.conf**

. . .  
ServerName server\_domain\_or\_IP

Guarde y cierre el archivo cuando haya terminado.

A continuación, compruebe si hay errores de sintaxis escribiendo:

sudo apache2ctl configtest

Como hemos añadido la directiva global ServerName, todo lo que debería ver es:

**Output**

Syntax OK

Reinicie Apache para implementar sus cambios:

sudo systemctl restart apache2

Ahora puede empezar a ajustar el cortafuegos.

### **Paso 2: Ajustar el cortafuegos**

Antes de que podamos probar Apache, necesitamos modificar nuestro firewall para permitir el acceso externo a los puertos web por defecto.

Durante la instalación, Apache se registra en la UFW para proporcionar algunos perfiles de aplicaciones. Podemos usar estos perfiles para simplificar el proceso de habilitar o deshabilitar el acceso a Apache a través de nuestro cortafuegos.

Podemos listar los perfiles de la aplicación ufw escribiendo:

sudo ufw app list

Debería obtener una lista de los perfiles de la aplicación:

**Output**  
Available applications:  
 Apache  
 Apache Full  
 Apache Secure  
 OpenSSH

Como puede ver, hay tres perfiles disponibles para Apache:

* **Apache:** Este perfil sólo abre el puerto 80 (tráfico web normal, no encriptado)
* **Apache Full:** Este perfil abre tanto el puerto 80 (tráfico web normal no cifrado) como el puerto 443 (tráfico cifrado TLS/SSL).
* **Apache Secure:** Este perfil sólo abre el puerto 443 (tráfico cifrado TLS/SSL)

Para nuestros propósitos, permitiremos el tráfico entrante para el perfil completo de Apache escribiendo:

sudo ufw allow in "Apache Full"  
 sudo ufw enable

Puede verificar el cambio escribiendo:

sudo ufw status

Debería ver el tráfico HTTP permitido en la salida mostrada:

**Output**  
Status: active  
  
To Action From  
-- ------ ----  
OpenSSH ALLOW Anywhere   
Apache Full ALLOW Anywhere   
OpenSSH (v6) ALLOW Anywhere (v6)   
Apache Full (v6) ALLOW Anywhere (v6)

Como puede ver, el perfil ha sido activado para permitir el acceso al servidor web.

#### **Cómo encontrar la dirección IP pública de su servidor**

Si no sabe cuál es la dirección IP pública de su servidor, hay varias maneras de encontrarla. Normalmente, esta es la dirección que utiliza para conectarse a su servidor a través de SSH.

Desde la línea de comandos, puede encontrar esto de varias maneras. Primero, puede usar las herramientas de iproute2 para obtener su dirección escribiendo esto:

ip addr show eth0 | grep inet | awk '{ print $2; }' | sed 's/\/.\*$//'

Esto te dará dos o tres líneas de vuelta. Todas son direcciones correctas, pero es posible que su ordenador sólo pueda utilizar una de ellas, así que no dude en probar cada una de ellas.

Un método alternativo es usar la utilidad **curl** para contactar con un tercero y decirle cómo ve su servidor. Puede hacerlo preguntando a un servidor específico cuál es su dirección IP:

sudo apt-get install curl  
 curl http://icanhazip.com

Independientemente del método que utilice para obtener su dirección IP, puede escribirla en la barra de direcciones de su navegador web para llegar a su servidor.

### **Paso 3: Compruebe su servidor web**

Al final del proceso de instalación, Ubuntu 16.04 inicia Apache. El servidor web ya debería estar en funcionamiento.

Podemos verificar con *systemd* para asegurarnos de que el servicio está funcionando escribiendo:

sudo systemctl status apache2

**Output**  
● apache2.service - LSB: Apache2 web server  
 Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)  
 Drop-In: /lib/systemd/system/apache2.service.d  
 └─apache2-systemd.conf  
 Active: active (running) since Fri 2017-05-19 18:30:10 UTC; 1h 5min ago  
 Docs: man:systemd-sysv-generator(8)  
 Process: 4336 ExecStop=/etc/init.d/apache2 stop (code=exited, status=0/SUCCESS)  
 Process: 4359 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCESS)  
 Tasks: 55  
 Memory: 2.3M  
 CPU: 4.094s  
 CGroup: /system.slice/apache2.service  
 ├─4374 /usr/sbin/apache2 -k start  
 ├─4377 /usr/sbin/apache2 -k start  
 └─4378 /usr/sbin/apache2 -k start  
  
May 19 18:30:09 ubuntu-512mb-nyc3-01 systemd[1]: Stopped LSB: Apache2 web server.  
May 19 18:30:09 ubuntu-512mb-nyc3-01 systemd[1]: Starting LSB: Apache2 web server...  
May 19 18:30:09 ubuntu-512mb-nyc3-01 apache2[4359]: \* Starting Apache httpd web server apache2  
May 19 18:30:09 ubuntu-512mb-nyc3-01 apache2[4359]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message  
May 19 18:30:10 ubuntu-512mb-nyc3-01 apache2[4359]: \*  
May 19 18:30:10 ubuntu-512mb-nyc3-01 systemd[1]: Started LSB: Apache2 web server.

Como puede ver arriba, el servicio parece haber comenzado con éxito. Sin embargo, la mejor manera de probar esto es solicitar una página a Apache.

Puede acceder a la página de destino predeterminada de Apache para confirmar que el software funciona correctamente. Puede acceder a ella a través del nombre de dominio o de la dirección IP de su servidor (generalmente es <http://localhost/> o <http://127.0.0.1/> ).

Debería ver la página web predeterminada de Ubuntu 16.04 Apache, que debería ser algo como en la siguiente imagen:



Ejemplo de servidor Apache activo.

### **Gestionar el proceso de Apache**

Ahora que tiene su servidor web en funcionamiento, podemos repasar algunos comandos básicos de administración.

Para detener su servidor web, puede escribir:

sudo systemctl stop apache2

Para iniciar el servidor web cuando se detiene, escriba:

sudo systemctl start apache2

Para detenerse y luego volver a iniciar el servicio, escriba:

sudo systemctl restart apache2

Si simplemente está haciendo cambios de configuración, Apache a menudo puede recargar sin dejar caer las conexiones. Para ello, puede utilizar este comando:

sudo systemctl reload apache2

Por defecto, Apache está configurado para que se inicie automáticamente cuando el servidor arranque. Si esto no es lo que quieres, puedes desactivar este comportamiento escribiendo:

sudo systemctl disable apache2

Para volver a habilitar el servicio para que se inicie al arrancar, puede escribir:

sudo systemctl enable apache2

Ahora Apache debería iniciarse automáticamente cuando el servidor arranque de nuevo.

### **Familiaricese con los archivos y directorios importantes de Apache**

Ahora que ya sabe cómo administrar el servicio en sí, debería tomarse unos minutos para familiarizarse con algunos directorios y archivos importantes.

#### **Contenido**

* **/var/www/html:** El contenido web real, que por defecto sólo consiste en la página por defecto de Apache que ha visto antes, se sirve desde el directorio **/var/www/html**. Esto se puede cambiar alterando los archivos de configuración de Apache.

#### **Configuración del servidor**

* **/etc/apache2:** El directorio de configuración de Apache. Todos los archivos de configuración de Apache residen aquí.
* **/etc/apache2/apache2.conf:** El archivo de configuración principal de Apache. Esto puede ser modificado para hacer cambios en la configuración global de Apache. Este fichero es responsable de cargar muchos de los otros ficheros en el directorio de configuración.
* **/etc/apache2/ports.conf:** Este archivo especifica los puertos en los que Apache escuchará. Por defecto, Apache escucha en el puerto 80 y adicionalmente escucha en el puerto 443 cuando un módulo que proporciona capacidades SSL está habilitado.
* **/etc/apache2/sites-available/:** El directorio donde se pueden almacenar los "hosts virtuales" de cada sitio. Apache no usará los ficheros de configuración que se encuentran en este directorio a menos que estén enlazados al directorio habilitado para sitios (ver más abajo). Típicamente, toda la configuración de bloques de servidor se realiza en este directorio, y luego se habilita enlazando al otro directorio con el comando **a2ensite**.
* **/etc/apache2/sites-enabled/:** El directorio donde está habilitado cada sitio "Virtual Host" es almacenado. Por lo general, se crean enlazando a los archivos de configuración que se encuentran en el directorio **sites-available** con **a2ensite**. Apache lee los archivos de configuración y los enlaces que se encuentran en este directorio cuando se inicia o se recarga para compilar una configuración completa.
* **/etc/apache2/conf-available/**, **/etc/apache2/conf-enabled/**: Estos directorios tienen la misma relación que **sites-available** y **sites-enabled**, pero se utilizan para almacenar fragmentos de configuración que no pertenecen a un Virtual Host. Los archivos en el directorio disponible pueden ser habilitados con el comando **a2enconf** y deshabilitados con el comando **a2disconf**.
* **/etc/apache2/mods-available/**, **/etc/apache2/mods-enabled/**: Estos directorios contienen los módulos disponibles y habilitados, respectivamente. Los archivos que terminan en **.load** contienen fragmentos para cargar módulos específicos, mientras que los que terminan en **.conf** contienen la configuración de esos módulos. Los módulos se pueden habilitar y deshabilitar utilizando los comandos **a2enmod** y **a2dismod**.

#### **Registros del servidor**

* **/var/log/apache2/access.log:** Por defecto, cada petición a su servidor web se registra en este archivo de registro a menos que Apache esté configurado para hacer lo contrario.
* **/var/log/apache2/error.log:** Por defecto, todos los errores se registran en este archivo. La directiva **LogLevel** en la configuración de Apache especifica cuánto detalle contendrán los registros de errores.

## **Preparar MySQL**

Ahora que tenemos nuestro servidor web funcionando, es el momento de preparar MySQL. MySQL es un sistema de gestión de bases de datos. Básicamente, organizará y proporcionará acceso a bases de datos donde nuestro sitio puede almacenar información.

Durante la instalación, su servidor le pedirá que seleccione y confirme una contraseña para el usuario "root" de MySQL. Esta es una cuenta administrativa en MySQL que ha aumentado los privilegios. Piense que es similar a la cuenta root del propio servidor (sin embargo, la que está configurando ahora es una cuenta específica de MySQL). Asegúrese de que se trata de una contraseña segura y única, y no la deje en blanco.

Cuando la instalación esté completa, queremos ejecutar un sencillo script de seguridad que eliminará algunos valores predeterminados peligrosos y bloqueará un poco el acceso a nuestro sistema de base de datos. Inicie el script interactivo ejecutando:

mysql\_secure\_installation

Se le pedirá que introduzca la contraseña que ha establecido para la cuenta root de MySQL. A continuación, se le preguntará si desea configurar el **VALIDATE PASSWORD PLUGIN**.

**Advertencia:** Habilitar esta función es algo así como un juicio de valor. Si está habilitado, las contraseñas que no coincidan con los criterios especificados serán rechazadas por MySQL con un error. Esto causará problemas si utiliza una contraseña débil junto con un software que configura automáticamente las credenciales de usuario de MySQL, como los paquetes Ubuntu para phpMyAdmin. Es seguro dejar la validación desactivada, pero siempre debe usar contraseñas fuertes y únicas para las credenciales de la base de datos.

Responde **y** para que sí, o para que cualquier otra cosa continúe sin permitirlo.

VALIDATE PASSWORD PLUGIN can be used to test passwords

and improve security. It checks the strength of password

and allows the users to set only those passwords which are

secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No:

Se le pedirá que seleccione un nivel de validación de contraseña. Tenga en cuenta que si introduce 2, para el nivel más alto, recibirá errores al intentar establecer cualquier contraseña que no contenga números, letras mayúsculas y minúsculas y caracteres especiales, o que esté basada en palabras comunes del diccionario.

There are three levels of password validation policy:

LOW Length >= 8

MEDIUM Length >= 8, numeric, mixed case, and special characters

STRONG Length >= 8, numeric, mixed case, special characters and dictionary file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 1

Si habilitó la validación de contraseña, se le mostrará una contraseña segura para la contraseña de root existente y se le preguntará si desea cambiarla. Si está satisfecho con su contraseña actual, introduzca n para "no" en la solicitud:

Using existing password for root.

Estimated strength of the password: 100

Change the password for root ? ((Press y|Y for Yes, any other key for No) : n

Para el resto de las preguntas, pulse Y y pulse la tecla Intro en cada pregunta. Esto eliminará algunos usuarios anónimos y la base de datos de prueba, deshabilitará los inicios de sesión remotos y cargará estas nuevas reglas para que MySQL respete inmediatamente los cambios que hemos realizado.

En este punto, su sistema de base de datos ya está configurado y podemos seguir adelante.

## **Preparar PHP**

PHP es el componente de nuestra configuración que procesará el código para mostrar contenido dinámico. Puede ejecutar scripts, conectarse a nuestras bases de datos MySQL para obtener información y entregar el contenido procesado a nuestro servidor web para su visualización.

En la mayoría de los casos, queremos modificar la forma en que Apache sirve los ficheros cuando se solicita un directorio. Actualmente, si un usuario solicita un directorio desde el servidor, Apache buscará primero un archivo llamado **index.html**. Queremos decirle a nuestro servidor web que prefiera los archivos PHP, así que haremos que Apache busque primero un archivo **index.php**.

Para ello, escriba este comando para abrir el archivo **dir.conf** en un editor de texto con privilegios de root:

sudo nano /etc/apache2/mods-enabled/dir.conf

Se verá así:

**/etc/apache2/mods-enabled/dir.conf**

<IfModule mod\_dir.c>  
 DirectoryIndex index.html index.cgi index.pl index.php index.xhtml index.htm  
</IfModule>

Queremos mover el archivo índice PHP resaltado arriba a la primera posición después de la especificación DirectoryIndex, así:

**/etc/apache2/mods-enabled/dir.conf**

<IfModule mod\_dir.c>  
 DirectoryIndex index.php index.html index.cgi index.pl index.xhtml index.htm  
</IfModule>

Cuando haya terminado, guarde y cierre el archivo presionando **Ctrl-X**. Tendrá que confirmar el archivo guardado escribiendo **Y** y luego presionando **Enter** para confirmar la ubicación del archivo guardado.

Después de esto, necesitamos reiniciar el servidor web Apache para que nuestros cambios sean reconocidos. Puede hacerlo escribiendo esto:

sudo systemctl restart apache2

También podemos comprobar el estado del servicio **apache2** usando **systemctl**:

sudo systemctl status apache2

**Sample Output**  
● apache2.service - LSB: Apache2 web server  
 Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)  
 Drop-In: /lib/systemd/system/apache2.service.d  
 └─apache2-systemd.conf  
 Active: active (running) since Wed 2016-04-13 14:28:43 EDT; 45s ago  
 Docs: man:systemd-sysv-generator(8)  
 Process: 13581 ExecStop=/etc/init.d/apache2 stop (code=exited, status=0/SUCCESS)  
 Process: 13605 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCESS)  
 Tasks: 6 (limit: 512)  
 CGroup: /system.slice/apache2.service  
 ├─13623 /usr/sbin/apache2 -k start  
 ├─13626 /usr/sbin/apache2 -k start  
 ├─13627 /usr/sbin/apache2 -k start  
 ├─13628 /usr/sbin/apache2 -k start  
 ├─13629 /usr/sbin/apache2 -k start  
 └─13630 /usr/sbin/apache2 -k start  
  
Apr 13 14:28:42 ubuntu-16-lamp systemd[1]: Stopped LSB: Apache2 web server.  
Apr 13 14:28:42 ubuntu-16-lamp systemd[1]: Starting LSB: Apache2 web server...  
Apr 13 14:28:42 ubuntu-16-lamp apache2[13605]: \* Starting Apache httpd web server apache2  
Apr 13 14:28:42 ubuntu-16-lamp apache2[13605]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName’  
Apr 13 14:28:43 ubuntu-16-lamp apache2[13605]: \*  
Apr 13 14:28:43 ubuntu-16-lamp systemd[1]: Started LSB: Apache2 web server.

### **Instalar módulos PHP**

PAra que Apache pueda ejecutar código PHP, se tiene que instalar los módulos correspondientes. para esto ejecutamos el siguiente comando

sudo apt-get install php libapache2-mod-php

Después de esto debemos habilitarlos para Apache. Tenemos que verificar la versión de apache que tenemos. En el resultado del comando anterior nos debe decir qué versión de módulo ha instalado. en nuestro caso ha sido el 7.2

sudo a2enmod mpm\_prefork && sudo a2enmod php7.2

Por último debemos reiniciar Apache

sudo service apache2 restart

Para mejorar la funcionalidad de PHP, opcionalmente podemos instalar algunos módulos adicionales.

Para ver las opciones disponibles para los módulos y bibliotecas PHP, puede canalizar los resultados de la búsqueda apt-cache hacia less, un buscapersonas que le permite desplazarse a través de la salida de otros comandos:

apt-cache search php- | less

Utilice las teclas de flecha para desplazarse hacia arriba y hacia abajo, y **q** para salir.

Los resultados son todos los componentes opcionales que puede instalar. Le dará una breve descripción de cada uno de ellos:

**libnet-libidn-perl - Perl bindings for GNU Libidn  
 php-all-dev - package depending on all supported PHP development packages  
 php-cgi - server-side, HTML-embedded scripting language (CGI binary) (default)  
 php-cli - command-line interpreter for the PHP scripting language (default)  
 php-common - Common files for PHP packages  
 php-curl - CURL module for PHP [default]  
 php-dev - Files for PHP module development (default)  
 php-gd - GD module for PHP [default]  
 php-gmp - GMP module for PHP [default]  
 …  
 :**

Para obtener más información sobre lo que hace cada módulo, puede buscar en Internet o puede ver la descripción larga del paquete escribiendo:

apt-cache show package\_name

Habrá mucha salida, con un campo llamado **Description-en** que tendrá una explicación más larga de la funcionalidad que proporciona el módulo.

Por ejemplo, para saber qué hace el módulo **php-cli**, podríamos escribir esto:

apt-cache show php-cli

Junto con una gran cantidad de otra información, encontrará algo que se parece a esto:

**Output  
 …  
 Description-en: command-line interpreter for the PHP scripting language (default)  
 This package provides the /usr/bin/php command interpreter, useful for  
 testing PHP scripts from a shell or performing general shell scripting tasks.  
 .  
 PHP (recursive acronym for PHP: Hypertext Preprocessor) is a widely-used  
 open source general-purpose scripting language that is especially suited  
 for web development and can be embedded into HTML.  
 .  
 This package is a dependency package, which depends on Debian's default  
 PHP version (currently 7.0).  
 …**

Si, después de investigar, decide que le gustaría instalar un paquete, puede hacerlo usando el comando **apt-get install** como hemos estado haciendo con nuestro otro software.

Si decidimos que **php-cli** es algo que necesitamos, podríamos escribir a máquina:

sudo apt-get install php-cli

Si desea instalar más de un módulo, puede hacerlo listando cada uno, separado por un espacio, siguiendo el comando apt-get install, así:

sudo apt-get install package1 package2 ...

En este punto, su pila LAMP está instalada y configurada. Sin embargo, aún así deberíamos probar nuestro PHP.

### **Pruebe el procesamiento de PHP en su servidor web**

Para comprobar que nuestro sistema está configurado correctamente para PHP, podemos crear un script PHP muy básico.

Llamaremos a este script **info.php**. Para que Apache pueda encontrar el archivo y servirlo correctamente, debe ser guardado en un directorio muy específico, que se llama "web root".

En Ubuntu 16.04, este directorio se encuentra en **/var/www/html/**. Podemos crear el archivo en esa ubicación escribiendo:

sudo nano /var/www/html/info.php

Esto abrirá un archivo en blanco. Queremos poner el siguiente texto, que es código PHP válido, dentro del archivo:

**info.php**

<?php  
 phpinfo();  
?>

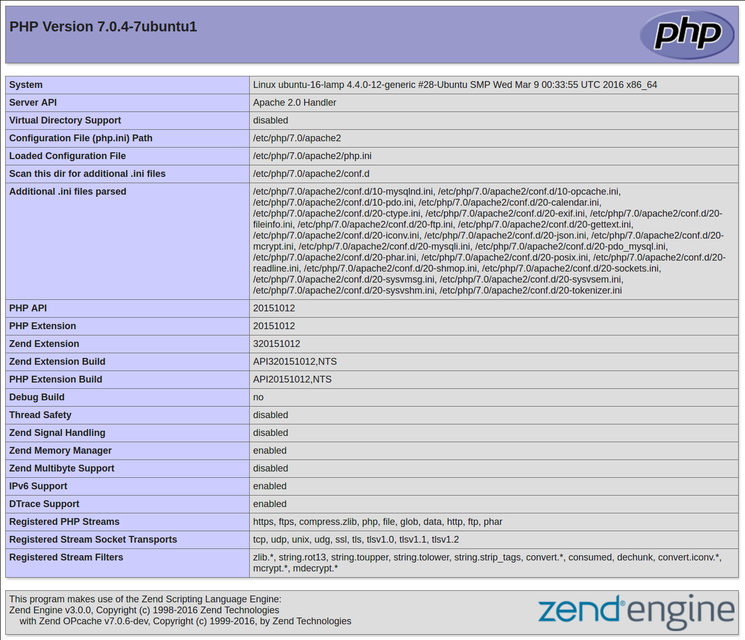
Cuando haya terminado, guarde y cierre el archivo.

Ahora podemos comprobar si nuestro servidor web puede mostrar correctamente el contenido generado por un script PHP. Para probar esto, sólo tenemos que visitar esta página en nuestro navegador web. Necesitará de nuevo la dirección IP pública de su servidor.

La dirección que desea visitar será:

[http://your\_server\_IP\_address/info.php](http://your_server_ip_address/info.php)

La página a la que llegas debe ser algo así:



Esta página básicamente le da información sobre su servidor desde la perspectiva de PHP. Es útil para depurar y para asegurarse de que la configuración se está aplicando correctamente.

Si esto fue exitoso, entonces su PHP está funcionando como se esperaba.

Es probable que desee eliminar este archivo después de esta prueba, ya que podría proporcionar información sobre su servidor a usuarios no autorizados. Para ello, puede escribirlo:

sudo rm /var/www/html/info.php

Siempre puede volver a crear esta página si necesita volver a acceder a la información más tarde.

# 

# **Instalación**

Instalar paquetes como usuario root es útil porque tiene todos los privilegios.

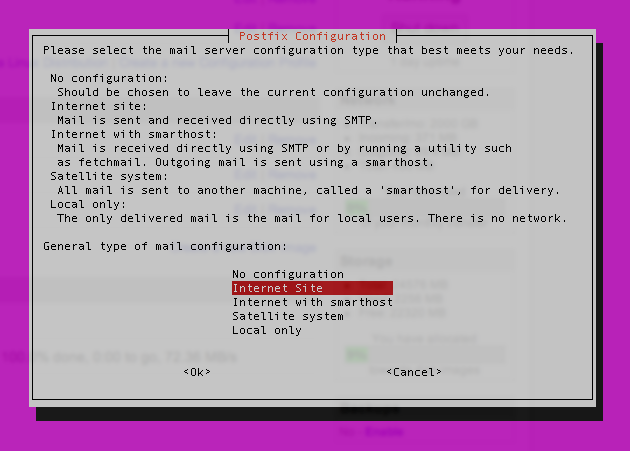
sudo -i

Introduzca la contraseña de su usuario. Una vez que tenga éxito, verá que el símbolo $ cambia a #.

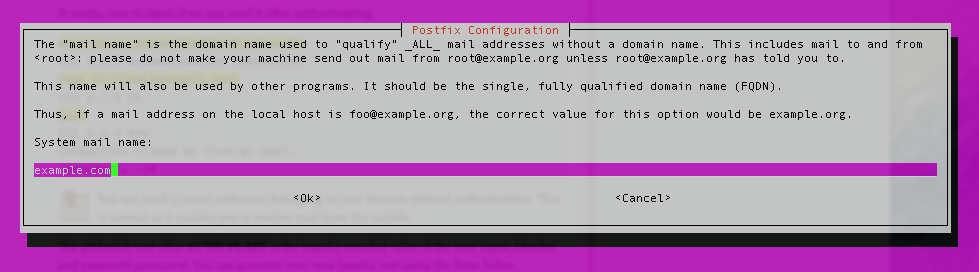
## **Instalar paquetes**

apt-get install postfix postfix-mysql dovecot-core dovecot-imapd dovecot-lmtpd dovecot-mysql

Cuando se le solicite la configuración de Postfix, seleccione Sitio de Internet:



La configuración de Postfix le preguntará sobre el nombre de correo del sistema - puede usar su FDQN o dominio principal, como ejemplo: example.com.



## **Crear base de datos MySQL, Dominios Virtuales, Usuarios y Aliases**

Una vez finalizada la instalación, vamos a crear una base de datos MySQL para configurar tres tablas diferentes: una para dominios, otra para usuarios y la última para alias.

Vamos a nombrar la base de datos servermail, pero puede usar el nombre que quiera.

Cree la base de datos de servermail:

mysqladmin -p create servermail

Iniciar sesión como usuario root de MySQL

mysql -u root -p

Ingrese la contraseña de su usuario root MySQL; si tiene éxito, verá:

mysql >

### **Crear Usuario de MySQL para Postfix**

MySQL es un manejador de base de datos de código libre que ayuda a los usuarios a almacenar, organizar y recolectar datos. Tiene variedad de opciones para otorgar a determinados usuarios permisos entre tablas y bases de datos, éste tutorial te dará una pequeña introducción a algunas de estas opciones.

Primero tenemos que crear un nuevo usuario, específico para la autenticación de correo, y también le vamos a dar permiso de tipo SELECT.

mysql > GRANT SELECT ON servermail.\* TO 'mysql\_user'@'127.0.0.1' IDENTIFIED BY 'mysqlpass';

Después de eso, necesitamos recargar los privilegios de MySQL para asegurarnos de que se aplicaron los permisos con éxito:

mysql > FLUSH PRIVILEGES;

Finalmente necesitamos usar la base de datos para crear tablas e introducir nuestros datos:

mysql> USE servermail;

**Nota:** Si quiere saber más sobre cómo crear usuarios en MySQL y otorgar permisos visite:

**https://www.digitalocean.com/community/tutorials/crear-un-nuevo-usuario-y-otorgarle-permisos-en-mysql-es**

### **Crear tablas para los VirtualHosts**

Vamos a crear una tabla para los dominios específicos, reconocidos como dominios autorizados.

CREATE TABLE `virtual\_domains` (  
 `id` INT NOT NULL AUTO\_INCREMENT,

`name` VARCHAR(50) NOT NULL,

PRIMARY KEY (`id`)

) ENGINE=InnoDB DEFAULT CHARSET=utf8;

Vamos a crear una tabla para presentar a los usuarios. Aquí usted agregará la dirección de correo electrónico y las contraseñas. Es necesario asociar a cada usuario con un dominio.

CREATE TABLE `virtual\_users` (

`id` INT NOT NULL AUTO\_INCREMENT,

`domain\_id` INT NOT NULL,

`password` VARCHAR(106) NOT NULL,

`email` VARCHAR(120) NOT NULL,

PRIMARY KEY (`id`),

UNIQUE KEY `email` (`email`),

FOREIGN KEY (domain\_id) REFERENCES virtual\_domains(id) ON DELETE CASCADE

) ENGINE=InnoDB DEFAULT CHARSET=utf8;

Finalmente vamos a crear una tabla de alias virtuales para especificar todos los emails que vas a reenviar al otro email.

CREATE TABLE `virtual\_aliases` (

`id` INT NOT NULL AUTO\_INCREMENT,

`domain\_id` INT NOT NULL,

`source` varchar(100) NOT NULL,

`destination` varchar(100) NOT NULL,

PRIMARY KEY (`id`),

FOREIGN KEY (domain\_id) REFERENCES virtual\_domains(id) ON DELETE CASCADE

) ENGINE=InnoDB DEFAULT CHARSET=utf8;

Hemos creado las tres tablas con éxito. Ahora vamos a introducir los datos.

#### **Dominios virtuales**

Aquí vamos a introducir sus dominios dentro de la tabla virtual\_domains. Puede añadir todos los dominios que quiera, pero en este tutorial vamos a introducir sólo el dominio principal (adminsr.org) y tu FQDN (nombre de host.adminsr.org).

INSERT INTO `servermail`.`virtual\_domains`

(`id` ,`name`)

VALUES

('1', 'adminsr.org'),

('2', 'hostname.adminsr.org');

#### **Emails Virtuales**

Vamos a introducir las cuentas de correo electrónico y las contraseñas asociadas a cada dominio. Asegúrese de cambiar toda la información con su información específica.

INSERT INTO `servermail`.`virtual\_users`

(`id`, `domain\_id`, `password` , `email`)

VALUES

('1', '1', ENCRYPT('123456', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'admin@adminsr.org'),

('2', '1', ENCRYPT('qwerty', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'user1@adminsr.org');

#### **Alias virtuales**

Vamos a introducir la dirección de correo electrónico (fuente) que vamos a reenviar a la otra dirección de correo electrónico (destino). En este tutorial no son necesarios alias, sin embargo en el siguiente código se puede ver como ingresar un registro en esta tabla.

INSERT INTO `servermail`.`virtual\_aliases`

(`id`, `domain\_id`, `source`, `destination`)

VALUES

('1', '1', 'alias@example.com', 'email1@example.com');

Salir de MySQL

mysql > exit

## **Configurar Postfix**

Vamos a configurar Postfix para manejar las conexiones SMTP y enviar los mensajes para cada usuario introducido en la base de datos MySQL.

Primero tenemos que crear una copia del archivo por defecto, en caso de que quieras volver a la configuración por defecto.

cp /etc/postfix/main.cf /etc/postfix/main.cf.orig

Abra el archivo main.cf para modificarlo:

nano /etc/postfix/main.cf

Primero tenemos que comentar los parámetros de TLS y añadir otros parámetros. En este tutorial, estamos utilizando los certificados SSL Gratuitos y las rutas que se sugieren en el tutorial, pero usted puede modificar en función de sus configuraciones personales.

**/etc/postfix/main.cf**

[…]

# TLS parameters

#smtpd\_tls\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

#smtpd\_tls\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key

#smtpd\_use\_tls=yes

#smtpd\_tls\_session\_cache\_database = btree:${data\_directory}/smtpd\_scache

#smtp\_tls\_session\_cache\_database = btree:${data\_directory}/smtp\_scache

smtpd\_tls\_cert\_file=/etc/ssl/certs/dovecot.pem

smtpd\_tls\_key\_file=/etc/ssl/private/dovecot.pem

smtpd\_use\_tls=yes

smtpd\_tls\_auth\_only = yes

[...]

Luego vamos a añadir los siguientes parámetros debajo de la configuración de TLS que hemos cambiado en el paso anterior:

**/etc/postfix/main.cf**

[…]

smtpd\_sasl\_type = dovecot

smtpd\_sasl\_path = private/auth

smtpd\_sasl\_auth\_enable = yes

smtpd\_recipient\_restrictions = permit\_sasl\_authenticated, permit\_mynetworks, reject\_unauth\_destination

[...]

Necesitamos comentar la configuración por defecto de mydestination y reemplazarla con localhost. Este cambio permite a su VPS utilizar los dominios virtuales dentro de la tabla MySQL.

**/etc/postfix/main.cf**

[…]

#mydestination = example.com, hostname.example.com, localhost.example.com, localhost

mydestination = localhost

[...]

Hágale saber a Postfix sobre las IPs que debe considerar parte de la LAN:

Asumiremos que 192.168.1.0/24 es su LAN local. Puede omitir este paso con seguridad si no tiene otros equipos en la misma red local.

**/etc/postfix/main.cf**

[…]

mynetworks = 127.0.0.0/8, 192.168.1.0/24

[...]

Verifique que el parámetro myhostname esté configurado con su FQDN.

**/etc/postfix/main.cf**

[…]

myhostname = adminsr.org

[...]

Añada la siguiente línea para la entrega de correo local a todos los dominios virtuales listados dentro de la tabla MySQL.

**/etc/postfix/main.cf**

[…]

virtual\_transport = lmtp:unix:private/dovecot-lmtp

[...]

Finalmente, necesitamos añadir estos tres parámetros para indicar a Postfix que configure los dominios, usuarios y alias virtuales.

**/etc/postfix/main.cf**

[…]

virtual\_mailbox\_domains = mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf

virtual\_mailbox\_maps = mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf

virtual\_alias\_maps = mysql:/etc/postfix/mysql-virtual-alias-maps.cf

virtual\_mailbox\_base = /var/mail/vhosts

**Nota:** Compare estos cambios con este archivo para detectar errores o equivocaciones:

**https://www.dropbox.com/s/kgny3l1es8cj16m/main.cf.txt**

### **Crear archivos para conectar con la base de datos**

Vamos a crear los tres últimos archivos que añadimos en el archivo main.cf para indicarle a Postfix cómo conectarse con MySQL.

Primero tenemos que crear el archivo mysql-virtual-mailbox-domains.cf. Es necesario cambiar los valores dependiendo de su configuración personal.

nano /etc/postfix/mysql-virtual-mailbox-domains.cf

**/etc/postfix/mysql-virtual-mailbox-domains.cf**

user = mysql\_user

password = mysqlpass

hosts = 127.0.0.1

dbname = servermail

query = SELECT 1 FROM virtual\_domains WHERE name='%s'

Entonces necesitamos reiniciar Postfix.

service postfix restart

Necesitamos asegurarnos de que Postfix encuentra su dominio, así que necesitamos probarlo con el siguiente comando. Si tiene éxito, debería devolver 1:

postmap -q adminsr.org mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf

Entonces necesitamos crear el archivo mysql-virtual-mailbox-maps.cf.

nano /etc/postfix/mysql-virtual-mailbox-maps.cf

**/etc/postfix/mysql-virtual-mailbox-maps.cf**

user = mysql\_user

password = mysqlpass

hosts = 127.0.0.1

dbname = servermail

query = SELECT 1 FROM virtual\_users WHERE email='%s'

Necesitamos reiniciar Postfix de nuevo.

service postfix restart

En este momento vamos a asegurarnos de que Postfix encuentre su primera dirección de correo electrónico con el siguiente comando. Debería devolver 1 si tiene éxito:

postmap -q admin@adminsr.org mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf

Finalmente, vamos a crear el último archivo para configurar la conexión entre Postfix y MySQL.

nano /etc/postfix/mysql-virtual-alias-maps.cf

**/etc/postfix/mysql-virtual-alias-maps.cf**

user = mysql\_user

password = mysqlpass

hosts = 127.0.0.1

dbname = servermail

query = SELECT destination FROM virtual\_aliases WHERE source='%s'

Reiniciar Postfix

service postfix restart

Necesitamos verificar que Postfix pueda encontrar sus alias. Introduzca el siguiente comando y devolverá el correo reenviado al alias:

postmap -q alias@example.com mysql:/etc/postfix/mysql-virtual-alias-maps.cf

### **Activar SSL**

Si desea habilitar el puerto 587 para conectarse de forma segura con clientes de correo electrónico, es necesario modificar el archivo **/etc/postfix/master.cf**

nano /etc/postfix/master.cf

Necesitamos descomentar estas líneas y añadir otros parámetros:

**/etc/postfix/master.cf**

[…]

submission inet n - - - - smtpd

-o syslog\_name=postfix/submission

-o smtpd\_tls\_security\_level=encrypt

-o smtpd\_sasl\_auth\_enable=yes

-o smtpd\_client\_restrictions=permit\_sasl\_authenticated,reject

-o smtpd\_relay\_restrictions=permit\_sasl\_authenticated,reject

[…]

**Nota:** Las líneas **-o** deben comenzar con al menos un espacio en blanco. **Master.cf** consiste en 'líneas lógicas' que pueden abarcar múltiples líneas reales. Una línea real termina con un final de línea; una línea lógica termina después del final de línea de la última continuación. Una continuación se define por uno o más espacios en blanco al principio. Lo más fácil es mostrar esto con un ejemplo:

Una línea real:

submission inet n - - - - smtpd

Una línea lógica:

submission inet n - - - - smtpd

-o syslog\_name=postfix/submission

-o smtpd\_tls\_security\_level=encrypt

Por lo tanto, tenga cuidado de comenzar las líneas de continuación con al menos un espacio y también al revés: por ejemplo, al descomentar la primera de una línea lógica, tenga cuidado de no dejar un espacio en blanco delante de ella o la línea se verá como una continuación de la línea anterior, lo que resultará en todo tipo de confusión.

En algunos casos, necesitamos reiniciar Postfix para asegurarnos de que el puerto 587 está abierto.

service postfix restart

**Nota:** Puede utilizar esta herramienta para analizar los puertos de dominio y comprobar que los puertos 25 y 587 están abiertos (**http://mxtoolbox.com/SuperTool.aspx**).

### **Configurar Relay**

En caso de no contar con un dominio público propio, se puede configurar un relay para poder mandar correos electrónicos a dominios externos en internet. A continuación se dará un ejemplo de cómo se puede hacer esto con Gmail.

Primero, instale todos los paquetes necesarios:

apt-get install mailutils libsasl2-2 ca-certificates libsasl2-modules

A continuación, abra el archivo de configuración de postfix:

nano /etc/postfix/main.cf

Y ponga las siguientes líneas como a continuación:

**/etc/postfix/main.cf**

[…]

relayhost = [smtp.gmail.com]:587

smtp\_sasl\_auth\_enable = yes

smtp\_sasl\_password\_maps = hash:/etc/postfix/sasl\_passwd

smtp\_sasl\_security\_options = noanonymous

smtp\_tls\_CAfile = /etc/postfix/cacert.pem

smtp\_use\_tls = yes

[…]

Es posible que haya notado que no hemos especificado nuestro nombre de usuario ni contraseña de Gmail en las líneas anteriores. Ellos irán a un archivo diferente. Abrir/Crear

nano /etc/postfix/sasl\_passwd

Y añade la siguiente línea:

**/etc/postfix/sasl\_passwd**

[smtp.gmail.com]:587 USERNAME@gmail.com:PASSWORD

Si quiere utilizar un dominio personal de Google App, sustituya @gmail.com por @dominio.com.

Corregir permisos y actualizar la configuración de postfix para usar el archivo sasl\_passwd:

sudo chmod 400 /etc/postfix/sasl\_passwd

sudo postmap /etc/postfix/sasl\_passwd

A continuación, valide los certificados para evitar errores. Sólo tiene que ejecutar el siguiente comando:

cat /etc/ssl/certs/Thawte\_Premium\_Server\_CA.pem | sudo tee -a /etc/postfix/cacert.pem

**Nota:** Si tiene problemas con el comando anterior, intente cambiar el nombre del certificado a **thawte\_Primary\_Root\_CA.pem** en el comando anterior.

Por último, vuelva a cargar la configuración de postfix para que los cambios surtan efecto:

sudo /etc/init.d/postfix reload

### **Pruebas**

#### **Compruebe si los mensajes se envían a través del servidor SMTP de Gmail.**

Si ha configurado todo correctamente, el siguiente comando debería generar un correo de prueba desde su servidor a su buzón de correo.

echo "Test mail from postfix" | mail -s "Test Postfix" you@example.com

Para verificar más precisamente, si el correo enviado desde el comando anterior se envía realmente a través del servidor SMTP de Gmail, puede iniciar sesión en la cuenta de Gmail USERNAME@gmail.com con CONTRASEÑA y comprobar la carpeta "Correo enviado" en esa cuenta de Gmail. De forma predeterminada, Gmail siempre conserva una copia del correo que se envía a través de su interfaz web, así como del servidor SMTP. Este registro es una de las razones por las que a menudo utilizamos Gmail cuando la entrega de correo es crítica.

Una vez configurado, todos los correos electrónicos de tu servidor se enviarán a través de Gmail. Este método será útil si tienes muchos sitios en tu servidor y quieres que todos envíen mensajes de correo electrónico a través del servidor SMTP de Gmail.

También puede utilizar un complemento como WP Mail SMTP para que los correos de su sitio WordPress concreto se envíen utilizando el servidor SMTP de Gmail.

Tenga en cuenta que el servidor SMTP de Gmail tiene un límite de 500 mensajes de correo electrónico al día. Por lo tanto, ¡utilícelo con prudencia! 🙂

### **Permitir Aplicaciones menos seguras en Gmail**

Para que Gmail sirva de relay, se deben permitir las aplicaciones menos seguras, esto se puede hacer siguiendo las instrucción de la siguiente liga

**https://support.google.com/accounts/answer/6010255**

### **Solución de problemas**

**Error: “SASL authentication failed; server smtp.gmail.com”**

Necesita desbloquear el captcha visitando esta página **https://www.google.com/accounts/DisplayUnlockCaptcha**

Puede ejecutar la prueba de nuevo después de desbloquear el captcha.

## **Configurar Dovecot**

Vamos a copiar los 7 archivos que vamos a modificar, para que pueda volver a la configuración predeterminada si es necesario. Introduzca los siguientes comandos uno por uno:

cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.orig

cp /etc/dovecot/conf.d/10-mail.conf /etc/dovecot/conf.d/10-mail.conf.orig

cp /etc/dovecot/conf.d/10-auth.conf /etc/dovecot/conf.d/10-auth.conf.orig

cp /etc/dovecot/dovecot-sql.conf.ext /etc/dovecot/dovecot-sql.conf.ext.orig

cp /etc/dovecot/conf.d/10-master.conf /etc/dovecot/conf.d/10-master.conf.orig

cp /etc/dovecot/conf.d/10-ssl.conf /etc/dovecot/conf.d/10-ssl.conf.orig

Edite el archivo de configuración desde Dovecot.

nano /etc/dovecot/dovecot.conf

Compruebe que esta opción no está comentada.

**/etc/dovecot/dovecot.conf**

[…]

!include conf.d/\*.conf

[…]

Vamos a habilitar protocolos (agregue pop3 si lo desea) debajo de la opción **!include\_try /usr/share/dovecot/protocols.d/\*.protocol line.**

**/etc/dovecot/dovecot.conf**

[…]

!include\_try /usr/share/dovecot/protocols.d/\*.protocol

protocols = imap lmtp

[…]

**Nota:** Compare estos cambios con este archivo para detectar errores o equivocaciones:

**https://www.dropbox.com/s/h0zqrosodve0crc/dovecot.conf.txt**

Luego vamos a editar el archivo de configuración de correo:

nano /etc/dovecot/conf.d/10-mail.conf

Busque la línea **mail\_location**, descoméntela y ponga el siguiente parámetro:

**/etc/dovecot/conf.d/10-mail.conf**

[…]

mail\_location = maildir:/var/mail/vhosts/%d/%n

[…]

Busque la línea **mail\_privileged\_group**, descoméntela y añada el parámetro mail así:

**/etc/dovecot/conf.d/10-mail.conf**

[…]

mail\_privileged\_group = vmail

[…]

**Nota:** Compare estos cambios con este archivo para detectar errores o equivocaciones:

**https://www.dropbox.com/s/pmjut5ah5xulcxq/10-mail.conf.txt**

### **¿A quién le pertenecen los correos?**

Postfix puede manejar dos tipos de usuarios: *usuarios virtuales* y *usuarios reales*. Root es un usuario real y el usuario principal también lo es, porque son cuentas de usuario en el servidor. Sin embargo, la mayoría de las personas que van a obtener una cuenta de correo electrónico en el servidor nunca se conectarán al servidor para trabajar con una cuenta de usuario local. No hay carpetas de inicio en el servidor, no hay preferencias de bash, etc. Así que para el correo vamos a usar usuarios virtuales.

En el caso de los usuarios reales, la pregunta de qué usuario debería ser el propietario del correo tenía una respuesta simple: *el usuario*. Con los usuarios virtuales esto es un poco diferente. Dado que no existe ningún usuario real, ¿quién debería ser el propietario del correo? Postfix ofrece dos opciones:

1. Crear uid's y gid's virtuales para acompañar las cuentas de usuario virtuales
2. Utilizar un uid y gid dedicado para todos los usuarios.

Dado que los usuarios virtuales no se conectarán al servidor, no hay nada malo en que no sean los propietarios de su correo. La opción 2 es más fácil y no menos segura, por lo que se optará por la opción 2.

Se debe agregar la siguiente informacion al archivo **main.cf** de **postffix**

nano /etc/postfix/main.cf

**/etc/postfix/main.cf**

[…]

virtual\_gid\_maps = static:5000

virtual\_uid\_maps = static:5000

virtual\_minimum\_uid = 5000

virtual\_minimum\_uid se utiliza para las configuraciones en las que se utilizarán usuarios separados para cada buzón de correo. Impide la recepción de correo para las cuentas del sistema. Usaremos un único propietario para todo el correo y su uid y gid serán 5000 por lo que el virtual\_mininum\_uid puede ser 5000 también.

#### **Verificar los permisos**

Introduzca este comando:

ls -ld /var/mail

Asegúrese de que los permisos sean así:

**Output:Add information about the owner of the mailboxes:**

drwxrwsr-x 3 root vmail 4096 Jan 24 21:23 /var/mail

Vamos a crear una carpeta para cada dominio que registremos en la tabla MySQL:

mkdir -p /var/mail/vhosts/adminsr.org

Crear un usuario y grupo de vmail con un ID de 5000

groupadd -g 5000 vmail

useradd -g vmail -u 5000 vmail -d /var/mail

Necesitamos cambiar el propietario de la carpeta **/var/mail** por el usuario de vmail.

chown -R vmail:vmail /var/mail

Luego tenemos que editar el archivo **/etc/dovecot/conf.d/10-auth.conf**:

nano /etc/dovecot/conf.d/10-auth.conf

Descomente la autenticación de texto plano y añada esta línea:

**/etc/dovecot/conf.d/10-auth.conf**

[…]

disable\_plaintext\_auth = yes

[…]

Modificar el parámetro **auth\_mechanisms**:

**/etc/dovecot/conf.d/10-auth.conf**

[…]

auth\_mechanisms = plain login

[…]

Comente esta línea:

**/etc/dovecot/conf.d/10-auth.conf**

[…]

#!include auth-system.conf.ext

[…]

Habilite la autorización MySQL descomentando esta línea:

**/etc/dovecot/conf.d/10-auth.conf**

[…]

!include auth-sql.conf.ext

[…]

**Nota:** Compare estos cambios con este archivo para detectar errores o equivocaciones:

**https://www.dropbox.com/s/frijd9eg0kt5ydr/10-auth.conf.txt**

Necesitamos modificar el archivo **/etc/dovecot/conf.d/auth-sql.conf.ext** con su información para la autenticación:

nano /etc/dovecot/conf.d/auth-sql.conf.ext

Introduzca el siguiente código en el archivo:

**/etc/dovecot/conf.d/auth-sql.conf.ext**

[…]

passdb {

driver = sql

args = /etc/dovecot/dovecot-sql.conf.ext

}

userdb {

driver = sql

args = /etc/dovecot/dovecot-sql.conf.ext

}

[…]

**Nota:** Compare estos cambios con este archivo para detectar errores o equivocaciones:

**https://www.dropbox.com/s/5mpdq9712hfktxs/auth-sql.conf.ext.txt**

Necesitamos modificar el archivo **/etc/dovecot/dovecot-sql.conf.ext** con nuestra información MySQL personalizada:

nano /etc/dovecot/dovecot-sql.conf.ext

Descomente el parámetro del controlador y configure mysql como parámetro:

**/etc/dovecot/dovecot-sql.conf.ext**

[…]

driver = mysql

[…]

Descomente la línea de conexión e introduzca su información específica de MySQL:

**/etc/dovecot/dovecot-sql.conf.ext**

[…]

connect = host=127.0.0.1 dbname=servermail user=mysql\_user password=mysqlpass

[…]

Descomente la línea de esquema **default\_pass\_scheme** y cámbiela a **SHA-512**.

**/etc/dovecot/dovecot-sql.conf.ext**

[…]

default\_pass\_scheme = SHA512-CRYPT

[…]

Descomente la línea **password\_query** y añada esta información:

**/etc/dovecot/dovecot-sql.conf.ext**

[…]

password\_query = SELECT email as user, password FROM virtual\_users WHERE email='%u';

[…]

Si lee los comentarios de **dovecot-sql.conf.ext** puede encontrar que puede usar consultas de usuario estáticas. Con las consultas estáticas de los usuarios, todas las búsquedas de los usuarios devuelven el mismo uid y gid, que es lo que necesitamos debido a la cuenta dedicada que usamos para los permisos en el correo. Así que por qué sacarlo de la base de datos con una consulta, usted puede preguntar. Porque se trata de una llamada consulta dinámica de usuario. Las consultas de usuario dinámicas son necesarias si desea poder utilizar la consulta de iteración. (Utilizar la consulta de iteración es preferible.)

Descomente la línea **user\_query** y añada esta información:

**/etc/dovecot/dovecot-sql.conf.ext**

[…]

user\_query = \

SELECT 5000 AS uid, 5000 as gid, email, \

'/var/mail/vmail/%d/%n' AS home \

FROM virtual\_users WHERE email = '%u'

[…]

Descomente la línea **iterate\_query** y añada esta información:

**/etc/dovecot/dovecot-sql.conf.ext**

[…]

iterate\_query = SELECT email AS user FROM virtual\_users

La consulta iterativa es necesaria para ciertos comandos de Dovecot como la búsqueda de correo con fines de gestión, como la eliminación automática de spam con más de treinta días de antigüedad o la compactación de buzones de correo.

**Nota:** Compare estos cambios con este archivo para detectar errores o equivocaciones:

**https://www.dropbox.com/s/i5m4pv0tvx12re7/dovecot-sql.conf.ext.txt**

Cambie el propietario y el grupo de la carpeta dovecot a usuario de vmail:

chown -R vmail:dovecot /etc/dovecot

chmod -R o-rwx /etc/dovecot

Abra y modifique el archivo **/etc/dovecot/conf.d/10-master.conf** (tenga cuidado porque se cambiarán diferentes parámetros).

nano /etc/dovecot/conf.d/10-master.conf

**/etc/dovecot/conf.d/10-master.conf**

[…]

##Uncomment inet\_listener\_imap and modify to port 0

service imap-login {

inet\_listener imap {

# se puede poner en 0, si se quiere forzar el uso de SSL

port = 143

}

inet\_listener imaps {

port = 993

ssl = yes

}

}

#Create LMTP socket and this configurations

service lmtp {

unix\_listener /var/spool/postfix/private/dovecot-lmtp {

mode = 0600

user = postfix

group = postfix

}

#inet\_listener lmtp {

# Avoid making LMTP visible for the entire internet

#address =

#port =

#}

}

[…]

Modifique el parámetro unix\_listener para service\_auth de esta manera:

**/etc/dovecot/conf.d/10-master.conf**

[…]

service auth {

unix\_listener /var/spool/postfix/private/auth {

mode = 0666

user = postfix

group = postfix

}

#unix\_listener auth-userdb {

#mode = 0600

#user = vmail

#group =

#}

#unix\_listener /var/spool/postfix/private/auth {

# mode = 0666

#}

user = dovecot

}

Modifique **service auth-worker** así:

**/etc/dovecot/conf.d/10-master.conf**

[…]

service auth-worker {

# Auth worker process is run as root by default, so that it can access

# /etc/shadow. If this isn't necessary, the user should be changed to

# $default\_internal\_user.

user = vmail

}

[…]

**Nota:** Compare estos cambios con este archivo para detectar errores o equivocaciones:

**https://www.dropbox.com/s/d4669daw2k1ri4t/10-master.conf.txt**

Finalmente, vamos a modificar el archivo de configuración SSL de Dovecot *(omita este paso si va a utilizar la configuración por defecto)*.

nano /etc/dovecot/conf.d/10-ssl.conf

Cambie el parámetro ssl a requerido:

**/etc/dovecot/conf.d/10-ssl.conf**

[…]

ssl = required

[…]

Y modificar la ruta para **ssl\_cert** y **ssl\_key**:

**/etc/dovecot/conf.d/10-ssl.conf**

[…]

ssl\_cert = </etc/ssl/certs/dovecot.pem

ssl\_key = </etc/ssl/private/dovecot.pem

[…]

Reinicie los servicios de dovecot y postfix:

service postfix restart && sudo service postfix restart

### **Instalando certificados**

TLS necesita OpenSSL; para instalar OpenSSL, simplemente ejecutamos:

apt-get -y install openssl

Después, podemos generar el certificado SSL de la siguiente manera:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/dovecot.pem -out /etc/ssl/certs/dovecot.pem

Se le harán una serie de preguntas. Antes de repasar eso, echemos un vistazo a lo que está sucediendo en el comando que estamos emitiendo:

* **openssl:** es la herramienta básica de la línea de comandos para crear y gestionar certificados, claves y otros archivos de OpenSSL.
* **req:** Este subcomando específica que queremos utilizar la gestión de solicitud de firma de certificado (CSR) X.509. El "X.509" es un estándar de infraestructura de clave pública al que se adhieren SSL y TLS para la gestión de claves y certificados. Queremos crear un nuevo cert X.509, así que estamos usando este subcomando.
* **-x509:** Esto modifica aún más el subcomando anterior al indicar a la utilidad que queremos hacer un certificado autofirmado en lugar de generar una solicitud de firma de certificado, como ocurriría normalmente.
* **-nodes:** Esto le indica a OpenSSL que omita la opción de asegurar nuestro certificado con una frase de contraseña. Necesitamos que Apache sea capaz de leer el archivo, sin intervención del usuario, cuando el servidor se inicie. Una frase de contraseña evitaría que esto ocurriera porque tendríamos que introducirla después de cada reinicio.
* **-days 365:** Esta opción establece el período de tiempo durante el cual el certificado se considerará válido. Lo fijamos para un año aquí.
* **-newkey rsa:2048:** Esto especifica que queremos generar un nuevo certificado y una nueva clave al mismo tiempo. No creamos la clave necesaria para firmar el certificado en un paso anterior, por lo que debemos crearla junto con el certificado. La porción rsa:2048 le dice que haga una clave RSA de 2048 bits de longitud.
* **-keyout:** Esta línea le indica a OpenSSL dónde colocar el archivo de clave privada generado que estamos creando.
* **-out:** Indica a OpenSSL dónde colocar el certificado que estamos creando.

Debemos descomentar los siguiente campos de **/etc/postfix/master.cf**:

**/etc/postfix/master.cf**

[…]

smtps inet n - - - - smtpd

-o syslog\_name=postfix/smtps

-o smtpd\_tls\_wrappermode=yes

-o smtpd\_sasl\_auth\_enable=yes

[…]

Reiniciar Dovecot

service dovecot restart

Debería comprobar que el puerto 993 está abierto y funcionando (en caso de que habilite pop3; debería comprobar también el puerto 995).

telnet example.com 993

Enhorabuena. Ha configurado correctamente su servidor de correo y puede probar su cuenta utilizando un cliente de correo electrónico:

- Username: email1@example.com

- Password: contraseña de la cuenta email1

- IMAP: example.com

- SMTP: example.com

**Nota:** utilice el puerto 993 para IMAP seguro y el puerto 587 o 25 para SMTP.

### **Pruebas**

El sistema está listo y configurado para que pueda empezar a hacer algunas pruebas. Puede verificar que los puertos y programas están corriendo con:

netstat -plntu

Puede intentar mandar un correo con Postfix desde telnet como se muestra a continuación (Tiene que ingresar uno por uno los comandos y modificando con su respectiva información):

#### **Postfix (SMTP)**

telnet localhost 25

EHLO adminsr.org

MAIL FROM:<SENDERADDRESS>

RCPT TO:<RECIPIENTADDRESS>

DATA

Subject: Testmessage

(Blank line, press Enter again)

This is a test.

(Blank line, press Enter again)

.

QUIT

#### **Dovecot (IMAP)**

Para probar Dovecot, que es el administrador de correos. puede probar con los siguientes comandos.

Primero de todo debemos hacer telnet al puerto IMAP (143):

telnet localhost 143

**Output**

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^]'.

\* OK Dovecot ready.

A continuación respondemos al servidor con “. LOGIN” seguido de el nombre de usuario y la contraseña:

. login admin@adminsr.org 123456

A continuación podemos listar todas las carpetas mediante el comando “**. LIST**“:

. list "" "\*"

A continuación podríamos ver el total de mensajes pendientes que hay en la carpeta **INBOX**. Esto lo podemos hacer mediante el comando “**. STATUS**“. Mediante “**messages**” nos indicará el total de mensajes y con “**unseen**” de estos lo que estan marcados como no leídos:

. status INBOX (messages)

. STATUS INBOX (unseen)

Para recuperar un mensaje primero de todo deberemos seleccionar la carpeta IMAP:

. SELECT INBOX

A continuación mediante “**. FETCH <primero>:<ultimo> FLAGS**” podemos obtener un listado de los mensajes y sus flags por rango:

. FETCH 1:3 FLAGS

Ahora sí nos interesa, por ejemplo, el mensaje 3 que no está leído podríamos obtener su subject mediante el siguiente comando:

. FETCH 3 (body[header.fields (subject)])

El contenido del mensaje lo podríamos obtener igualmente mediante **FETCH**:

. FETCH 3 rfc822.text

Para finalizar la sesión lo hacemos con “**. LOGOUT**“:

. LOGOUT

#### **Dovecot (IMAPS)**

Para probar la configuración de Dovecot mediante un puerto con una capa encriptada podemos ingresar al servidor con el siguiente comando:

openssl s\_client -connect localhost:993

Una vez ingresado podemos probar con los mismo comandos que utilizamos para IMAP, pero esta vez la comunicación entre cliente y servidor estará encriptada.

## 

## **Configurar SpamAssassin**

Tenga en cuenta que el filtrado de spam se realiza en dos fases:

1. El spam se identifica al entrar en el sistema.
2. El spam se entrega en una carpeta dedicada en la cuenta del usuario.

Estas fases son cosas separadas. Spamassassin identifica y etiqueta el spam mientras que el plugin Sieve de Dovecot permite poner automáticamente el spam en la carpeta Junk del usuario. Primero haremos la identificación de spam.

Primero necesitamos instalar SpamAssassin.

apt-get install spamassassin spamc

Entonces necesitamos crear un usuario para SpamAssassin.

adduser spamd --disabled-login

Para configurar correctamente SpamAssassin, es necesario abrir y modificar los ajustes de configuración.

nano /etc/default/spamassassin

Necesitamos cambiar el parámetro **ENABLED** para habilitar el demonio SpamAssassin.

**/etc/default/spamassassin**

[…]

ENABLED=1

[…]

Necesitamos configurar los parámetros de inicio y opciones.

**/etc/default/spamassassin**

[…]

SPAMD\_HOME="/var/log/spamassassin/"

OPTIONS="--create-prefs --max-children 5 --username spamd --helper-home-dir ${SPAMD\_HOME} -s ${SPAMD\_HOME}spamd.log"

[…]

Entonces necesitamos especificar el parámetro **PID\_File** así:

**/etc/default/spamassassin**

[…]

PIDFILE="${SPAMD\_HOME}spamd.pid"

[…]

Finalmente, necesitamos especificar que las reglas de SpamAssassin se actualizarán automáticamente.

**/etc/default/spamassassin**

[…]

CRON=1

**Nota:** Compare estos cambios con este archivo para detectar errores o equivocaciones:

**https://www.dropbox.com/s/ndvpgc2jipdd4bk/etc.default.spamassassin.txt**

Necesitamos abrir **/etc/spamassassin/local.cf** para establecer las reglas anti-spam.

nano /etc/spamassassin/local.cf

SpamAssassin calificará cada correo y si determina que este correo electrónico es superior a 5.0 en su verificación de spam, entonces automáticamente será considerado spam. Puede utilizar los siguientes parámetros para configurar las reglas antispam:

**/etc/spamassassin/local.cf**

[…]

rewrite\_header Subject \*\*\*\*\* SPAM \_SCORE\_ \*\*\*\*\*

report\_safe 0

required\_score 4.0

use\_bayes 1

use\_bayes\_rules 1

bayes\_auto\_learn 1

skip\_rbl\_checks 0

use\_razor2 0

use\_dcc 0

use\_pyzor 0

[…]

Necesitamos cambiar el archivo Postfix **/etc/postfix/master.cf** para indicarle que cada correo electrónico será verificado con SpamAssassin.

nano /etc/postfix/master.cf

Entonces necesitamos encontrar la siguiente línea y añadir el filtro spamassassin:

**/etc/postfix/master.cf**

[…]

smtp inet n - - - - smtpd

-o content\_filter=spamassassin

[…]

Por último, debemos añadir los siguientes parámetros:

**/etc/postfix/master.cf**

[…]

spamassassin unix - n n - - pipe

user=spamd argv=/usr/bin/spamc -f -e /usr/sbin/sendmail -oi -f ${sender} ${recipient}

Es necesario iniciar SpamAssassin y reiniciar Postfix para comenzar a verificar el spam de los correos electrónicos.

service spamassassin start && service postfix restart

### **Mover el spam a la carpeta Junk automáticamente**

Esto es realmente parte de algo más grande, a saber, un sistema de filtrado de correo. Usando filtros (también conocidos como reglas) puede aplicar acciones al correo utilizando la lógica, por ejemplo, mover el correo etiquetado como spam a la carpeta Junk.

Dovecot tiene un plugin llamado Sieve que maneja reglas. Sieve es en realidad un lenguaje de programación diseñado para reglas de filtrado de correo.

Para instalar las librerías necesarias para que Dovecot pueda utilizar Sieve, usaremos el siguiente comando:

apt-get install dovecot-sieve dovecot-managesieved

A continuación, configuraremos dovecot para que utilice el plugin:

**/etc/dovecot/conf.d/15-lda.conf**

[…]

protocol lda {

mail\_plugins = $mail\_plugins sieve

}

[…]

en

**/etc/dovecot/conf.d/20-lmtp.conf**

[…]

protocol lmtp {

# Space separated list of plugins to load (default is global mail\_plugins).

mail\_plugins = $mail\_plugins sieve

postmaster\_address = admin@example.com

}

[…]

Es una buena idea tener una dirección de correo local para evitar los bucles de correo. También es requerido por el smtp rfc (aunque técnicamente no estamos usando smtp sino lmtp aquí - aún así es una buena idea).

Ahora configuraremos Dovecot para que utilice el script de Sieve:

**/etc/dovecot/conf.d/90-sieve.conf**

[…]

plugin {

sieve = ~/.dovecot.sieve

sieve\_dir = ~/sieve

}

[…]

Estableceremos una regla global de spam que moverá el spam a la carpeta Junk del usuario de forma automática.

**/etc/dovecot/conf.d/90-sieve.conf**

[…]

sieve\_after = /etc/dovecot/sieve/spamfilter.sieve

[…]

¿Por qué sieve\_after? Si hubiera utilizado sieve\_before entonces cualquier regla aplicable (a ese correo en particular) el usuario no se habría ejecutado. Usando sieve\_after las reglas del usuario se ejecutan primero para que puedan anular las reglas sieve\_after.

Debemos abrir los puertos para que Sieve trabaje adecuadamente

**/etc/dovecot/conf.d/20-managesieve.conf**

[…]

protocols = $protocols sieve

service managesieve-login {

inet\_listener sieve {

port = 4190

}

}

[…]

Para que Dovecot pueda filtrar los correos en conjunto con Sieve, necesitamos crear un script que reconozca las cabeceras de los correos que contengan spam

Creamos el siguiente directorio

mkdir /etc/dovecot/sieve

Y dentro de éste, creamos creamos el archivo **spamfilter.sieve**e introducimos lo siguiente

nano /etc/dovecot/sieve/spamfilter.sieve

**/etc/dovecot/sieve/spamfilter.sieve**

require ["fileinto", "mailbox"];

if header :contains "X-Spam-Flag" "YES" {

fileinto :create "Spam";

}

Y finalmente reiniciamos Dovecot

service dovecot restart

Para comprobar que Sieve está funcionando correctamente, podemos enviar un correo desde nuestro cliente preferido que contenga en el cuerpo los siguiente:

XJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL\*C.34X

Lo anterior se conoce como GTUBE - Generic Test for Unsolicited Bulk Email y sirve como prueba para comprobar que el filtro de spam del servidor de correos funciona correctamente.

**¡Felicitaciones!** Usted ha configurado con éxito su servidor de correo con Postfix y Dovecot con autenticación MySQL y filtrado de spam con SpamAssassin!

### **Borrar automáticamente spam después de 30 días**

Usando doveadm podemos borrar automáticamente todo el correo de la carpeta Spam que tenga más de un cierto tiempo, por ejemplo 30 días.

Doveadm es la utilidad de administración de Dovecot. Lee man doveadm para más información sobre doveadm. Otra lectura relevante para este caso: man doveadm-search y man doveadm-search-query.

Supongamos que desea buscar todos los documentos en todas las bandejas de entrada con más de cuatro horas de antigüedad:

sudo doveadm search -A mailbox Inbox savedbefore 4h

**Output**  
 admin@example.com 74b4db2757f9f05661350000595b2a1f 1

admin@example.com 74b4db2757f9f05661350000595b2a1f 2

**-A** significa buscar en todos los buzones de correo, no sólo en el que especificamos. ¿Recuerdas la consulta de iteración? Esto es para lo que sirve. Si hubiera estado usando una consulta de usuario estática en **/etc/dovecot/dovecot-sql.conf.ext** entonces la búsqueda de doveadm **-A** habría arrojado un error.

Sin embargo, no queremos buscar en la Bandeja de entrada y queremos correos con más de 30 días de antigüedad:

sudo doveadm search -A mailbox Spam savedbefore 30

**Nota:** Para saber más del formato de búsqueda utilice: man doveadm-search-query

No sólo queremos buscar, sino también borrar los mensajes. (Utilice la búsqueda primero para verificar que obtiene los resultados que esperaba.)

sudo doveadm expunge -A mailbox Spam savedbefore 30d

No querrá que ejecutar esto manualmente todos los días. Vamos a programarlo:

sudo crontab -e

y agregue la siguiente línea:

@daily /usr/bin/doveadm expunge -A mailbox Junk savedbefore 30d > /dev/null 2>&1

**@daily** hará que el comando se ejecute automáticamente una vez cada 24 horas, mientras que **/dev/null 2>&1** evitará que se le notifique por correo la ejecución del comando

## **Configurar ClamAV**

ClamAV es una herramienta antivirus de código abierto. Viene con Freshclam, que se encarga de las actualizaciones de definición. Clamsmtp es la parte que permite a Clam escanear el tráfico smtp.

Para poder instalarlo utilizaremos la siguiente línea de comandos

sudo apt-get install clamav clamav-freshclam clamsmtp clamav-daemon

Hay que darle los permisos a las carpetas con los siguientes comandos

sudo chown -R clamav. /var/spool/clamsmtp  
 sudo chown -R clamav. /var/run/clamsmtp

Ahora vamos a modificar el archivo **clamsmptd.conf** usando el editor nano

sudo nano /etc/clamsmtpd.conf

Agregando o modificando las siguientes líneas:

**/etc/clamsmtpd.conf**

[…]

OutAddress: 10025

Listen: 127.0.0.1:10026

Header: X-AV-Checked: ClamAV using ClamSMTP

User:clamav

[...]

Guardamos y salimos del editor, para posteriormente reiniciar el servicio de clamAV usando la siguiente instrucción.

sudo service clamsmtp restart

Vamos añadir clamav a postfix modificando el archivo de configuración de este utilizando la siguiente instrucción.

sudo nano /etc/postfix/main.cf

Y agregaremos las siguientes líneas:

**/etc/postfix/main.cf**

[…]

content\_filter = scan:127.0.0.1:10026

receive\_override\_options = no\_address\_mappings

[...]

Así mismo modificaremos el archivo “master.cf” utilizando la siguiente instrucción y las líneas que se presentan:

sudo nano /etc/postfix/master.cf

**/etc/postfix/master.cf**

[…]

# Antivirus

scan unix - - n - 16 smtp

-o smtp\_send\_xforward\_command=yes

# For injecting mail back into postfix from the filter

127.0.0.1:10025 inet n - n - 16 smtpd

-o content\_filter=

-o receive\_override\_options=no\_unknown\_recipient\_checks,no\_header\_body\_checks

-o smtpd\_helo\_restrictions=

-o smtpd\_client\_restrictions=

-o smtpd\_sender\_restrictions=

-o smtpd\_recipient\_restrictions=permit\_mynetworks,reject

-o mynetworks\_style=host

-o smtpd\_authorized\_xforward\_hosts=127.0.0.0/8

Reiniciamos los servicios de postfix y clamsmtp con las siguientes instrucciones

sudo postfix reload && sudo service clamav-daemon start

Vamos actualizar las firmas de los cambios que hemos realizado utilizando las siguientes instrucciones.

Para esto debemos modificar la línea de **DatabaseMirror** en el siguiente archivo, de la siguiente manera:

**/etc/clamav/freshclam.conf**

[…]

DatabaseMirror db.XX.clamav.net

[…]

Cambie **XX** a su código de país (NL para los Países Bajos, MX para México, etc.).

sudo service clamav-daemon start

**Nota:** No se olvide de volver a inicializar el demonio de “refresh” ya que esto nos permite tener conocimiento de los errores y archivos que se han bloqueado.

sudo systemctl start clamav-freshclam.service

Si se detecta un virus **/var/log/clamav/clamav.log** mostrará algo como:

**/etc/clamav/freshclam.conf**

[…]

Tue Mar 22 15:27:47 2016 -> /var/spool/clamsmtp/clamsmtpd.N3lkUG: Eicar-Test-Signature(c88982d8fd9fe8013389c4f801a237b6:851) FOUND

sudo /var/log/mail.log | grep -i clam

**/var/log/mail.log**

[…]

from=vorkbaard@example.com, to=tinus@example.com, status=VIRUS:Eicar-Test-Signature

## **Instalar RoundCube**

### **Paso 1: Instalación de dependencias**

El primer paso para configurar Roundcube es instalar sus dependencias y configurar PHP. Una vez instalado Roundcube, podemos usar su útil página de comprobación de dependencias para verificar que todo está configurado correctamente.

Estas son las dependencias de Roundcube que no se incluyen con la aplicación:

* Varias librerías PHP (que son los paquetes php-\* de abajo, incluyendo soporte para XML y cadenas multi-byte)
* Herramientas de soporte (zip y unzip para manejar archivos comprimidos)
* Git para el control de versiones
* El sistema de gestión de plugins PHP (composer)

Actualice su índice de paquetes e instale todas estas dependencias a la vez.

sudo apt-get update

sudo apt-get install php-xml php-mbstring php-intl php-zip php-pear zip unzip git composer

A continuación, algunas de las bibliotecas PHP deben estar habilitadas en el archivo php.ini del servidor, que se encuentra en /etc/php/**7.2**/apache2/php.ini. Abra este archivo con nano o su editor de texto favorito.

sudo nano /etc/php/7.2/apache2/php.ini

Muchos de los cambios necesarios son sólo la habilitación de opciones que han sido comentadas. En los archivos php.ini, las líneas comentadas comienzan con un punto y coma (en lugar del símbolo # hash más común). Para descomentar una línea, borre este punto y coma principal; para comentar una línea, añada un punto y coma principal.

Busque la sección que contiene muchas líneas comentadas que comienzan con extension=. Descomente las líneas de las extensiones php\_mbstring.dll y php\_xmlrpc.dll.

**/etc/php/7.2/apache2/php.ini**

[…]

;extension=php\_ldap.dll

extension=php\_mbstring.dll

;extension=php\_exif.dll ; Must be after mbstring as it depends on it

;extension=php\_mysqli.dll

. . .

extension=pdo\_mysql

. . .

;extension=php\_sqlite3.dll

;extension=php\_tidy.dll

extension=php\_xmlrpc.dll

;extension=php\_xsl.dll

[…]

Luego agregue extension=dom.so a la parte inferior del bloque de extensión.

**/etc/php/7.2/apache2/php.ini**

[…]

extension=php\_xmlrpc.dll

;extension=php\_xsl.dll

extension=dom.so

[…]

Hay algunas otras modificaciones que necesitamos hacer en este archivo.

Primero, busque la configuración date.timezone. Descomente la línea y añada su zona horaria entre comillas. Para ver cómo formatear su zona horaria en el archivo php.ini, puede consultar la página de zona horaria de PHP (http://www.php.net/manual/en/timezones.php). Por ejemplo, si usted vive en Eastern Standard Time, su archivo podría verse así:

**/etc/php/7.2/apache2/php.ini**

[…]

[Date]

; Defines the default timezone used by the date functions

; http://php.net/date.timezone

date.timezone = "America/New\_York"

[…]

A continuación, busque la configuración upload\_max\_filesize. Esta configuración afecta principalmente a la carga de archivos adjuntos. De forma predeterminada, está configurado en 2 MB. Puede establecer la cantidad que desee, pero la mayoría de los servidores de correo electrónico limitan el tamaño total de los archivos adjuntos a 10 MB. Lo pondremos a 12MB aquí en el caso de que varios usuarios estén añadiendo archivos adjuntos al mismo tiempo.

**/etc/php/7.2/apache2/php.ini**

[…]

; Maximum allowed size for uploaded files.

; http://php.net/upload-max-filesize

upload\_max\_filesize = 12M

[…]

A continuación, busque post\_max\_size. Mientras que la configuración upload\_max\_filesize se aplica sólo a los archivos adjuntos, esta configuración se aplica al tamaño de todo el correo electrónico (incluidos los archivos adjuntos). Para evitar bloqueos, lo pondremos en un valor ligeramente superior.

**/etc/php/7.2/apache2/php.ini**

[…]

; Maximum size of POST data that PHP will accept.

; Its value may be 0 to disable the limit. It is ignored if POST data reading

; is disabled through enable\_post\_data\_reading.

; http://php.net/post-max-size

post\_max\_size = 18M

[…]

Finalmente, busque mbstring.func\_overload, descoméntelo y verifique que su valor sea 0. Esto permite soportar funciones de cadenas de varios bytes.

**/etc/php/7.2/apache2/php.ini**

[…]

mbstring.func\_overload = 0

[…]

Guarde y cierre el archivo.

Su servidor está ahora configurado con una pila LAMP, las dependencias de Roundcube y la configuración necesaria de PHP. El siguiente paso es descargar el software Roundcube, instalarlo y configurarlo.

### **Paso 2 - Descargar Roundcube**

Como con muchos proyectos en el mundo Linux, hay dos maneras de instalar Roundcube: desde un paquete o desde el código fuente. Existe un PPA para Roundcube, pero debido a que el proyecto está en desarrollo activo, el PPA a menudo está desactualizado. (En el momento de redactar este documento, el PPA está en la versión 1.2.3, pero el proyecto en sí está en la 1.3). Para asegurarnos de que estamos obteniendo la versión más reciente, instalaremos desde el código fuente.

Vaya a la página de descarga de Roundcube (**https://roundcube.net/download/**). Busque en la sección **Versión estable** y localice el paquete **completo**. Haga clic con el botón derecho del ratón en el botón **Descargar** y seleccione **Copiar dirección de enlace**.

Utilice esta dirección con **wget** para descargar el tarball de Roundcube en el servidor.

wget https://github.com/roundcube/roundcubemail/releases/download/1.3.8/roundcubemail-1.3.8-complete.tar.gz

Descomprimir el archivo Roundcube.

tar -xvzf roundcubemail-1.3.8-complete.tar.gz

Los argumentos de tar pueden ser un poco intimidantes, así que esto es lo que hace cada bandera:

* La bandera x significa extracto.
* La bandera v significa verboso, que le dice a tar que imprima la ruta y el nombre de cada archivo extraído.
* La bandera z le dice a tar que no sólo quite la envoltura de tar sino que descomprima el archivo usando gzip. Sabemos que el archivo está comprimido con gzip porque la extensión de archivo tiene .gz en el extremo.
* La bandera f significa archivo. Esta debe ser la última bandera porque tar utiliza lo que le sigue inmediatamente como el archivo que se va a extraer.

A continuación, mueva el directorio descomprimido a /var/www y renómbrelo a roundcube. Asegúrese de omitir el arrastre / en los nombres de los directorios porque queremos mover y renombrar todo el directorio, no los contenidos del directorio.

sudo mv roundcubemail-1.3.8 /var/www/roundcube

Finalmente, cambie los permisos para permitir que Apache cree y edite los archivos (como los archivos de configuración y los registros). Específicamente, cambie el propietario y el grupo a **www-data**, y cambie los permisos de lectura y escritura para el propietario y el grupo, pero lea sólo para los demás.

sudo chown -R www-data:www-data /var/www/roundcube/

sudo chmod 775 /var/www/roundcube/temp/ /var/www/roundcube/logs/

Hemos descargado el código de Roundcube y actualizado su ubicación y permisos, pero sólo está instalado parcialmente en este momento. Para terminar la instalación, necesitamos conectar Roundcube a nuestra base de datos a través del GUI de Roundcube. Antes de que podamos hacer eso, necesitamos decirle a Apache dónde está Roundcube para que pueda cargar el sitio web.

### **Paso 3 — Configurando Apache**

El archivo que necesitamos editar para configurar Apache es un archivo de host virtual. Los hosts virtuales son una característica que permite a Apache alojar múltiples sitios en el mismo servidor. Incluso si este es el único sitio que Apache está alojando, es más simple y limpio usar un archivo de configuración de host virtual que editar la configuración principal de Apache.

Cada archivo .conf ubicado en /etc/apache2/sites-available/ representa un sitio diferente. Aquí crearemos un archivo de host virtual para Roundcube, y luego se lo diremos a Apache para que pueda estar disponible a través de un navegador.

Primero, copie el archivo de configuración predeterminado para utilizarlo como punto de partida para el nuevo archivo.

sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/roundcube.conf

Abra el archivo con su editor de texto.

sudo nano /etc/apache2/sites-available/roundcube.conf

Tendremos que hacer algunos cambios en este archivo. Primero pasaremos por cada uno de ellos y luego le proporcionaremos el archivo completo para que lo copie y pegue.

En el bloque VirtualHost existente, modificará las siguientes directivas:

* El ServerName le dice a Apache qué dominio escuchar. Esta debe ser la dirección IP de su servidor o el nombre de dominio, si está utilizando uno.
* DocumentRoot especifica dónde enviar tráfico cuando llega. En nuestro caso, debemos enviarlo a Roundcube en /var/www/roundcube.
* ServerAdmin le permite especificar una dirección de correo electrónico de contacto para cualquier problema con Apache. No estamos configurando Apache para que lo haga en este tutorial, pero es una buena práctica incluirlo de todos modos.
* Las dos líneas de registro, ErrorLog y CustomLog, definen dónde guardar los registros de conexión y los registros de errores de este sitio. Necesitamos dar nombres específicos a los registros de errores para que, si hay algún problema, los registros específicos de este sitio se encuentren fácilmente.

Luego, agregará un nuevo bloque Directory que le dirá a Apache qué hacer con el directorio Roundcube. La primera palabra en cada línea de un bloque Directory es el nombre de la configuración seguido de las opciones de configuración reales.

* **Options -Indexes** le dice a Apache que muestre una advertencia si no puede encontrar un archivo index.html o index.php. Por defecto, en su lugar, mostrará el contenido del directorio.
* **AllowOverride All** le dice a Apache que si se encuentra un archivo .htaccess local, cualquier opción en ese archivo anula la configuración global de ese archivo.
* **Order allow,deny** le dice a Apache primero que permita a los clientes que coincidan el acceso al sitio, y luego que rechace los que no coincidan.
* **allow from all** es un seguimiento a la línea de la Orden. Define qué tipo de cliente está permitido, que es cualquiera en nuestro caso.

A continuación se muestra el aspecto que tendrá el archivo una vez que haya realizado estos cambios. Por razones de brevedad, se han eliminado los comentarios.

**/etc/apache2/sites-available/roundcube.conf**

<VirtualHost \*:80>

ServerName your\_server\_ip\_or\_domain

DocumentRoot /var/www/roundcube

ServerAdmin sammy@example.com

ErrorLog ${APACHE\_LOG\_DIR}/roundcube-error.log

CustomLog ${APACHE\_LOG\_DIR}/roundcube-access.log combined

<Directory /var/www/roundcube>

Options -Indexes

AllowOverride All

Order allow,deny

allow from all

</Directory>

</VirtualHost>

Guarde y cierre el archivo.

A continuación, dígale a Apache que deje de alojar el sitio por defecto.

sudo a2dissite 000-default

Entonces dígale a Apache que empiece a alojar el sitio Roundcube. Asegúrese de no incluir el archivo .conf cuando habilite el sitio; a2ensite requiere el nombre de archivo de la configuración sin la extensión.

sudo a2ensite roundcube

Habilite el módulo mod\_rewrite de Apache, que requiere Roundcube.

sudo a2enmod rewrite

Finalmente, reinicie Apache, lo que hará que la instalación de Roundcube sea accesible.

sudo apache2ctl restart

El cliente de webmail está casi listo para usar. El último paso del proceso de instalación es configurar la base de datos para que Roundcube pueda almacenar sus datos específicos de la aplicación.

### **Paso 4 — Configurando MySQL**

En este punto, si abre un navegador web e intenta acceder a su servidor (por dirección IP o nombre de dominio, si está utilizando uno), verá una página de error de configuración. Esto se debe a que Roundcube está buscando un archivo generado durante la configuración, pero aún no hemos pasado por la configuración. Antes de que podamos pasar por esa configuración, necesitamos preparar la base de datos.

Conéctese al shell interactivo de MySQL. Este comando le dice a MySQL que se autentique como usuario (-u) **root** y que especificaremos una contraseña (-p).

mysql -u root -p

Después de introducir el comando se le pedirá la contraseña de root que creó cuando instaló MySQL.

Ahora que estamos en el shell de MySQL, crearemos una base de datos y un usuario de base de datos, y luego daremos a ese usuario permisos para ejecutar comandos en esa nueva base de datos.

Cree primero la base de datos. Este comando crea una base de datos llamada roundcubemail y luego proporciona opciones de base de datos, como el juego de caracteres a usar (utf8).

CREATE DATABASE roundcubemail /\*!40101 CHARACTER SET utf8 COLLATE utf8\_general\_ci \*/;

A diferencia de muchos otros sistemas de autenticación, MySQL define a un usuario por un nombre y desde dónde se conectará. Este comando crea un usuario llamado **roundcube** y define a ese usuario para conectarse desde localhost. En el caso de las aplicaciones que acceden a una base de datos, la definición del lugar desde el que el usuario va a realizar la solicitud ayuda a reforzar la seguridad.

Cree este usuario, asegurándose de cambiar la contraseña a algo seguro.

CREATE USER 'roundcube'@'localhost' IDENTIFIED BY '**password**';

Dar al usuario de **roundcube** todos los permisos de la base de datos de roundcubemail y de todas sus tablas.

GRANT ALL PRIVILEGES ON roundcubemail.\* to 'roundcube'@'localhost';

Luego guarde los cambios y salga del shell interactivo de MySQL.

FLUSH PRIVILEGES;

EXIT;

Hemos creado una base de datos en blanco, roundcubemail, y un usuario, roundcube@localhost, y luego le hemos dado a ese usuario permisos completos para la base de datos. Ahora necesitamos configurar la estructura de la base de datos para que Roundcube sepa dónde guardar su información. La instalación de Roundcube proporciona un archivo que configurará la base de datos para nosotros, así que no tenemos que hacerlo a mano.

El siguiente comando le dice a MySQL que use nuestro usuario recién creado para leer en un archivo /var/www/roundcube/SQL/mysql.initial.sql y aplicar la configuración a la base de datos roundcubemail.

mysql -u roundcube -p roundcubemail < /var/www/roundcube/SQL/mysql.initial.sql

Se te pedirá que introduzcas la contraseña del usuario de **roundcube**.

Configurar la base de datos de esta manera la prepara para el uso de Roundcube y también nos permite verificar que tenemos los permisos correctos. Si todo fue un éxito, no recibirá ninguna respuesta y volverá a la línea de comandos. Entonces estamos listos para decirle a Roundcube nuestra configuración de correo electrónico y finalizar la instalación.

### **Paso 5 — Configurando Roundcube**

Como se mencionó anteriormente, si intentas acceder a tu instalación de Roundcube ahora, obtendrás una página de error. Para terminar la instalación, necesitamos visitar **http://your\_server\_ip\_or\_domain/installer**.

Si todo está configurado correctamente, habrá un **OK** verde a la derecha de cada elemento de línea, excepto por algunos pocos: la configuración opcional de LDAP y cada línea de base de datos excepto MySQL. Si hay una **NO DISPONIBLE** junto a cualquier otra línea que no sea la mencionada, deberá instalar esas dependencias. Roundcube proporciona un enlace útil para cualquier dependencia que falte, de modo que pueda saber qué instalar.

Una vez que todo esté configurado correctamente, desplácese hacia abajo hasta la parte inferior de la página y haga clic en el botón **SIGUIENTE**.

El formulario de la página siguiente, que está dividido en siete secciones, pasa por la generación del archivo de configuración Roundcube. Abajo están las porciones del formulario que necesitamos llenar, divididas por sección. Si se excluye una línea del formulario en las secciones siguientes, puede saltarse esa línea y dejarla con la configuración predeterminada.

#### **Configuración general**

La sección Configuración general proporciona algunas opciones cosméticas para la personalización y algunas opciones generales para la configuración.

* Asegúrese de que **ip\_check** esté marcado para mayor seguridad. Comprueba la autorización de la IP del cliente durante la sesión.

Hay algunos otros cambios opcionales que también puede hacer:

* Puede cambiar el **product\_name**. Puede ser cualquier cosa que desee y todas las referencias a "Roundcube" en el texto se sustituirán por este nombre.
* El **support\_url** es una URL donde los usuarios pueden obtener soporte para su instalación de Roundcube. No es estrictamente necesario, pero puede ser bueno que Roundcube se proporcione a un grupo de personas que puedan necesitar ayuda. Si no tiene un sitio de ayuda dedicado, puede utilizar una dirección de correo electrónico, como mailto:sammy@example.com.
* Puede reemplazar el logotipo de Roundcube por **skin\_logo**, que lleva una URL a un archivo PNG (178px por 47px). Si va a habilitar HTTPS (muy recomendable, y que se explica más adelante en este tutorial), asegúrese de que la URL de la imagen sea una URL HTTPS.

Todas las demás opciones pueden dejarse en sus valores predeterminados.

#### **Registro y depuración**

Deje todo en esta sección en su configuración predeterminada.

#### **Configuración de la base de datos**

Roundcube utiliza MySQL para almacenar la información para ejecutar el cliente web (no sus correos electrónicos). En esta sección, debes indicarle a Roundcube cómo acceder a la base de datos que configuraste en el paso 4. Necesitará el usuario de la base de datos, la contraseña de usuario y el nombre de la base de datos que creó anteriormente.

* Ya debería estar configurado, pero seleccione MySQL en el menú desplegable **Tipo de base de datos**.
* Introduzca localhost para el **servidor de base de datos**.
* Introduzca el nombre de la base de datos, roundcubemail, en el campo **Nombre de la base de datos**.
* Introduzca el usuario de la base de datos, roundcube, en el campo **Nombre de usuario de la base de datos**.
* Para el campo **Contraseña de base de datos**, introduzca la contraseña que definió al crear la base de datos en el paso 4.
* La última opción, **db\_prefix**, no es necesaria a menos que esté usando una base de datos compartida con otras aplicaciones. Si es así, introduzca algo como, rc\_.

#### **Configuración IMAP**

Para esta sección, necesitará la configuración de IMAP y SMTP para su servidor de correo electrónico. Debido a que este tutorial utiliza Gmail como ejemplo, la configuración de Gmail se incluye a continuación, pero si tienes tu propio proveedor de correo electrónico, debería proporcionarte los detalles que necesitas, principalmente sustituyendo la url de **Gmail** por **localhost**. La mayoría de los proveedores de correo electrónico admiten conexiones con o sin cifrado. Asegúrese de evitar el uso de conexiones no seguras utilizando las direcciones URL y los puertos SSL IMAP/SMTP.

* En el campo **default\_host** introduzca la URL del servidor IMAP. Cuando utilice conexiones SSL, prefija la URL con ssl:// en lugar de https://. Para Gmail, introduce ssl://imap.gmail.com.

1. A continuación se configura el **default\_port**, que es el puerto del servidor IMAP. Las conexiones SSL y no SSL utilizarán puertos diferentes, así que asegúrese de utilizar el puerto SSL. El puerto SSL IMAP de Gmail utiliza 993.
2. El campo **username\_domain** es una opción conveniente para los proveedores de correo electrónico que utilizan una dirección de correo electrónico completa como nombre de usuario. Este campo es opcional. Ingresar un dominio - no el correo electrónico completo - le permitirá ingresar a Roundcube sólo con su nombre, antes de la @, en lugar del correo electrónico completo. Por ejemplo, si introduce gmail.com en el campo, user@gmail.com podrá iniciar sesión en Roundcube con el usuario.
3. Asegúrese de que la casilla de verificación **auto\_create\_user** está activada. Si no está marcada, Roundcube no creará un usuario en su propia base de datos, lo que le impedirá iniciar sesión.
4. Por ahora, deje todos los campos **\*\_mbox**, como **sent\_mbox**, con sus valores por defecto. Esto se puede actualizar más tarde en la interfaz de Roundcube, y la mayoría de los clientes de correo electrónico utilizan estos nombres de carpeta de todos modos.

#### **Configuración SMTP**

El servidor SMTP es la parte del correo electrónico que envía correos electrónicos. Al igual que en la sección del servidor IMAP, utilizaremos la URL y el puerto SSL, y Gmail como referencia.

1. Introduzca la dirección del servidor **SMTP** en el campo smtp\_server. El servidor SMTP de Gmail es ssl://smtp.gmail.com.
2. Introduzca el puerto del servidor SMTP SSL en el campo **smtp\_port**. El puerto SSL de Gmail es 465.
3. Dado que SMTP e IMAP son dos servicios separados, ambos necesitan un nombre de usuario y una contraseña. Roundcube nos da la opción de usar el nombre de usuario y la contraseña de IMAP configurados anteriormente para que no tengamos que configurarlo de nuevo aquí. Esto significa que debe dejar los campos en **smtp\_user/smtp\_pass** en blanco y marcar la casilla situada junto a **Usar el nombre de usuario y la contraseña IMAP actuales para la autenticación SMTP**.
4. Por último, asegúrese de que la casilla de verificación para **smtp\_log** está marcada.

**Nota:** Si obtiene algún error de falla de autenticación con el servidor SMTP postfix, vaya al archivo **/var/www/roundcube/config/config.inc.php** y edite los siguiente campos para que queden así:

$config['smtp\_user'] = '';

$config['smtp\_pass'] = '';

#### **Configuración de pantalla y preferencias de usuario**

Dejaremos todas estas opciones con sus valores por defecto. Si desea personalizar su instalación de Roundcube para que esté en un idioma diferente al del sistema operativo en el que se está ejecutando, configúrelo manualmente haciendo clic en el enlace **RFC1766** en la página de configuración y actualizando el campo de **idioma**.

#### **Plugins**

El soporte para plugins de Roundcube es lo que realmente hace que este cliente de webmail destaque. A continuación se muestra un buen conjunto de valores predeterminados que puede instalar. Todos los plugins son opcionales, es decir, no son necesarios para usar Roundcube, pero la siguiente lista es un buen conjunto para hacer la experiencia más fácil o más segura.

Echa un vistazo a las descripciones de cada plugin e instala el que quieras. Si no seleccionas un plugin aquí, siempre puedes instalarlo más tarde. Esto preconfigura Roundcube con estos plugins.

* **archivo:** Te ofrece un botón Archivo, similar al funcionamiento de Gmail.
* **emoticonos:** Simplemente facilita el uso de emoticonos en los correos electrónicos.
* **enigma:** Permite el cifrado de correo electrónico GPG. Vamos a entrar en detalles sobre cómo configurar esto en nuestro tutorial de seguridad Roundcube.
* **archivos\_adjuntos\_del\_sistema\_de\_ficheros:** Un plugin central que permite guardar archivos adjuntos en el servidor Roundcube temporalmente al componer o guardar un correo electrónico borrador.
* **hide\_blockquote:** Oculta la parte citada de los mensajes de correo electrónico respondidos para mantener la interfaz de usuario más limpia.
* **identidad\_seleccionar:** Si tienes varias direcciones de correo electrónico (identidades), te permite seleccionarlas fácilmente mientras escribes un correo electrónico.
* **markasjunk:** Permite marcar un correo electrónico como spam y moverlo a la carpeta Spam.
* **newmail\_notifier:** Utiliza el sistema de notificación de su navegador para avisarle de nuevos correos electrónicos.

Por fin, esa es toda la configuración. Pulse el botón **UPDATE CONFIG** en la parte inferior de la página para guardar su configuración. Vamos a probar que todo funciona a continuación.

### **Paso 6 - Prueba de la configuración de Roundcube**

Después de actualizar la configuración, la página se actualizará y verá un cuadro de información amarillo en la parte superior de la página que dice **El archivo de configuración se guardó correctamente en el directorio RCMAIL\_CONFIG\_DIR de su instalación Roundcube.**

Desde aquí, haga clic en el botón **CONTINUAR** para probar su configuración. Al igual que en la página de comprobación de la dependencia, si no hay errores, verá un marcador verde de **OK** en cada línea. Si no es así, vuelva y compruebe lo que ha introducido.

Para probar el resto de la configuración, introduzca su nombre de usuario y contraseña IMAP y SMTP en las secciones **Probar configuración SMTP** y **Probar configuración IMAP** y, a continuación, haga clic en **Enviar correo electrónico de prueba** y **Comprobar inicio de sesión**, respectivamente. Si una prueba tiene éxito, la página se recargará y verás el símbolo verde 'OK' bajo la sección que has probado.

**Nota:** Si utilizas Gmail y tienes habilitada la autenticación de dos pasos, deberás generar una contraseña específica de la aplicación (https://support.google.com/accounts/answer/185833?hl=en) porque Roundcube no sabe cómo solicitar tu token de autenticación de dos pasos.

Una vez que haya comprobado las conexiones SMTP e IMAP y ambas estén en verde, es hora de volver a la sesión SSH y eliminar el directorio del instalador. Esto evitará que otra persona genere una nueva configuración y anulará los ajustes correctos.

sudo rm -rf /var/www/roundcube/installer/

Ahora puede visitar su instancia Roundcube utilizando la IP de su servidor o su nombre de dominio, iniciar sesión y comprobar su correo electrónico.

### **Conclusión**

Con Roundcube, usted puede tener el conjunto de características y la apariencia de un cliente de escritorio nativo con la flexibilidad de un cliente de correo web. Ahora tiene una instalación totalmente funcional, pero hay algunos pasos adicionales que debe seguir para asegurarse de que está completamente seguro (cómo añadir soporte HTTPS y usar encriptación GPG para su correo electrónico). Puede hacerlo siguiendo el procedimiento de seguridad de Roundcube en Ubuntu 16.04

(https://www.digitalocean.com/community/tutorials/how-to-secure-roundcube-on-ubuntu-16-04).

Además, puede instalar nuevos temas para mejorar el aspecto de su cliente y plugins para añadir nuevas funcionalidades. A diferencia de los plugins, no hay un sitio central para encontrar temas, pero puedes encontrar Skins de Roundcube o foros de Roundcube como lugares para encontrar algunos.

## **Cuotas**

La cuota de almacenamiento de correo se define en **/etc/dovecot/conf.d/90-quota.conf**:

**/etc/dovecot/conf.d/90-quota.conf**

plugin {

quota\_rule = \*:storage=50M

quota\_rule2 = Trash:storage=+10M

quota\_grace = 10%%

quota\_status\_overquota = "552 5.2.2 Mailbox is full"

quota\_max\_mail\_size = 8M

quota\_status\_success = DUNNO

quota\_status\_nouser = DUNNO

quota\_status\_overquota = "552 5.2.2 Mailbox is full"

}

##

## Quota backends

##

plugin {

quota = maildir:User quota

}

service quota-status {

executable = quota-status -p postfix

inet\_listener {

port = 12340

# You can choose any port you want

}

client\_limit = 1

}

**/etc/dovecot/conf.d/10-mail.conf**

[...]

mail\_plugins = $mail\_plugins quota

[...]

**/etc/dovecot/conf.d/20-imap.conf**

[...]

mail\_plugins = $mail\_plugins imap\_quota

[...]

Reinicie Dovecot

sudo dovecot reload

# **Servidor de monitoreo - Monit**

### Introducción

Monit es una pequeña utilidad de código abierto que se ha desarrollado para administrar y monitorear los sistemas Unix. Al utilizar la aplicación Monit, es responsable de llevar a cabo el mantenimiento y la reparación automática de los procesos fallidos y tiene la capacidad de ejecutar acciones de administración en situaciones de error para mantener la operatividad del sistema operativo.

### Instalación.

Para la instalación y configuración revisamos el manual de la página principal de Monit.[23]

Ejecutamos el siguiente comando

sudo apt-get install monit

Para habilitar Monit en el inicio ejecutar la siguiente línea

sudo systemctl enable monit

Algunas otras opciones para controlar Monit son:

* Consulta el estado de Monit

sudo systemctl status monit

* Detener el servicio de Monit.

sudo systemctl stop monit

* Reinicie el servicio de Monit.

sudo systemctl restart monit

* Inicia el servicio de Monit.

sudo systemctl start monit

### Configuración

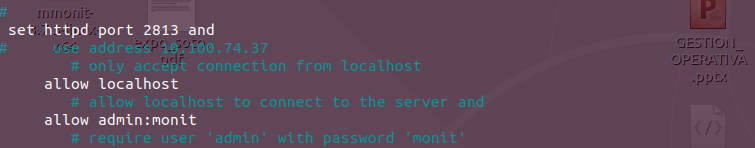
Monit se puede administrar desde dos directorios principales que son:

* Archivo de configuración principal: / etc / monit / monitrc
* Directorios para procesos específicos o archivos de servidor: / etc / monit / conf-available y / etc / monit / conf-enabled /

Accederemos al directorio principal de configuración utilizando cualquiera de los editores deseados

sudo nano /etc/monit/monitrc

Para habilitar la interfaz HTTP integrada a través de la cual puede ver el estado de los servicios monitoreados y administrar los servicios desde una interfaz web, debemos ubicar la siguiente línea “set httpd port 2812 and”



# 

# **Referencias**

[1]. <https://es.wikipedia.org/wiki/Correo_electr%C3%B3nico>

[2]. <https://mx.godaddy.com/blog/enterate-de-6-tipos-de-servidores-de-correo-electronico-y-sus-caracteristicas/>

[3]. <https://www.xatakamovil.com/conectividad/protocolo-smtp-como-se-envian-y-reciben-los-emails-a-traves-de-internet>

[4]. <https://blog.embluemail.com/como-funciona-smtp-pop3-e-imap/>

[5]. <https://blog.dopplerrelay.com/ventajas-de-un-servidor-smtp/>

[6]. <https://clouding.io/kb/imap-y-pop3-diferencias-ventajas-y-desventajas/>

[7]. Ap Solange Mikeliunas. (2012). Administración de Infraestructuras Tecnólogo en Informática. España: Sistemas Operativos.

[8]. <https://es.wikipedia.org/wiki/Postfix>

[9]. <https://es.wikipedia.org/wiki/Dovecot>

[10]. <https://en.wikipedia.org/wiki/Apache_SpamAssassin>

[11]. <https://es.wikipedia.org/wiki/ClamAV>

[12]. <https://es.wikipedia.org/wiki/Cacti>

[13]. <https://es.wikipedia.org/wiki/RRDtool>

[14]. <https://es.wikipedia.org/wiki/Licencia_P%C3%BAblica_IBM>

[15]. <https://es.wikipedia.org/wiki/Licencia_MIT>

[16]. <https://es.wikipedia.org/wiki/Apache_License>

[17]. <https://es.wikipedia.org/wiki/GNU_General_Public_License>

[18]. <https://www.20minutos.es/noticia/8418/0/herramientas/correo/electronico/>

[19]. <https://askubuntu.com/questions/909273/clamav-error-var-log-clamav-freshclam-log-is-locked-by-another-process>

[20]. <https://www.osradar.com/how-to-setup-a-mail-server-on-ubuntu-18-04/>

[21]. <https://computingforgeeks.com/how-to-install-observium-on-ubuntu-18-04-lts-with-nginx/>

[22]<http://www.postfix.org/postconf.5.html#mydestination>

[23]<https://mmonit.com/monit/documentation/monit.html>