

**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**](#_t1qdnxi7zmsk) **2**

[**Introducción**](#_375g4y5agiq0) **4**

[Servidores de salida y entrada.](#_kfi200zewzng) 4

[Funcionamiento.](#_diy5sajfe0ox) 5

[SMTP (Simple Mail Transfer Protocol)](#_bd3qgwkmzjc0) 5

[Pop3 (Post Office Protocol)](#_ud7nehs8g82r) 5

[IMAP (Internet Message Access Protocol)](#_hyrdxfcbkc5w) 5

[Ventajas.](#_bttvsf6wrz75) 6

[SMTP (Simple Mail Transfer Protocol)](#_9li8selato5h) 6

[Pop3 (Post Office Protocol)](#_21c8k7pxprma) 6

[IMAP (Internet Message Access Protocol)](#_ytaorftr05ra) 6

[**Herramientas**](#_8cludv93lsva) **6**

[Instalación y configuración de herramientas.](#_o5657b2ura08) 7

[Requisitos previos](#_sbbs7i5mln5x) 7

[Postfix](#_ujaqeit3nc61) 7

[Ajustar la configuración de Postfix](#_kixy332rgtvv) 9

[Asignación de direcciones de correo a cuentas Linux](#_q0g41a9pfwp8) 10

[Ajustar el Firewall](#_udpaek9lvw1t) 10

[Configuración del entorno para que coincida con la ubicación del correo](#_iti09iyqqrp4) 11

[Dovecot](#_ipkzgunvxgqn) 11

[SpamAssassin](#_qbfpm4efhso1) 12

[ClamAV](#_bzq95z9dcx8g) 14

[**Instalación y configuración de herramientas de usuario.**](#_9iu52x6u7xiq) **16**

[Aplicación web (SquirrelMail) [20]](#_inmr2ocl2vk7) 16

[Configurar el Virtual](#_iqhm71e07cfz) 16

[Configurar SquirrelMail](#_hw6cpal6zb1) 18

[**Servidor de monitoreo (Observium)**](#_1q8vqk5wcg9z) **21**

[Requerimientos](#_ntkqr83lzqd0) 21

[Instalación](#_nqnxqo8rx3wa) 22

[Configuración de SNMP](#_4vdzchmzv0ca) 24

[Configuración del servidor Nginx](#_ns6jeg7dz8jm) 24

[Configurar observium en la interfaz de usuario web](#_nvd9jv62lclu) 25

[**Bibliografía**](#_mnv7haqkfmc7) **27**

# 

# **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.**

* **Simple Mail Transfer Protocol (SMTP)**: 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).

* **Post Office Protocol (Pop3)**: 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).

* **Internet Message Access Protocol (IMAP**): 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 |

## 

## **Instalación y configuración de herramientas.**

**Nota:** La instalación, configuración y pruebas de este manual está implementadas en el sistema operativo Ubuntu 18.04.2

### **Requisitos previos**

Antes de comenzar, debe tener un usuario regular, no root, con privilegios sudo configurados en su servidor.

## **Postfix**

Postfix está incluido en los repositorios por defecto de Ubuntu, por lo que la instalación es increíblemente sencilla.

Para empezar, actualice la caché local del paquete **apt** e instale el software. Pasaremos la variable de entorno **DEBIAN\_PRIORITY=low** a nuestro comando de instalación para responder a algunas preguntas adicionales:

sudo apt-get update

sudo DEBIAN\_PRIORITY=low apt-get install postfix

Utilice la siguiente información para rellenar correctamente las preguntas para su entorno:

* **Configuración general del tipo de correo?** Para ello, elegiremos el **Sitio de Internet** que mejor se adapte a nuestras necesidades de infraestructura.
* **Nombre de correo del sistema:** Este es el dominio base utilizado para construir una dirección de correo electrónico válida cuando sólo se da la parte de la cuenta de la dirección. Por ejemplo, el nombre de host de nuestro servidor es mail.example.com, pero probablemente queramos configurar el nombre de correo del sistema a example.com para que, dado el nombre de usuario1, Postfix utilice la dirección user1@example.com.
* **Destinatario del correo raíz y del correo postal:** Esta es la cuenta de Linux que será reenviada a root@ y postmaster@. Use su cuenta principal para esto. En nuestro caso, **Sammy**.
* **Otros destinos para los que se puede aceptar correo:** Esto define los destinos de correo que aceptará esta instancia de Postfix. Si necesita añadir otros dominios que este servidor se encargará de recibir, añádalos aquí, de lo contrario, el predeterminado debería funcionar bien.
* **Forzar actualizaciones sincrónicas en la cola de correo:** Como es probable que esté utilizando un sistema de archivos con registro en diario, acepte **No** aquí.
* **Redes locales:** Esta es una lista de las redes para las que su servidor de correo está configurado para retransmitir mensajes. El valor predeterminado debería funcionar para la mayoría de los escenarios. Si decide modificarlo, asegúrese de ser muy restrictivo con respecto al rango de red.
* **Límite de tamaño del buzón de correo:** se puede utilizar para limitar el tamaño de los mensajes. Ponerlo en "0" deshabilita cualquier restricción de tamaño.
* **Carácter de extensión de dirección local:** Este es el carácter que se puede utilizar para separar la parte regular de la dirección de una extensión (utilizado para crear alias dinámicos).
* **Protocolos de Internet a utilizar:** Elija si desea restringir la versión IP compatible con Postfix. Escogeremos "todos" para nuestros propósitos.

Para ser explícitos, estos son los ajustes que usaremos para esta guía:

* **Configuración general del tipo de correo?** Sitio de Internet
* **Nombre de correo del sistema:** example.com (no mail.example.com)
* **Destinatario del correo raíz y del correo postal:** sammy
* **Otros destinos para los que se puede aceptar correo:** $myhostname, example.com, mail.example.com, localhost.example.com, localhost
* **¿Forzar actualizaciones sincrónicas en la cola de correo?:** No
* **Redes locales:** 127.0.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
* **Límite de tamaño de buzón:** 0
* **Carácter de extensión de dirección local:** +
* **Protocolos de Internet a utilizar:** todos

Si alguna vez necesita volver para reajustar estos ajustes, puede hacerlo escribiendo:

sudo dpkg-reconfigure postfix

Las preguntas se rellenarán previamente con sus respuestas anteriores.

Cuando haya terminado, ahora podemos hacer un poco más de configuración para configurar nuestro sistema como nos gustaría.

### **Ajustar la configuración de Postfix**

A continuación, podemos ajustar algunas configuraciones que el paquete no nos pidió.

Para empezar, podemos configurar el buzón de correo. Usaremos el formato **Maildir**, que separa los mensajes en archivos individuales que luego se mueven entre directorios según la acción del usuario. La otra opción es el formato mbox (que no trataremos aquí) que almacena todos los mensajes en un solo archivo.

Estableceremos la variable home\_mailbox en Maildir/ que creará una estructura de directorios bajo ese nombre dentro del directorio home del usuario. El comando postconf se puede utilizar para consultar o establecer los ajustes de configuración. Configure home\_mailbox escribiendo:

sudo postconf -e 'home\_mailbox= Maildir/'

A continuación, podemos establecer la ubicación de la tabla virtual\_alias\_maps. Esta tabla asigna cuentas de correo electrónico arbitrarias a cuentas de sistema Linux. Crearemos esta tabla en /etc/postfix/virtual. De nuevo, podemos usar el comando postconf:

sudo postconf -e 'virtual\_alias\_maps= hash:/etc/postfix/virtual'

Su archivo principal “main.cf” contiene una serie de parámetros y directivas que permiten la declaración de permisos, redes permitidas y otras cuestiones que se verán más adelante.

Accederemos al archivo para hacer algunas configuraciones mediante un editor de texto nano con la siguiente línea de código.

sudo nano /etc/postfix/main.cf

Vamos a modificar y agregar las siguientes líneas:

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

[…]

inet\_protocols=ipv4

home\_mailbox=Maildir/

mydestination= \*aquí se agregan los dominios con los cuales estaremos trabajando, separados cada uno por comas\*. Por ejemplo (adminsr.org, redes.com).

mynetworks= \*aquí se agregaran las redes a las cuales tendrán permitido el acceso separados cada uno por comas\*. Por ejemplo (10.100.0.0/8, 192.168.0.0/8).

[...]

### **Asignación de direcciones de correo a cuentas Linux**

A continuación, podemos configurar el archivo de mapas virtuales. Abra el archivo en su editor de texto:

sudo nano /etc/postfix/virtual

La tabla del mapa de alias virtuales utiliza un formato muy simple. A la izquierda, puede listar las direcciones para las que desea aceptar correo electrónico. Después, separado por espacios en blanco, introduzca el usuario de Linux al que desea que se entregue el correo.

Por ejemplo, si desea aceptar correos electrónicos en contact@example.com y admin@example.com y desea que esos correos electrónicos sean enviados al usuario de Sammy Linux, puede configurar su archivo de la siguiente manera:

**/etc/postfix/virtual**

[…]

contact@example.com sammy

admin@example.com sammy

[...]

Una vez que haya asignado todas las direcciones a las cuentas de servidor correspondientes, guarde y cierre el archivo.

Podemos aplicar el mapeo escribiendo:

sudo postmap /etc/postfix/virtual

Reinicie el proceso de Postfix para asegurarse de que se han aplicado todos nuestros cambios:

sudo systemctl restart postfix

Por último solo verificamos el estado del servicio con el comando

sudo systemctl status postfix

**Nota:** Si el status aparece un mensaje de error o inhabilitado, el archivo de configuración no fue debidamente modificado, revisar la sintaxis de las líneas añadidas y/o modificadas.

### **Ajustar el Firewall**

Si está ejecutando el cortafuegos UFW, tal y como se configuró en la guía inicial de configuración del servidor, tendremos que permitir una excepción para Postfix.

Puede permitir conexiones al servicio escribiendo:

sudo ufw allow Postfix

El componente de servidor Postfix está instalado y listo. A continuación, configuraremos un cliente que pueda manejar el correo que Postfix procesará.

### **Configuración del entorno para que coincida con la ubicación del correo**

Antes de instalar un cliente, debemos asegurarnos de que nuestra variable de entorno MAIL está configurada correctamente. El cliente inspeccionará esta variable para averiguar dónde buscar el correo del usuario.

Para que la variable se configure independientemente de cómo acceda a su cuenta (a través de ssh, su, su, su -, sudo, etc.) necesitamos configurar la variable en unas cuantas ubicaciones diferentes. Lo añadiremos a /etc/bash.bashrc y a un fichero dentro de /etc/profile.d para asegurarnos de que cada usuario tiene esta configuración.

Para agregar la variable a estos archivos, escriba:

echo 'export MAIL=~/Maildir' | sudo tee -a /etc/bash.bashrc | sudo tee -a /etc/profile.d/mail.sh

Para leer la variable en su sesión actual, puede obtener el archivo /etc/profile.d/mail.sh:

source /etc/profile.d/mail.sh

## 

## **Dovecot**

Para instalar dovecot para el protocolo POP3 ejecutamos el siguiente comando

sudo apt-get install dovecot-pop3d

Y lo mismo será para el protocolo IMAP

sudo apt-get install dovecot-imapd

Vamos a modificar el archivo de configuración de dovecot “dovecot.conf” agregando las siguientes líneas de código abriremos el archivo con el editor de texto

sudo nano /etc/dovecot/dovecot.conf

e introducimos en cualquier parte del documento:

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

[…]

protocols = pop3 imap

mail\_location=maildir:~/Maildir

[...]

Guardamos el archivo, salimos del editor y reiniciamos y vemos el status con las siguientes líneas

sudo /etc/init.d/dovecot restart  
 sudo /etc/init.d/dovecot status

**Nota:** Si el status aparece un mensaje de error o inhabilitado, el archivo de configuración no fue debidamente modificado, revisar la sintaxis de las líneas añadidas y/o modificadas.

## **SpamAssassin**

Para instalar SpamAssassins ocuparemos la siguiente línea de comando

sudo apt-get install spamassassin

Ahora vamos a crear un grupo para el manejo del spam

sudo groupadd spamd

Ahora vamos a crear un usuario para el manejo del log del grupo “spamd”

sudo useradd -g spamd -s /bin/false -d /var/log/spamassassin spam

Creamos el directorio para el manejo de los log.

sudo mkdir /var/log/spamassassin

Le damos permiso al directorio

sudo chown root:spamd -R /var/log/spamassassin

Modificamos el archivo de configuración

sudo nano /etc/default/spamassassin

Y agregamos o modificamos las siguientes líneas

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

[…]

ENABLE=1

CRON=1

SAHOME=”/var/log/spamassassin/”

OPTIONS=”create-prefs --max-children 5 --username spamd\ -H ${SAHOME} -s ${SAHOME}spamd.log”

Iniciamos el servicio y verificamos el status con las siguientes líneas

sudo service spamassassin start  
 sudo service spamassassin status

Añadiremos spamassassin a postfix de la siguiente manera. Abriremos y cambiaremos la configuración en el archivo “master.cf” con el siguiente comando

sudo nano /etc/postfix/master.cf

En el apartado “smpt inet n - y - - smtpd agregamos la siguiente instrucción

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

[…]

-o content\_filter=spamassassin

[...]

Y al final del archivo agregamos lo siguiente

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

[…]

spamassassin unix - n - - pipe

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

Guardamos los cambios y salimos del editor reiniciamos y verificamos el status del servidor

sudo service postfix restart  
 sudo service postfix status

Editaremos el spamassassin en el Servidor Virtual Privado (VPS) de la siguiente manera

sudo nano /etc/spamassassin/local.cf

Descomentamos la siguiente línea

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

[…]

rewrite\_header Subject \*\*\*\*\*SPAM\*\*\*\*\*

[...]

Y después agregaremos o modificaremos las siguientes tres líneas

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

[…]

required\_score 3.0

use\_bayes 1

bayes\_auto\_learn 1

[...]

Reiniciamos y habilitamos los servicios de postfix y spamassassin con los siguientes comandos

sudo systemctl restart postfix.service  
 sudo systemctl enable spamassassin.service  
 sudo systemctl start spamassassin.service

## **ClamAV**

Para poder instalarlo utilizaremos la siguiente línea de comandos

sudo apt-get install clamav clamav-freshclam clamsmpt

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 /etc/init.d/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

En la sección #AV scan filter (used by content\_filter) scan unix - - n - 16 smtp

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

[…]

-o smtp\_send\_xforward\_command = yes

-o smtp\_tls\_security\_level = may

[...]

En la sección #For injecting mail back into postfix from the filter

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

[…]

127.0.0.1:10026 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 smtp\_sender\_restrictions=

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

-o mynetworks\_style=host

-o smtp\_authorized\_xforward\_host=127.0.0.0/8

[...]

Reiniciamos los servicios de postfix y clamsmtp con las siguientes instrucciones

sudo /etc/init.d/postfix restart  
 sudo /etc/init.d/clamsmtp restart

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

Primero vamos a agregar la instrucción “refresh” al usuario root con:

sudo crontab -e

Esto nos ayudará después al definir una hora de actualización de firmas diarias, o en pocas palabras que se actualice cada cierto tiempo y para ello vamos agregar la siguiente línea al archivo que abra la instrucción pasada

00 1 \* \* \* /usr/bin/freshclam --quiet for the definitions to be update at 2am every day

Esto quiere decir que vuelva a actualizarse cada día a las 2 am

Después y para finalizar desactivaremos el demonio de “refresh” para poder guardar los cambios del ajuste automático y posteriormente actualizarlo manualmente.

sudo systemctl stop clamav-freshclam.service  
 sudo freshclam

**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

# **Instalación y configuración de herramientas de usuario.**

El correo electrónico es indispensable en la comunicación de las personas y esto ocasiona que las personas busquen en diversas herramientas para hacerlo, pensando en sus necesidades ocuparemos tres diferentes recursos para hacerlo, y estos son vía: aplicación web, aplicación de escritorio y aplicación móvil.

## **Aplicación web (SquirrelMail) [20]**

Ya que al ser un servicio web necesitamos de un servidor web para poder acceder a él, en este caso ocuparemos apache y su instalación es la siguiente:

sudo apt-get install apache2

Procederemos a instalar SquirrelMail descargando el paquete con el siguiente comando.

sudo apt-get install squirrelmail

### **Configurar el Virtual**

Para acceder a la interfaz web de SquirrelMail, cree y configure una copia de su archivo de configuración de host virtual predeterminado en el directorio Apache. Configure los ajustes en el archivo copiado para que coincidan con los ajustes de su dominio.

1. SquirrelMail proporciona un archivo de configuración por defecto para Apache en **/etc/squirrelmail/apache.conf**. Copie este archivo de configuración en la carpeta **sites-available** con el comando:

sudo cp /etc/squirrelmail/apache.conf /etc/apache2/sites-available/squirrelmail.conf

1. Edite el archivo de configuración para descomentar el bloque **<VirtualHost 1.2.3.4:80>** eliminando el símbolo de numeral **(#)**, como se muestra a continuación. Edite la IP y el Nombre del Servidor para que coincidan con la configuración de su Linodo y dominio:

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

Alias /squirrelmail /usr/share/squirrelmail

<Directory /usr/share/squirrelmail>

Options FollowSymLinks

<IfModule mod\_php5.c>

php\_flag register\_globals off

</IfModule>

<IfModule mod\_dir.c>

DirectoryIndex index.php

</IfModule>

# access to configtest is limited by default to prevent information leak

<Files configtest.php>

order deny,allow

deny from all

allow from 127.0.0.1

</Files>

</Directory>

# users will prefer a simple URL like http://webmail.example.com

<VirtualHost \*:80>

DocumentRoot /usr/share/squirrelmail

ServerName squirrelmail.example.com

</VirtualHost>

# redirect to https when available (thanks omen@descolada.dartmouth.edu)

#

# Note: There are multiple ways to do this, and which one is suitable for

# your site's configuration depends. Consult the apache documentation if

# you're unsure, as this example might not work everywhere.

#

#<IfModule mod\_rewrite.c>

# <IfModule mod\_ssl.c>

# <Location /squirrelmail>

# RewriteEngine on

# RewriteCond %{HTTPS} !^on$ [NC]

# RewriteRule . https://%{HTTP\_HOST}%{REQUEST\_URI} [L]

# </Location>

# </IfModule>

#</IfModule>

**Nota:** Si Apache está sirviendo a otros hosts virtuales, es posible que tenga que ajustarlos y/o modificar este archivo de configuración para evitar conflictos. Si está ejecutando Apache únicamente para SquirrelMail, es posible que desee eliminar el host virtual predeterminado de los **sites-enabled**.

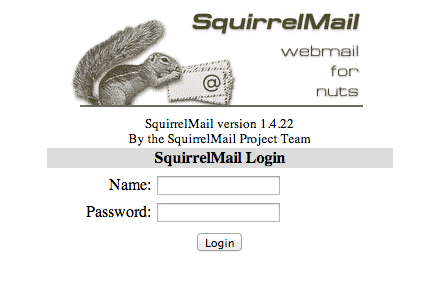
1. Habilite el nuevo host virtual:

sudo a2ensite squirrelmail.conf

1. Recarga Apache:

sudo systemctl reload apache2.service

Ahora debería poder ver la página de inicio de sesión predeterminada de SquirrelMail en su navegador después de navegar a la dirección IP o dominio:



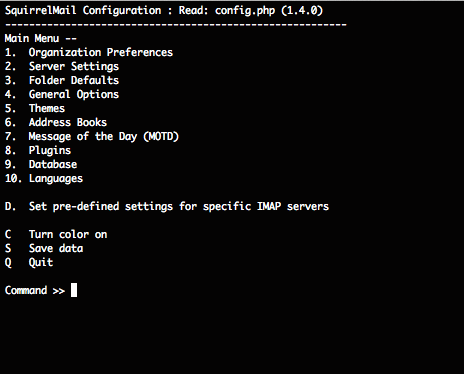
### **Configurar SquirrelMail**

Antes de usar SquirrelMail por primera vez, configúrelo para acceder a su servidor de correo. SquirrelMail proporciona una herramienta llamada **squirrelmail-configure**, una interfaz interactiva que edita el archivo **/etc/squirrelmail/config.php** para usted con la entrada que usted proporciona.

1. Inicie la aplicación squirrelmail-configure:

sudo squirrelmail-configure

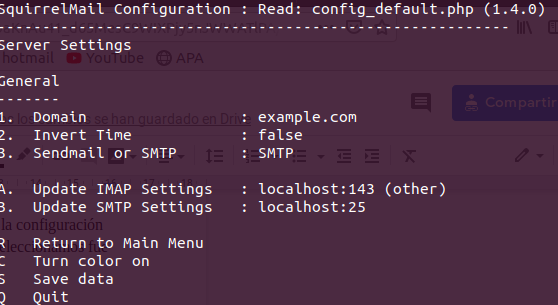
Se abrirá el menú que se muestra a continuación:



Img. 3 Menú de configuración Squirrelmail.

1. Lo que vamos a configurar es definir el dominio que habíamos introducido en la configuración de postfix (véase capítulo Postfix), en este caso el nombre del dominio que seleccionamos fue “adminsr.org”. Para ello seleccionaremos la opción 2 “Server Settings”.

Nos aparecerá otro menú como este

  
Img. 4 Menú Server Settings.

Aquí seleccionamos la opción 1 y podremos cambiar el nombre del dominio, le damos enter y nos aparecerá el cambio que hemos realizado.

1. Después regresamos al menú principal introduciendo “r” y enter, para seleccionar la opción 4 “**General Options**” y dentro del menú que despliegue seleccionar la opción 11 “**Allow server-side sorting**” cambiando el valor predeterminado “**false**” por verdadero escribiendo solo “**y**”.

Regresamos al menú principal con “r”, guardamos los cambios con “s” y salimos del script con “q”.

1. Para finalizar hay que comprobar que se instalo y configuro correctamente.

Abrimos una nueva ventana de la terminal y escribimos “ifconfig” esto para verificar nuestra dirección ip, ya que lo vamos a utilizar a continuación.

  
Img. 5 Dirección IP.

Con esa dirección ip vamos a nuestro navegador (Firefox) y en la barra de dirección escribimos “192.168.1.68/src” el cual nos dará como resultado la siguiente página.

Img. 6 Página principal squirrelmail.

# Servidor de monitoreo (Observium)

### Requerimientos

Para instalar este servidor de monitoreo, primero tenemos que instalar los módulos de PHP necesarios para su funcionamiento y los instalaremos desde la terminal con la siguiente instrucción.

sudo apt-get -y install wget php php-pear php-cgi php-common php-curl \

php-mbstring php-gd php-mysql php-gettext php-bcmath \

php-imap php-json php-xml php-snmp php-fpm php-zip

Tenemos que asegurarnos de que la zona horaria de la configuración de apache sea la correcta a la de nuestra ubicación para ello es necesario buscar la siguiente parte del código

[Date]

; Defines the default timezone used by the date functions

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

date.timezone = America/Mexico\_City

Esta configuración se debe realizar en los siguientes archivos

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

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

**Nota:** Para verificar la sintaxis correcta de las zonas horarias admitidas podemos consultar la siguiente página <https://www.php.net/manual/es/timezones.php>

Reiniciamos el archivo fpm

sudo systemctl restart php7.2-fpm.service

Para este ejemplo utilizamos el Servidor Nginx, pero se puede ocupar Apache2, Cherokee u otro servidor de sitios web. Y para instalarlo se ejecutamos:

sudo apt-get install nginx

Lo habilitamos

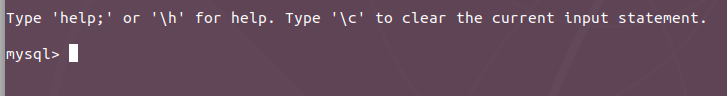
sudo systemctl enable nginx

**Nota:** Si tiene más de un servidor de sitios web en su equipo tendrá que deshabilitarlos o detenerlos.

Crearemos una base de datos para el servidor de monitoreo. Para este ejemplo se ocupó MySQL y para ello ejecutamos lo siguiente en la terminal

sudo mysql -u root -p

Nos pedirá la contraseña con la cual hayamos configurado posteriormente mysql y nos abrira el editor que se puede observar de la siguiente manera.



Una vez dentro del editor escribiremos las siguientes instrucciones:

create database observium;

flush privileges;

quit grant all privileges on observium.\* to observium@localhost IDENTIFIED by "StrongPassword";

Donde

* La primer línea la utilizamos para crear la base de datos.
* La segunda otorga los permisos necesarios para que podamos acceder a la base de datos desde el sitio web.
* La tercera permite que los privilegios se mantengan y no sea necesario reiniciar mysql.
* La cuarta solo salimos del editor de mysql.

### Instalación

Primer paso instalaremos wget que nos permite descargar contenido desde servidores web

sudo apt-get install wget

Agregamos al usuario Observium en el sistema

sudo useradd -r -M -d /opt/observium observium

Y lo agregamos al grupo de usuarios web www-data

sudo usermod -a -G observium www-data

Al terminar procederemos con la instalación de paquetes requeridos por observium

sudo apt-get update

sudo apt install rrdtool whois fping imagemagick graphviz \

mtr-tiny nmap python-mysqldb snmp snmpd python-memcache mtr-tiny acl

Nos dirigimos a la carpeta “opt”, descargamos la última versión extraemos los archivos del comprimido y posteriormente borramos el gz.

cd /opt

wget http://www.observium.org/observium-community-latest.tar.gz

tar xvf observium-community-latest.tar.gz

rm observium-community-latest.tar.gz

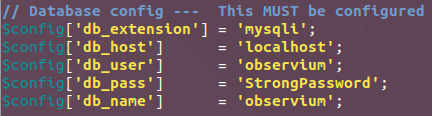
Cambie al directorio de observium y cree un archivo de configuración.

sudo cp /opt/observium/config.php.default /opt/observium/config.php

Editamos el archivo para establecer la conexión de base de datos:

sudo nano /opt/observium/config.php

Los cambios los establecemos de la siguiente manera



**Nota:** La password y usuario puede variar según la forma en como creo la base de datos.

Creamos los directorios de registro y de rrd

sudo mkdir /opt/observium/{rrd,logs}

Cambiamos los permisos del directorio

sudo chown -R observium:observium /opt/observium/

sudo chmod -R 775 /opt/observium/

### 

### Configuración de SNMP

Copiamos el archivo de muestra, esto para asegurar que no se pierda la configuración principal en caso de cometer algún error.

sudo cp /opt/observium/snmpd.conf.example /etc/snmp/snmpd.conf

Abrimos el archivo y verificamos que tenga la siguiente sintaxis, sino copiamos y pegamos.

sudo nano /etc/snmp/snmpd.conf

com2sec readonly default 0bs3rv1um

Para finalizar reiniciamos el servicio

sudo systemctl restart snmpd

### Configuración del servidor Nginx

sudo vim /etc/nginx/conf.d/observium.conf

Dentro de este archivo colocamos lo siguiente

server {

listen 80;

server\_name observium.example.com;

root /opt/observium/html;

index index.php;

charset utf-8;

gzip on;

gzip\_types text/css application/javascript text/javascript application/x-javascript image/svg+xml text/plain text/xsd text/xsl text/xml image/x-icon;

location / {

try\_files $uri $uri/ /index.php?$query\_string;

}

location /api/v0 {

try\_files $uri $uri/ /api\_v0.php?$query\_string;

}

location ~ \.php {

include fastcgi.conf;

fastcgi\_split\_path\_info ^(.+\.php)(/.+)$;

fastcgi\_pass unix:/var/run/php/php7.2-fpm.sock;

}

location ~ /\.ht {

deny all;

}

}

Verificamos la sintaxis y nos debe salir algo similar a la segunda y tercer línea:

sudo nginx -t

nginx: the configuration file /etc/nginx/nginx.conf syntax is ok

nginx: configuration file /etc/nginx/nginx.conf test is successful

Si todo esta bien, solo reiniciamos el servidor

sudo systemctl restart nginx

### 

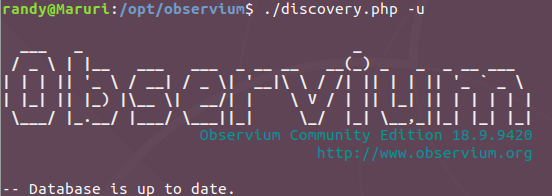
### Configurar observium en la interfaz de usuario web

Importamos el esquema de mysql, para ello nos direccionamos en la dirección de carpeta “/opt/observium”.

cd /opt/observium

./discovery.php -u

Nos debe mostrar algo como lo siguiente:



Añadimos un usuario administrador (se agrega un usuario para acceder al portal de Observium. Puede agregar más de un usuario). Dentro de la misma dirección de carpetas

./adduser.php admin AdminPass 10

El cual “admin” es el nombre de usuario y “AdminPass” la contraseña

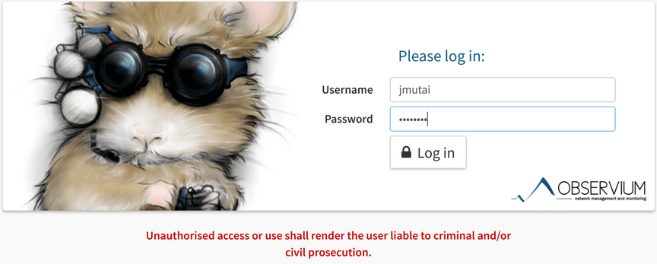
Para finalizar solo modificamos el archivo de hosts que se encuentra en la dirección “/etc”

sudo nano /etc/hosts

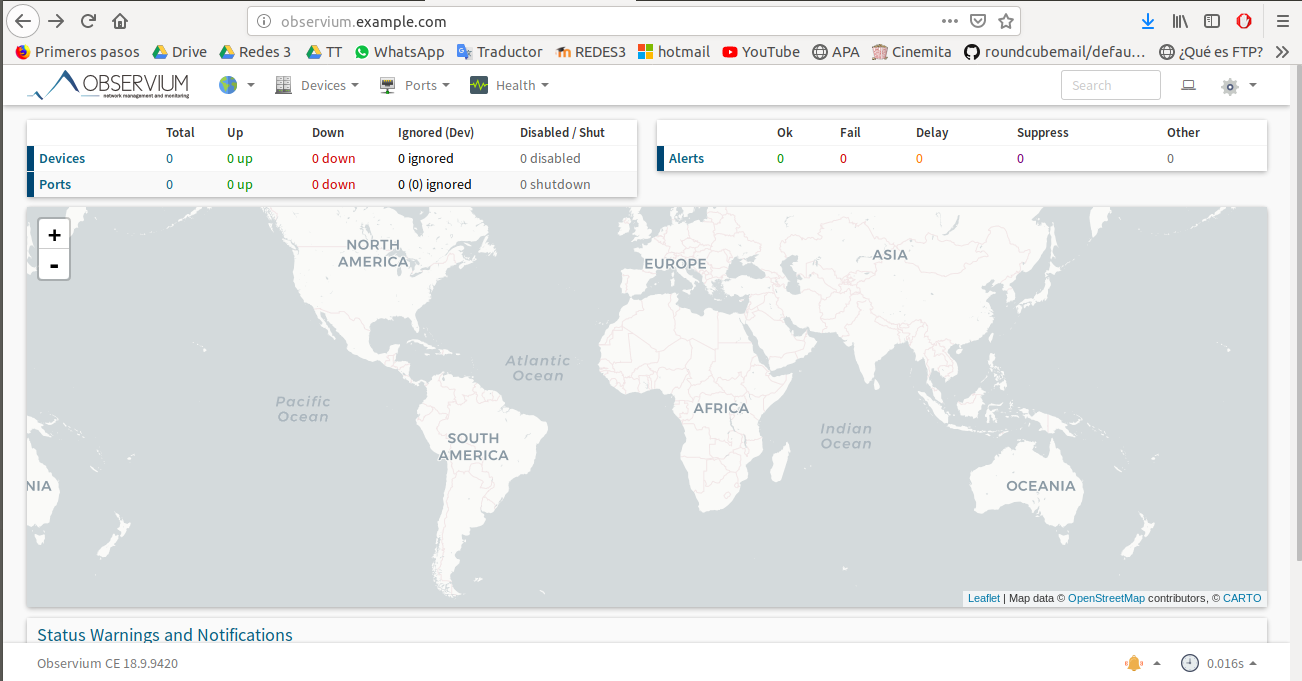
Y agregamos nuestra dirección IP seguido del nombre del dominio de nuestro sitio web en este caso “observium.example.com”



Abrimos el navegador e inicia el instalador, nos aparecera la pagina principal donde nos pedirá un usuario y una contraseña (estas son las mismas que agrego en el punto anterior).



Al introducir correctamente los valores nos direccionara a una página similar a la siguiente.



# **Bibliografía**

[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/>