

UNIVERSIDAD DEL PAÍS VASCO



SÉFTIC INFORMÁTICA

---

## Proxmox Mail Gateway

---

*Autor:*

Jon Ander Asua

<https://www.proxmox.com/en/proxmox-mail-gateway>

2021



# Índice

Índice de imágenes	3
Índice de cuadros	4
<b>1. Presentación</b>	<b>5</b>
1.1. ¿Qué es Proxmox?	5
1.2. ¿Cómo funciona?	5
1.3. Normas	6
1.4. Definiciones	7
<b>2. Preparación</b>	<b>10</b>
2.1. Crear máquinas virtuales	10
2.2. Instalar el servidor <i>Postfix</i>	10
2.3. Descargar la ISO de <i>Proxmox Mail Gateway</i>	15
<b>3. Instalación</b>	<b>16</b>
<b>4. Configuración</b>	<b>23</b>
4.1. Configuración del <i>DNS</i>	23
4.2. Configuración general	23
4.2.1. <i>Network/Time</i>	23
4.2.2. <i>Options</i>	24
4.3. <i>Mail Proxy</i>	24
4.3.1. <i>Relaying</i>	25
4.3.2. <i>Relay Domains</i>	25
4.3.3. <i>Ports</i>	26
4.3.4. <i>Options</i>	26
4.3.5. <i>Transports</i>	28
4.3.6. <i>Networks</i>	29
4.3.7. <i>TLS</i>	29
4.3.8. <i>DKIM</i>	30
4.3.9. <i>Whitelist</i>	31
4.4. <i>SPAM Detector</i>	31
4.4.1. <i>Options</i>	31
4.4.2. <i>Quarantine</i>	32
4.4.3. <i>Status</i>	33
4.4.4. <i>Custom Scores</i>	34
4.5. <i>Virus Detector</i>	34
4.5.1. <i>Options</i>	34
4.5.2. <i>ClamAV</i>	35
4.5.3. <i>Quarantine</i>	35

<b>5. Gestión de usuarios</b>	<b>37</b>
5.0.1. <i>Local</i> . . . . .	37
5.0.2. <i>LDAP</i> . . . . .	37
5.0.3. <i>Fetchmail</i> . . . . .	38
<b>6. Crear reglas</b>	<b>39</b>
6.1. <i>Listas</i> . . . . .	39
6.2. <i>Objetos</i> . . . . .	39
6.3. <i>Acciones</i> . . . . .	41
6.4. <i>Periodo de tiempo</i> . . . . .	42
6.5. <i>Crear normas</i> . . . . .	43
6.6. <i>Prueba</i> . . . . .	44
<b>7. Administración</b>	<b>46</b>
7.1. <i>Administration</i> . . . . .	46
7.1.1. <i>Status</i> . . . . .	46
7.1.2. <i>Services</i> . . . . .	46
7.1.3. <i>Updates</i> . . . . .	47
7.1.4. <i>Repositories</i> . . . . .	47
7.1.5. <i>Syslog</i> . . . . .	48
7.1.6. <i>Tasks</i> . . . . .	49
7.2. <i>SPAM Quarantine</i> . . . . .	49
7.3. <i>Attachment Quarantine</i> . . . . .	50
7.4. <i>Virus Quarantine</i> . . . . .	51
7.5. <i>User Whitelist</i> . . . . .	51
7.6. <i>User Blacklist</i> . . . . .	51
7.7. <i>Tracking Center</i> . . . . .	51
7.8. <i>Queues</i> . . . . .	52
7.8.1. <i>Summary</i> . . . . .	52
7.8.2. <i>Deferred Mail</i> . . . . .	53
<b>8. Dashboard</b>	<b>54</b>
<b>9. Crear y gestionar un <i>Cluster</i></b>	<b>55</b>
<b>10. Estadísticas</b>	<b>57</b>
10.1. <i>SPAM Scores</i> . . . . .	58
10.2. <i>Virus Charts</i> . . . . .	59
10.3. <i>Hourly Distribution</i> . . . . .	59
10.4. <i>Postscreen</i> . . . . .	60
10.5. <i>Domain</i> . . . . .	61
10.6. <i>Sender, Receiver y Contact</i> . . . . .	61

<b>11. Programa para enviar mensajes automáticamente</b>	<b>63</b>
11.1. Fichero main.py . . . . .	63
11.1.1. Métodos . . . . .	63
11.1.2. Liburutegiak . . . . .	63
11.1.3. Parametroak . . . . .	63
11.2. Fitxategiak . . . . .	64
11.2.1. Fichero de direcciones . . . . .	64
11.2.2. Fichero del texto del mensaje . . . . .	64
<b>12. Bibliografía</b>	<b>66</b>

## Índice de imágenes

1. Flujo de correo sin el servidor <i>Proxmox Mail Gateway</i> . . . . .	5
2. Flujo de correo con el servidor <i>Proxmox Mail Gateway</i> . . . . .	6
3. Forma del fichero <i>/etc/postfix/virtual</i> . . . . .	12
4. Forma del fichero <i>/etc/s-nail.rc</i> . . . . .	13
5. Opciones que ofrece el cliente de correo <i>S-nail</i> . . . . .	14
6. Texto del mensaje que se quiere enviar . . . . .	15
7. Menú de inicio de la instalación . . . . .	16
8. Licencia de usuario . . . . .	17
9. Menú para configurar la memoria . . . . .	18
10. Menú de selección de país, zona horaria e idioma del teclado . . .	19
11. Menú para la introducción de la contraseña del servidor y el correo de administración . . . . .	20
12. Menú para la configuración de red . . . . .	21
13. Informe final . . . . .	22
14. Configuración del <i>DNS</i> . . . . .	23
15. La interfaz de red que tiene el servidor . . . . .	24
16. Configuración de la ventana <i>Options</i> . . . . .	24
17. Configuración puesta en <i>Relaying</i> . . . . .	25
18. Configuración puesta en <i>Relay Domains</i> . . . . .	25
19. Configuración puesta en <i>Options</i> . . . . .	28
20. Configuración puesta en la ventana <i>Transports</i> . . . . .	29
21. Configuración puesta en la ventana <i>TLS</i> . . . . .	30
22. Configuración establecida en la ventana <i>DKIM</i> . . . . .	31
23. Configuración puesta en la ventana de <i>Options</i> de <i>SPAM Detector</i> .	32
24. Configuración establecida en la ventana <i>Quarantine</i> . . . . .	33
25. Configuración puesta en la ventana <i>Status</i> . . . . .	34
26. Configuración puesta en la ventana <i>Options</i> de <i>Virus Detector</i> .	35
27. Configuración establecida en la ventana <i>Quarantine</i> . . . . .	36
28. Ventana <i>pop-up</i> para añadir un usuario local . . . . .	37
29. Ventana <i>pop-up</i> para añadir un usuario LDAP . . . . .	38
30. Ventana <i>pop-up</i> para añadir un nuevo correo . . . . .	38
31. Ventana <i>pop-up</i> para crear una lista . . . . .	39

32.	Ventana <i>pop-up</i> para añadir un elemento a la lista . . . . .	39
33.	Ventana <i>pop-up</i> para crear una lista en el apartado <i>Action</i> . . . . .	40
34.	Ventana <i>pop-up</i> para añadir un <i>SPAM Filter</i> a la lista . . . . .	41
35.	Ventana <i>pop-up</i> para crear una nueva acción . . . . .	42
36.	Ventana <i>pop-up</i> para añadir una nueva franja horaria . . . . .	43
37.	Ventana <i>pop-up</i> para la creación de una nueva norma . . . . .	43
38.	Mensaje enviado desde <i>From</i> helbidetik bidalitako mezua . . . . .	44
39.	Buzón de entrada del receptor . . . . .	45
40.	Informe de actualización de paquetes . . . . .	47
41.	Repositorios que tiene <i>Proxmox Mail Gateway</i> . . . . .	48
42.	Forma del registro . . . . .	48
43.	Estructura de las tareas . . . . .	49
44.	Estructura de un registro de SPAM . . . . .	50
45.	Estructura del registro del filtro de archivos adjuntos . . . . .	50
46.	Estructura del registro de <i>Tracking Center</i> . . . . .	52
47.	Estructura del resumen de la fila de correo . . . . .	53
48.	Estructura de la sección <i>Dashboard</i> . . . . .	54
49.	La dirección IP y el <i>fingerprint</i> del <i>cluster master</i> . . . . .	55
50.	Ventana <i>pop-up</i> que sale en un nodo . . . . .	55
51.	Estructura de un <i>cluster</i> . . . . .	56
52.	Gráfico de <i>Total Mail Count</i> . . . . .	57
53.	Gráfico de <i>Incoming Mails</i> . . . . .	58
54.	Gráfico de <i>Outgoing mails</i> . . . . .	58
55.	Sección <i>SPAM Scores</i> . . . . .	59
56.	Gráficos que aparecen en la sección <i>Hourly Distribution</i> . . . . .	60
57.	Gráficos que salen en la sección <i>Postscreen</i> . . . . .	61
58.	Dominios y datos que aparecen en el apartado <i>Domain</i> . . . . .	61
59.	Estructura del fichero 'helbideak.txt' . . . . .	64
60.	Estructura del fichero 'message.txt' . . . . .	65

## Índice de cuadros

1.	Comandos que ofrece el servidor <i>Postfix</i> para gestionar las colas . . . . .	8
2.	Los puertos que utiliza el servidor <i>Proxmox Mail Gateway</i> . . . . .	10
3.	Atributos de las normas y sus valores . . . . .	44
4.	Métodos que componen el fichero <i>main.py</i> . . . . .	63
5.	Librerías usadas . . . . .	63
6.	Parámetros . . . . .	64

## 1. Presentación

### 1.1. ¿Qué es Proxmox?

Una herramienta *open source* que garantiza una seguridad en el email, filtra todo los correos que llegan al servidor establecido y los mensajes anteriormente decididos mediante unas reglas son eliminados o metidos en una cuarentena.

### 1.2. ¿Cómo funciona?

El servidor de correo *Proxmox Mail Gateway* se coloca entre el firewall y el servidor de correo para que pueda funcionar como filtro

Antes de instalarlo todos los correos llegan al *firewall*, de ahí van directos al servidor de correo y de ahí pasan finalmente a la terminal correspondiente. (Mirar la imagen 1)

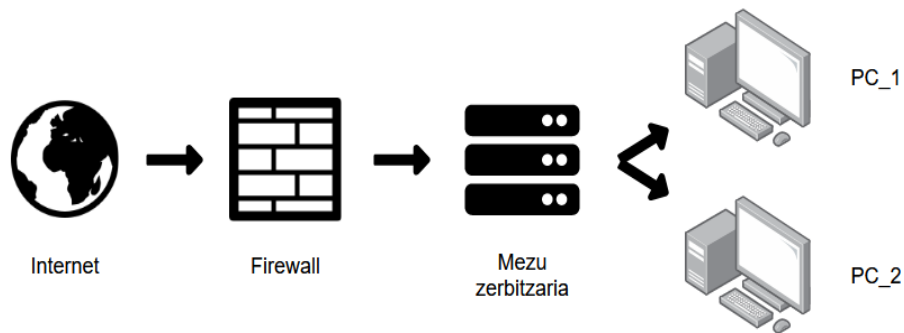


Figura 1: Flujo de correo sin el servidor *Proxmox Mail Gateway*

Como se ha comentado al inicio de este apartado si se pone el servidor *Proxmox Mail Gateway* todos los correos que pasan por el *firewall* pasan al servidor de *Proxmox* para que este pueda filtrar los correos no deseados. Los mensajes que pasan el filtro van al servidor de correo y de ahí se les manda a su respectivo terminal. (Mirar la imagen 2)

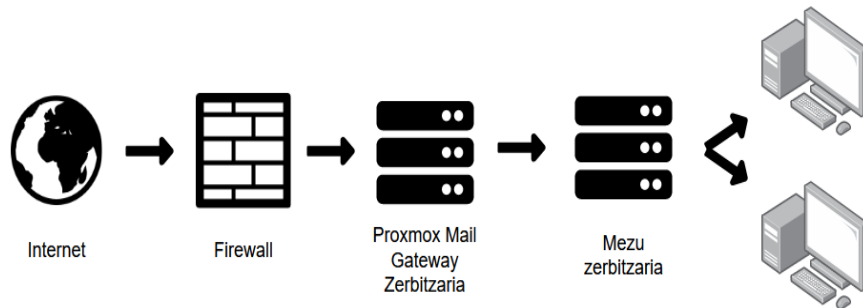


Figura 2: Flujo de correo con el servidor *Proxmox Mail Gateway*

### 1.3. Normas

Para poder hacer el filtrado anteriormente mencionado *Proxmox Mail Gateway* utiliza unos mecanismos llamados reglas y cada una de ellas está compuesta por cinco objetos:

- Objetos *who* (se utiliza dos veces): Indica quien es el emisor y el receptor de cada mensaje, puede coger estos diferentes valores:
  - Direcciones email.
  - Dominios.
  - Expresiones regulares (Para coger una dirección de email completa).
  - Direcciones IP.
  - Usuarios o grupos LDAP.
- Objeto *what*: Analiza el contenido del mensaje y toma una decisión gracias a los siguientes elementos:
  - Filtro SPAM: Captura todos los mensajes que pasen el nivel máximo de SPAM indicado.
  - Filtro de malware: Captura los mensajes contaminados.
  - Filtro de cabecera: Captura las cabeceras indicadas en la configuración.
  - Filtro de *Content type*: Captura todos los *content type* indicados en la configuración.
  - Filtro de ficheros: Captura ciertos *content type* de los ficheros adjuntos en los mensajes.
  - Utilizar expresiones regulares para cazar ciertos elementos adjuntos en los mensajes.



- Utilizar expresiones regulares para cazar los títulos de ciertos elementos adjuntos en los mensajes.
- Objeto *when*: Indica en que momentos va a estar el servidor *Proxmox Mail Gateway* en marcha, por defecto suele coger el horario de oficina.
- Objeto *Action*: Frente a una situación exacta se indica la acción que tiene que tomar el servidor. Pueden ser de tres tipos, *In* (entrada), *Out* (salida) edo *In & Out* (entrada y salida) y estas son las opciones que da:
  - Aceptar: Enviar el mensaje a quien corresponda.
  - Bloquear: Deshabilitar el envío del mensaje.
  - Cuarentena: Meter el mensaje en una cuarentena, el tiempo que tiene que estar en ella se determina en la configuración.
  - Avisar: Enviar un aviso a una persona determinada avisando del contenido del correo y si contiene SPAM o algún malware.
  - Sumar BCC (Blind Carbon Copy) : Enviar a cierta persona el mensaje procesado y sin procesar.
  - Cambiar los atributos de las cabeceras: Modificar o sumar las cabeceras de los mensajes.
  - Eliminar los ficheros adjuntos: Antes de enviar el mensaje borrar todos los ficheros adjuntados en el mensaje.
  - Añadir un *Disclaimer*: Para quitar responsabilidades a la empresa se añade un elemento HTML que es un *disclaimer*.

## 1.4. Definiciones

Antes de empezar con la instalación y la configuración hay que definir un par de términos:

- *Cluster*(1): Son un grupo de ordenadores unidos por una red de alta velocidad, gracias a esto funcionan como un ordenador único. Existen tres tipos:
  - *Clusters* de alto rendimiento: Se utiliza en sistemas que requieren una gran capacidad de cálculo y bastante memoria.
  - *Clusters* de alta disponibilidad: Se utiliza en sistemas que requieren una gran fiabilidad. Para garantizar esto utiliza *hardware* duplicado.
  - *Clusters* de alta eficiencia: El objetivo de estos sistemas es hacer la mayor cantidad de tareas en el mínimo tiempo posible.

Aparte de todo esto un *cluster* se compone de los siguientes elementos:

- Nodos: Son las terminales que componen el *cluster*, puede ser un ordenador o un servidor.

- Sistema operativo: Se puede utilizar cualquier sistema operativo pero tiene que cumplir dos requisitos, que sea multitarea y multiusuario.
  - Conexión de red: Todos los nodos tienen que estar conectados a la red, para eso se va a utilizar la conexión *ethernet* o algún otra conexión de alta velocidad.
  - *Middleware*: Software que se coloca entre el sistema operativo y las aplicaciones. Su trabajo es unir todos los nodos que componen el *cluster* para crear un único ordenador.
  - Sistema de almacenado: Los datos se pueden almacenar por un lado de forma local en un disco duro o por otro lado se pueden utilizar diferentes herramientas, como por ejemplo *Network Attaches Storage* o *Storage Area Network*.
- Cola de mensajes (2): Es una fila que se compone de los mensajes que están esperando para que su envío sea procesado. En este proyecto se va a utilizar el servidor de correo *postfix*. Este servidor ofrece los siguientes comandos para gestionar estas colas: (Mirar la tabla 1)

Tarea	Comando
Listar los mensajes de la lista	postqueue -p
Volver a enviar todos los mensajes de la lista	postqueue -f
Borrar todos los mensajes de la lista	postsuper -d ALL
Borrar un mensaje específico	postsuper -d "Queue ID"postsuper -d <message-id>

Cuadro 1: Comandos que ofrece el servidor *Postfix* para gestionar las colas

- *TLS*(3): Es la siguiente versión del cifrado *SSL*. Para cifrar los correos sigue los siguientes pasos:
- *TLS Record Protocol*: En este apartado se garantiza que el envío del mensaje se va a hacer de una forma privada y segura.
  - *TLS Handshake Protocol*: El mensaje se manda de una forma segura, en cada apartado de la cabecera se coloca un *content type* y se crea un código de autenticación.
- *SMTP*(4): Es el protocolo que permite enviar correos mediante internet, normalmente se une a los protocolos POP3 (los mensajes recibidos se guardan de forma local) o IMAP (los mensajes recibidos se guardan en un servidor). Este protocolo utiliza dos tipos de puertos. Por un lado están los puertos sin protección (25, 587 y 2525) y por el otro los puertos con un cifrado *SSL* (4065 y 25025).

- *SPF*(5): Se determina las direcciones que pueden mandar mensajes por cada dominio. Este protocolo se registra mediante un fichero `.txt` en el *DNS*. Su estructura es la siguiente:
  - `v.spf1`: Se determina el registro como *SPF*.
  - *Mechanism*: Un registro que puede tener diferentes mecanismos.
  - `a`: Indica el servidor *DNS* X que es válido para hacer envíos.
  - `mx`: Indica el registro MX que es válido para hacer envíos.
  - `ptr`: El nombre de la dirección IP contraria del host.
  - `IP4`: Lista de direcciones IPv4 que pueden hacer envíos.
  - `IP6`: Lista de direcciones IPv6 que pueden hacer envíos.
  - `include.domain`: Se añade el registro *SPF* al dominio.
  - `exists`: Verifica si existe un registro para el dominio.
- *DNS*: Es un servidor que sirve para traducir dominios. Al llegar un dominio al servidor este lo traduce y devuelve su dirección IP pública. Por ejemplo si se le envía el dominio 'jonander.xyz' el servidor *DNS* va a devolver la dirección '157.90.30.163'.
- Registro MX: Son unos registros obligatorios para un servidor *DNS* sea capaz de recibir correos electrónicos. Gracias a este registro a la hora de mandar un correo a un dominio este lo reenviará a la terminal que toque.

## 2. Preparación

Antes de instalar y configurar *Proxmox Mail Gateway* hay que preparar un entorno apto, para eso se van a configurar los siguientes elementos.

### 2.1. Crear máquinas virtuales

Para empezar hay que crear dos máquinas virtuales, una va a coger el rol de ser el servidor de correo y el otro va a tener la instalación de *Proxmox Mail Gateway*.

- Servidor de correo: Es un servidor con el sistema operativo Ubuntu 20.04, en él se va a instalar el servidor de correo *postfix* y se va a conectar con un email creado en el servidor (en este caso el correo 'root@jonander.xyz' en el dominio 'jonander.xyz'). Para conectarse contra este servidor se va a utilizar el servicio SSH.
- Servidor *Proxmox Mail Gateway*: En un servidor alojado físicamente en la empresa se va a crear una máquina virtual y ahí se va a instalar el servidor *Proxmox Mail Gateway* mediante una ISO. Para gestionar este servidor se va a utilizar el programa *VMWare*.

Aparte de esto, el servidor en el que está alojado *Proxmox Mail Gateway* tiene que tener abiertos los siguientes puertos: (Mirar tabla 2)

Servicio	Puerto (TCP)	Dirección
SMTP	25	Entrada / Salida
SMTP	26	Entrada
NTP	123	Salida
RAZOR	2703	Salida
DNS	53	Salida
HTTP	80	Salida
GUI/API	8006	Entrada

Cuadro 2: Los puertos que utiliza el servidor *Proxmox Mail Gateway*

### 2.2. Instalar el servidor *Postfix*

Para instalar el servidor *Postfix* hay que seguir los siguientes pasos: (6)

- Para empezar se va a instalar el paquete de *postfix* con el siguiente comando:

```
$ sudo DEBIAN_PRIORITY=low apt install postfix
```

Al hacer 'DEBIAN\_PRIORITY=low' se permite configurar más elementos.

- Al ejecutar el comando se va a abrir una ventana para empezar la configuración, esta tiene los siguientes elementos:

- *General type of mail configuration*: En cada caso se va a elegir la configuración que más se desee, las opciones son las siguientes:
  - *No configuration*: Cuando se quiere la configuración por defecto.
  - *Internet site*: Para utilizar el protocolo de comunicación SMTP.
  - *Satellite system*: Cuando todos los mensajes se redireccionan a otra máquina llamada *Smarthost*.
  - *Local only*: Cuando solo se utiliza entre usuarios locales.

En este caso se va a coger la opción de *Internet Site*.

- *System mail name*: Es la raíz del dominio para crear una dirección email, se va a poner el dominio que se quiere que tenga el correo. En este caso se va a utilizar el dominio de 'jonander.xyz'.
- *Mail recipient*: Se especifica a quien enviar los correos enviados a los usuarios 'root@' y 'postmaster@'. En este caso se le van a enviar al usuario 'root'.
- *Other destinations to accept mail for*: Se especifica que instancias va a aceptar el servidor *Postfix* como metas de correo. En este caso se va a poner la configuración por defecto la cual es: '\$myhostname, jonander.xyz, ubuntu-2gb-nbg1-2, localhost.localadmin,localhost'.
- *Force synchronous updates on mail queue*: Cuand hay un envío de mensajes masivo el protocolo SMTP crea una fila de mensajes. En este caso se va a elegir la opción 'No'. (7)
- *Local networks*: Se declara la lista de redes capaces que tiene el servidor configurado a la hora de transmitir. En este caso se va a poner la opción por defecto.
- *Mailbox size limit*: Se determina el tamaño de los mensajes, en este caso se ha escogido el '0' ya que con esto se consigue desactivar esta configuración.
- *Local adress extension character*: Se declara que caracter sirve para separar la parte regular de la extensión, en este caso se va a utilizar el caracter '+'. (7)
- *Internet protocols to use*: Se declara la lista de tipos de direcciones IP que el servidor *Postfix* va a aceptar. En este caso se van a aceptar todas (la opción *All*), tanto las de IPv4 como las de IPv6.

Una vez se han configurado todos los elementos anteriormente mencionados el servidor *Postfix* se ha instalado, para cambiar la configuración se ejecutará el siguiente comando:

```
$ sudo dpkg-reconfigure postfix
```

- Después de instalar el servidor de correo *Postfix* se procederá a cambiar la configuración, para eso se van a seguir los siguientes pasos:

- Para empezar se va a poner el buzón de correo de todos los usuarios que no sean 'root', la carpeta *Mailbox*. Para eso se va a ejecutar el siguiente comando:

```
$ sudo postconf -e 'home_mailbox= Maildir/'
```

- Después, se va a colocar la dirección 'virtual\_alias\_maps', para eso se va a ejecutar el siguiente comando:

```
$ sudo postconf -e 'virtual_alias_maps= hash:/etc/postfix/virtual'
```

- Una vez puesta la dirección del fichero se va a crear y se van a poner las direcciones de correo electrónico y sus respectivos usuarios con el siguiente comando: (Mirar imagen 3)

```
$ sudo nano /etc/postfix/virtual
```

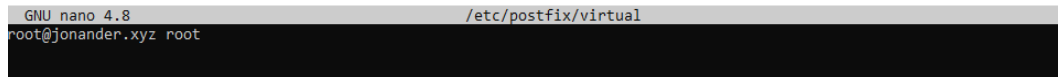


Figura 3: Forma del fichero `/etc/postfix/virtual`

- Para verificar todos los cambios hechos se van a ejecutar los siguientes comandos:

```
$ sudo postmap /etc/postfix/virtual
```

```
$ sudo systemctl restart postfix
```

- Al acabar con la configuración hay que iniciar el servicio *postfix*, para eso se va a utilizar el *firewall* UFW y se va a ejecutar el siguiente comando:

```
$ sudo ufw allow Postfix
```

- Después de configurar y habilitar el servidor de correo se va a proceder a la instalación del cliente de correo, para ello se seguirán los siguientes pasos:

- Para empezar se va a declarar la variable 'Mail' en el fichero /etc/bash.bashrc eta /etc/profile.d utilizando el siguiente comando:

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

- Al acabar se va a instalar el cliente de correo *s-nail* mediante el siguiente comando:

```
$ sudo apt install s-nail
```

- Después de instalar *S-nail* se va a abrir el fichero /etc/s-nail.rc y al final se van a añadir las siguientes lineas (Mirar la imagen 4):

```
GNU nano 4.8 /etc/s-nail.rc
# colour mono mle-error ft=reverse
#endif

# Install file-extension handlers to handle MBOXes in various formats.
# filetype \
#   bz2 'bz2 -dc' 'bz2 -zc' \
#   bzip2 'bzip2 -dc' 'bzip2 -zc' \
#   gz 'gzip -dc' 'gzip -c' \
#   xz 'xz -dc' 'xz -zc' \
#   zstd 'zstd -dc' 'zstd -19 -zc' \
#   zstd.pgp 'pgp -d | zstd -dc' 'zstd -19 -zc | pgp -e'

# If mail is send from cron scripts and iconv(3) is compiled it, it could be
# that sending fails because of invalid (according to locale) character input.
# This undesired event can be prevented as follows, the (possibly) resulting
# octet-stream message data can be read nonetheless via
# *mime-counter-evidence*=0b1111:
# if ! terminal && [ "$LOGNAME" == root ]
#   set mime-force-sendout
# endif

# s-it-mode
set emptystart
set folder=Maildir
set record=+sent
```

Figura 4: Forma del fichero /etc/s-nail.rc

Las lineas insertadas significan lo siguiente:

- *set emptystart*: Aun que la bandeja de entrada esté vacía el usuario puede abrirla.

- *set folder* = Maildir: Se le asigna el valor Maildir a la variable 'folder'.
- *set folder* = Maildir: Bidali egin diren mezu elektronikoen erregistroa 'Maildir' karpetan gordetzen dira, defektuz 'sent' izeneko karpeta bat sortzen du.
- Se va a enviar localmente un mensaje al usuario 'root', para eso se va a ejecutar el siguiente comando:

```
$ echo 'Kaixo Mundua' | s-nail -s 'kaixoMundua' -Snorecord root
```

Para saber si el correo ha llegado, se va a mirar en el fichero 'Maildir/new'.

- Para abrir el cliente se ejecutará el siguiente comando:

```
$ s-nail
```

- Al abrirse el cliente se va a sacar la tecla ENTER y aparecerá el correo enviado en el punto anterior. Aparte, el cliente ofrece diferentes opciones. (Mirar la imagen 5)

```
type <msglist>      type ('print') messages (honour 'headerpick' etc.)
Type <msglist>      like 'type' but always show all headers
next               goto and type next message
headers            header summary ... for messages surrounding "dot"
search <msglist>    ... for the given expression list (alias for 'from')
delete <msglist>    delete messages (can be 'undelete'd)

save <msglist> folder append messages to folder and mark as saved
copy <msglist> folder like 'save', but do not mark them ('move' moves)
write <msglist> file  write message contents to file (prompts for parts)
Reply <msglist>      reply to message sender(s) only
reply <msglist>      like 'Reply', but address all recipients
lreply <msglist>     forced mailing list 'reply' (see 'mlist')

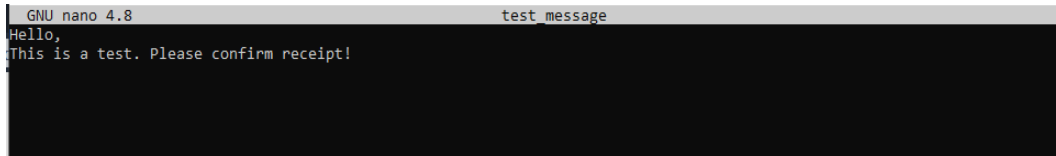
mail <recipients>   compose a mail for the given recipients
file folder         change to another mailbox
File folder         like 'file', but open readonly
quit               quit and apply changes to the current mailbox
xit or exit        like 'quit', but discard changes
!shell command     shell escape
list [<anything>]  all available commands [in search order]
?
```

Figura 5: Opciones que ofrece el cliente de correo *S-nail*

- Para enviar un mensaje desde el cliente *S-nail* se van a seguir los siguientes pasos:



- Se va a escribir el mensaje que se quiera enviar en un fichero de texto. (Mirar la imagen 6)



```
GNU nano 4.8 test_message
Hello,
This is a test. Please confirm receipt!
```

Figura 6: Texto del mensaje que se quiere enviar

- Una vez se ha escrito el texto se va a ejecutar el siguiente comando para enviar el mensaje:

```
$ cat /test_message | s-nail -s 'Test email subject line' -r emisor@ejemplo.com receptor@email.com
```

En este caso el comando es el siguiente

```
$ cat /test_message | s-nail -s 'Test email subject line' -r root@jonander.xyz jasumiranda1998@gmail.com
```

Esto quiere decir que la dirección 'root@jonander.xyz' le va a enviar a la dirección 'jasumiranda1998@gmail.com' el mensaje escrito en el fichero 'test\_message' con el asunto 'test email subject line'.

### 2.3. Descargar la ISO de *Proxmox Mail Gateway*

Para poder descargar la ISO de *Proxmox Mail Gateway* se va a ir a su página web oficial y se va a descargar la última versión, en este caso se ha elegido la 7.0.

La descarga se ha hecho desde el siguiente link:

<https://www.proxmox.com/en/downloads>

### 3. Instalación

Para hacer la instalación del servidor *Proxmox Mail Gateway* se seguirán los siguientes pasos:

- Para empezar la ISO descargada se va a cargar en la maquina virtual creada mediante *VMWare*.
- Después de cargar la ISO la configuración de *Proxmox Mail Gateway* arrancará. Para empezar, aparecerá un menú con cuatro opciones (*Install Proxmox Mail Gateway*, *Install Proxmox Mail Gateway (debug mode)*, *Rescue boot*, *Test memory (legacy BIOS)*). Se ha elegido la opción '*Install Proxmox Mail Gateway*'. (Mirar la imagen 7)



Figura 7: Menú de inicio de la instalación

- Después se va a aceptar la licencia de usuario (Mirar la imagen 8)



### END USER LICENSE AGREEMENT (EULA)

#### END USER LICENSE AGREEMENT (EULA) FOR PROXMOX MAIL GATEWAY

By using Proxmox Mail Gateway software you agree that you accept this EULA, and that you have read and understand the terms and conditions. This also applies for individuals acting on behalf of entities. This EULA does not provide any rights to Support Subscriptions Services as software maintenance, updates and support. Please review the Support Subscriptions Agreements for these terms and conditions. The EULA applies to any version of Proxmox Mail Gateway and any related update, source code and structure (the Programs), regardless of the delivery mechanism.

1. License. Proxmox Server Solutions GmbH (Proxmox) grants to you a perpetual, worldwide license to the Programs pursuant to the GNU Affero General Public License V3. The license agreement for each component is located in the software component's source code and permits you to run, copy, modify, and redistribute the software component (certain obligations in some cases), both in source code and binary code forms, with the exception of certain binary only firmware components and the Proxmox images (e.g. Proxmox logo). The license rights for the binary only firmware components are located within the components. This EULA pertains solely to the Programs and does not limit your rights under, or grant you rights that supersede, the license terms of any particular component.

2. Limited Warranty. The Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose. Neither Proxmox nor its affiliates warrants that the functions contained in the Programs will meet your requirements or that the operation of the Programs will be entirely error free, appear or perform precisely as described in the accompanying documentation, or comply with regulatory requirements.

3. Limitation of Liability. To the maximum extent permitted under applicable law, under no

Abort

Previous

I agree

Figura 8: Licencia de usuario

- Después de aceptar la licencia va a aparecer una ventana nueva para elegir la partición del disco duro en el que se quiera instalar el servidor *Proxmox*. En este caso al haber solo una partición se va a elegir esa. (Mirar la imagen 9)



Figura 9: Menú para configurar la memoria

- Posteriormente se va a seleccionar el país, la zona horaria y el idioma del teclado. En este caso la configuración establecida ha sido la siguiente: (Mirar la imagen 10)



### Location and Time Zone selection

**The Proxmox Installer** automatically makes location-based optimizations, like choosing the nearest mirror to download files from. Also make sure to select the correct time zone and keyboard layout.

Press the Next button to continue the installation.

- **Country:** The selected country is used to choose nearby mirror servers. This will speed up downloads and make updates more reliable.
- **Time Zone:** Automatically adjust daylight saving time.
- **Keyboard Layout:** Choose your keyboard layout.

A screenshot of the installation form. It has a light gray background. At the top, there are three labels: 'Country', 'Time zone', and 'Keyboard Layout'. Each label is followed by a text input field. The 'Country' field contains the text 'Spain'. The 'Time zone' field is a dropdown menu showing 'Europe/Madrid'. The 'Keyboard Layout' field is a dropdown menu showing 'Spanish'. At the bottom of the form, there are three buttons: 'Abort' on the left, 'Previous' in the middle, and 'Next' on the right.

Figura 10: Menú de selección de país, zona horaria e idioma del teclado

- Al acabar el anterior punto se van a poner la contraseña del servidor y un correo de administración. (Mirar la imagen 11)

The screenshot shows the 'Mail Gateway Installer' window for Proxmox. The title bar includes the Proxmox logo and the text 'Mail Gateway Installer'. The main heading is 'Administration Password and Email Address'. Below this, there is explanatory text about Proxmox Mail Gateway and instructions to provide the root password. Two bullet points provide guidelines for the password and email address. A blue button labeled 'Next' is highlighted with a tooltip that says 'Press the Next button to continue installation.' The form contains three input fields: 'Password' (masked with dots), 'Confirm' (masked with dots), and 'Email' (containing 'uamiranda1998@gmail.com'). At the bottom, there are three buttons: 'Abort', 'Previous', and 'Next'.

**PROXMOX** Mail Gateway Installer

### Administration Password and Email Address

**Proxmox Mail Gateway** is a full featured highly secure GNU/Linux system based on Debian.

Please provide the *root* password in this step.

- **Password:** Please use a strong password. It should have 8 or more characters. Also combine letters, numbers, and symbols.
- **Email:** Enter a valid email address. Your Proxmox Mail Gateway will send important alert notifications to this email account (all mails for 'root').

Press the **Next** button to continue installation.

Password: [masked]  
Confirm: [masked]  
Email: uamiranda1998@gmail.com

Abort Previous Next

Figura 11: Menú para la introducción de la contraseña del servidor y el correo de administración

- Después de esto se va a configurar la red. En este caso se va a poner la configuración por defecto pero se va a introducir el dominio 'jonander.xyz'. (Mirar la imagen 12)

The screenshot shows the 'Mail Gateway Installer' window with the title 'Management Network Configuration'. It includes instructions to verify network settings and lists three required fields: IP address (CIDR), Gateway, and DNS Server. Below the text is a form with the following fields: Management Interface (dropdown menu showing 'enp0s3 - 08:00:27:74:85:7c (e1000)'), Hostname (FQDN) (text input with 'jonander.xyz'), IP Address (CIDR) (text input with '10.0.2.15' and a dropdown for '24'), Gateway (text input with '10.0.2.2'), and DNS Server (text input with '192.168.1.1'). At the bottom are 'Abort', 'Previous', and 'Next' buttons.

**PROXMOX** Mail Gateway Installer

### Management Network Configuration

**Please verify** the displayed network configuration. You will need a valid network configuration to access the management interface after installing.

After you have finished, press the Next button. You will be shown a list of the options that you chose during the previous steps.

- **IP address (CIDR):** Set the main IP address and netmask for your server in CIDR notation.
- **Gateway:** IP address of your gateway or firewall.
- **DNS Server:** IP address of your DNS server.

Management Interface: enp0s3 - 08:00:27:74:85:7c (e1000) ▼

Hostname (FQDN): jonander.xyz

IP Address (CIDR): 10.0.2.15 / 24


Gateway: 10.0.2.2

DNS Server: 192.168.1.1

Abort Previous Next

Figura 12: Menú para la configuración de red

- Para acabar aparecerá un informe de la configuración hecha, si está todo bien puesto se pulsará el botón 'Install' y automáticamente va a empezar la instalación del servidor. (Mirar la imagen 13)

Mail Gateway Installer

### Summary

**Please confirm** the displayed information. Once you press the **Install** button, the installer will begin to partition your drive(s) and extract the required files.

Option	Value
Filesystem:	ext4
Disk(s):	/dev/sda
Country:	Spain
Timezone:	Europe/Madrid
Keymap:	es
Email:	jasuamiranda1998@gmail.com
Management Interface:	enp0s3
Hostname:	jonander
IP CIDR:	10.0.2.15/24
Gateway:	10.0.2.2
DNS:	192.168.1.1

☒ Automatically reboot after successful installation

Abort

Previous

Install

Figura 13: Informe final



## 4. Configuración

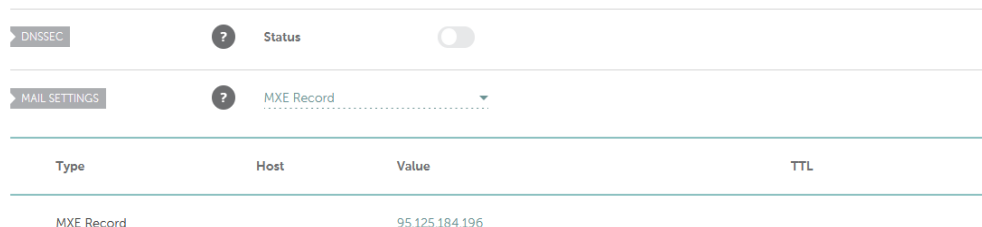
Después de la instalación se va a configurar el servidor *Proxmox Mail Gateway*, para ello se van a utilizar el gestor de *hosting* y la GUI que ofrece el mismo *Proxmox Mail Gateway*. En este caso la GUI está alojada en la dirección '192.168.1.202' y como se ha dicho en la primera tabla utiliza el puerto 8006. La información utilizada para hacer este punto ha sido en mayor parte sacada en la documentación original de *Proxmox Mail Gateway*, para ver dicha documentación el link es el siguiente:

<https://www.proxmox.com/en/downloads/category/documentation-pmg>

### 4.1. Configuración del *DNS*

Para configurar el *DNS*, en este caso mediante el gestor <https://www.namecheap.com/>, en el apartado 'Mail Settings' se va a elegir el valor 'MXE Record' y en el apartado 'Value' se pondrá la dirección IP pública en la que está instalado el servidor *Proxmox* (Mirar la imagen 14). Para saber esa dirección de IP pública se ejecutará el siguiente comando:

```
$ curl ifconfig.me
```



Type	Host	Value	TTL
MXE Record		95.125.184.196	

Figura 14: Configuración del *DNS*

### 4.2. Configuración general

La configuración general tiene dos ventanas principales:

#### 4.2.1. *Network/Time*

Esta ventana tiene tres apartados principales:

- *Time*: En este apartado se especifica la hora y la zona horaria del servidor.

- *DNS*: En este punto se determinan que servidores *DNS* utiliza el servidor. En este caso se van a poner las direcciones '8.8.8.8', '8.8.4.4' y '37.235.1.174'.
- *Interfaces*: Se determinan las interfaces de red que tiene el servidor, en este caso la configuración es la siguiente: (Mirar la imagen 15)

Interfaces									
<div> <div>Create</div> <div>Revert</div> <div>Edit</div> <div>Remove</div> <div>Apply Configuration</div> </div>									
Name ↑	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
ens192	Network Device	Yes	Yes	No			192.168.1.202/24	192.168.1.1	

Figura 15: La interfaz de red que tiene el servidor

#### 4.2.2. Options

La ventana *Options* tiene los siguientes apartados:

- *Send daily admin reports*: Opción de crear y enviar informes para la administración todos los días.
- *Use advanced statistic filters*: Permite el uso de filtros de estadística avanzada.
- *User statistic lifetime*: Determinar el número de días que permanecen en el servidor los informes estadísticos.
- *Administration email*: Se determina la dirección de correo electrónico establecida con el rol de administrador.
- *HTTP proxy*: Capacidad para identificar tráfico web, malware u otro tipo de intrusiones, incluso de proteger el servidor frente a ataques HTTP. (8)

En este caso se ha establecido la siguiente configuración: (Mirar la imagen 16)

<div> <div>Network/Time</div> <div>Options</div> </div>	
Edit	
Send daily admin reports	Yes
Use advanced statistic filters	Yes
User statistic lifetime (days)	7
Administrator EMail	jonander@seftic.com
HTTP proxy	none

Figura 16: Configuración de la ventana *Options*

### 4.3. Mail Proxy

Para la configuración de *Mail proxy* hay 9 diferentes ventanas, son las siguientes:

#### 4.3.1. *Relaying*

En esta ventana se configura todo lo relacionado con el *relay*, estos son sus apartados:

- *Default relay*: Se determina la Ip pública del servidor de correo a la que *Proxmox* se va a conectar.
- *Relay port*: Se determina el puerto al que tiene que ir, por defecto al 25.
- *Relay protocol*: Se determina el protocolo que utiliza el servidor anteriormente mencionado.
- *Disable MX lookup (SMTP)*: Dado un dominio permite devolver el registro MX.(9)

En este caso se ha puesto la siguiente configuración (Mirar la imagen 17)

Configuration: Mail Proxy	
Relaying	Relay Domains Ports Options Transports Networks TLS DKIM Whitelist
Edit	
Default Relay	116.203.233.29
Relay Port	25
Relay Protocol	smtp
Disable MX lookup (SMTP)	No
Smarthost	none

Figura 17: Configuración puesta en *Relaying*

#### 4.3.2. *Relay Domains*

En esta ventana se definen los dominios puestos en el servidor de correo. En este caso se ha puesto el siguiente: (Mirar la imagen 18)

Configuration: Mail Proxy	
Relaying	Relay Domains Ports Options Transports Networks TLS DKIM Whitelist
Edit Create Remove	
Relay Domain ↑	Comment
jonander.xyz	

Figura 18: Configuración puesta en *Relay Domains*

#### 4.3.3. *Ports*

En la ventana *Ports* hay dos apartados principales, *External* e *Internal SMTP Port*. Aquí se define que puertos va a tener como entrada y salida el *SMTP*. En este caso al usar dos servidores diferentes se ha puesto tanto en *External* como en *Internal* el puerto 25.

#### 4.3.4. *Options*

En esta ventana aparece la configuración general de *Mail Proxy*:

- *Message size*: Se determina el peso máximo en bytes que soporta cada mensaje.
- *Reject unknown clients*: Se determina si se pueden aceptar receptores desconocidos.
- *Reject unknown senders*: Se determina si se pueden aceptar remitentes desconocidos.
- *SMTP HELO check*: Permite verificar la dirección SMTP del remitente. (10)
- *DNSBL sites*: Permite utilizar listas negras predefinidas. (11)
- *DNSBL threshold*: Determina el límite inferior para bloquear un cliente SMTP remoto.
- *Verify receivers*: Permite verificar al receptor.
- *Use greylisting for IPv4*: Permite utilizar listas grises compuestas por direcciones IPv4. (12)
- *Netmask for greylisting IPv4*: Permite el uso de las *netmask* para filtrar direcciones IPv4. (13)
- *Use greylisting for IPv6*: Permite utilizar listas grises compuestas por direcciones IPv6. (12)
- *Netmask for greylisting IPv6*: Permite el uso de las *netmask* para filtrar direcciones IPv6. (13)
- *Use SPF*: Permite el uso de SPF para enviar mensajes solo de servidores de correos específicos.
- *Hide internal hosts*: A la hora de enviar mensajes al exterior permite eliminar los hosts internos de la cabecera. (14)
- *Delay warning time (hours)*: Cuando un mensaje está atrasado el límite de horas que tiene que pasar para que se le envíe un correo de aviso al administrador.

- *Client connection count limit*: Se determina el número máximo de usuarios que pueden estar conectados a la vez. (15)
- *Client connection rate limit*: Determina el número de conexiones máximas que puede hacer un usuario en un tiempo determinado. (15)
- *Client message rate limit*: Se determina la cantidad de solicitudes de correo máxima que un usuario puede hacer en un tiempo determinado. (15)
- *SMTPD banner*: Respues SMTP que recibe el servidor a la hora de conectarse a un servidor *Exchange*. (16)
- *Send NDR or block emails*: Permite envitar un correo NDR (mensaje que se le envía al remitente cuando hay algún error a la hora de enviar el correo) o bloquear el mensaje.
- *Before queue filtering*: Antes de añadir un mensaje a la fila permite pasarlo por un filtro. (17)

En este caso se va a poner la siguiente configuración: (Mirar la imagen 19)

Configuration: Mail Proxy

Relaying
Relay Domains
Ports
Options
Transports
Networks
TLS
DKIM
Whitelist

Edit

Message Size (bytes)	5242880
Reject Unknown Clients	No
Reject Unknown Senders	No
SMTP HELO checks	Yes
DNSBL Sites	zen.spamhaus.org,b.barracudacentral.org
DNSBL Threshold	1
Verify Receivers	No
Use Greylisting for IPv4	Yes
Netmask for Greylisting IPv4	24
Use Greylisting for IPv6	No
Netmask for Greylisting IPv6	64
Use SPF	Yes
Hide Internal Hosts	No
Delay Warning Time (hours)	4
Client Connection Count Limit	50
Client Connection Rate Limit	0
Client Message Rate Limit	0
SMTPD Banner	ESMTP Proxmox
Send NDR on Blocked E-Mails	No
Before Queue Filtering	No

Figura 19: Configuración puesta en *Options*

#### 4.3.5. *Transports*

En esta ventana se configuran los casos en los que el servidor de correo y el de *Proxmox Mail Gateway* no están en la misma red. Para ello se van a añadir el nombre del dominio, el *host* (la dirección IP), el protocolo, el puerto y si usa MX. En este caso se ha configurado de la siguiente manera (Mirar la imagen 20)

Relaying	Relay Domains	Ports	Options	Transports	Networks	TLS	DKIM	Whitelist
Edit	Create	Remove						
Relay Domain ↑	Host	Protocol	Port	Use MX				
jonander.xyz	116.203.233.29	smtp	25	No				

Figura 20: Configuración puesta en la ventana *Transports*

#### 4.3.6. *Networks*

Esta ventana permite añadir direcciones de IP locales, en este caso no se ha añadido ninguna.

#### 4.3.7. *TLS*

Esta ventana permite la configuración para garantizar la seguridad en la capa de transporte. Se dan las siguientes opciones:

- *Enable TLS*: Habilita la seguridad en la capa de transporte anteriormente mencionada.
- *Enable TLS logging*: Proporciona información sobre la actividad de SMTP *TLS*.
- *Add TLS received header*: Permite obtener el protocolo usado e información del cifrado.

En este caso no se ha utilizado esta opción así que en consecuencia en las opciones anteriormente mencionadas se ha puesto 'No'. (Mirar la imagen 21)  
Para añadir un protocolo *TLS* hay que pinchar sobre el botón *Create* y ahí hay que determinar que política se quiere utilizar.

Configuration: Mail Proxy

Relaying   Relay Domains   Ports   Options   Transports   Networks   **TLS**   DKIM   Whitelist

---

Settings

Edit

Enable TLS	No
Enable TLS Logging	No
Add TLS received header	No

---

TLS Destination Policy

Edit   **Create**   Remove

Destination	Policy
-------------	--------

Figura 21: Configuración puesta en la ventana *TLS*

#### 4.3.8. DKIM

En esta ventana se da la opción de verificar el remitente de un correo de forma criptográfica usando una firma *DomainKeys Identified Mail (DKIM)*. Las opciones son las siguientes:

- *Enable DKIM signing*: Permite habilitar las firmas *DKIM*.
- *Selector*: Permite elegir una firma concreta en la lista de firmas *DKIM*.
- *Sign all outgoing mail*: Permite controlar que todo aquel correo que salga (o solo de unos servidores en específico) tiene la firma correspondiente.

Para crear una firma *DKIM* hay que pinchar sobre el botón *Create* y en la ventana *pop-up* que aparece hay que insertar el dominio que se desea. En este caso no se ha utilizado esta opción así que la configuración ha quedado de esta manera: (Mirar la imagen 22)



Settings	
View DNS Record Edit	
Enable DKIM Signing	No
Selector	
Sign all Outgoing Mail	No

Sign Domains	
Edit Create Remove	
Sign Domain ↑	Comment

Figura 22: Configuración establecida en la ventana *DKIM*

#### 4.3.9. *Whitelist*

Permite la creación de una lista blanca en la que se pueden añadir direcciones IP, dominios, expresiones regulares y direcciones de correo. En este caso la lista está vacía.

### 4.4. *SPAM Detector*

En la sección *SPAM Detector* se gestionan los mensajes que contienen SPAM. Tiene cuatro ventanas principales y son las siguientes:

#### 4.4.1. *Options*

Aquí está la configuración general de *SPAM Detector* y estas son sus partes:

- *Use auto-whitelists*: Permite el uso de listas blancas generadas automáticamente.
- *Use Bayesian filter*: Permite el uso de filtros basados en modelos de Naive Bayes.
- *Use RBL checks*: Permite activar la verificación mediante el *Real time blacklists*.
- *Use Razor2 checks*: Permite la verificación basada en el envío de SPAM de los usuarios. (18)
- *Max SPAM Size*: Se determina el tamaño máximo en bytes que pueden tener los mensajes.

- *Languages*: Se determina el idioma en el que tienen que estar los mensajes.
- *Backscatter Score*: *Proxmox* da una puntuación a los correos desviados y gracias a esto es capaz de detectar los mensajes con SPAM.(19)
- *Heuristic Score*: Hace lo mismo que el anterior punto pero para sacar la puntuación se basa en modelos de ebaluación heurísticos. (20)

En este caso se ha hecho la siguiente configuración: (Mirar la imagen 23)

Options		Quarantine	Status	Custom Scores
Edit				
Use auto-whitelists			Yes	
Use Bayesian filter			Yes	
Use RBL checks			Yes	
Use Razor2 checks			Yes	
Max Spam Size (bytes)			262144	
Languages			all	
Backscatter Score			0	
Heuristic Score			3	

Figura 23: Configuración puesta en la ventana de *Options* de *SPAM Detector*

#### 4.4.2. *Quarantine*

En esta ventana se configura la cuarentena que tienen que pasar los mensajes de SPAM. Estos son los siguientes elementos:

- *Lifetime*: Se determina la cantidad de días que un mensaje tiene que estar en cuarentena.

- *Authentication mode*: Se determina la forma para entrar a la interfaz de la cuarentena.
- *User Spamreport style*: Permite enviar a un apartado de autoridad los mensajes de SPAM atrapados. (21)
- *Quarantine Host*: Indica el *host* de la cuarentena.
- *Quarantine Port*: Indica el puerto que utiliza la cuarentena.
- *Email 'From'*: Se determina a que correo electrónico hay que enviar los reportes de SPAM diarios.
- *View images*: Permite cargar las imágenes de los mensajes en cuarentena.
- *Allow HREFs*: Permite el visionado de hiperlinks.

la configuración puesta en este apartado es el siguiente: (Mirar la imagen 24)

Options	Quarantine	Status	Custom Scores
Edit			
Lifetime (days)	7		
Authentication mode	Ticket		
User Spamreport Style	Verbose		
Quarantine Host	none		
Quarantine port	Default		
EMail 'From:'	none		
View images	Yes		
Allow HREFs	Yes		

Figura 24: Configuración establecida en la ventana *Quarantine*

#### 4.4.3. *Status*

En esta ventana se indica la situación del detector de SPAM, los que se están utilizando, cuando ha sido la última actualización, el identificador de la versión y si hay alguna actualización nueva.

En este proyecto se han utilizado los dos detectores que vienen por defecto. (Mirar la imagen 25)

Options	Quarantine	Status	Custom Scores
---------	------------	--------	---------------

Update Now
------------

Channel	Last Update	Version	Update Available
updates.spamassassin.org	Mon Aug 09 2021 12:09:25 GMT+0200 (hora de verano de Europa central)	1892106	No
kam.sa-channels.mcgrail.com	Mon Aug 09 2021 12:09:30 GMT+0200 (hora de verano de Europa central)	1628497873	No

Figura 25: Configuración puesta en la ventana *Status*

#### 4.4.4. *Custom Scores*

Aun que el conjunto de reglas establecido por *SpamAssassin* tiene una tasa de detección bastante alta a veces algunos medios necesitan reglas específicas y de ahí se puede sacar beneficio.  
En este caso no se ha configurado nada.

### 4.5. *Virus Detector*

En la sección *Virus Detector* se gestionan los correos que contienen algún tipo de malware. Estas son las tres ventanas que tiene:

#### 4.5.1. *Options*

En esta ventana aparece la configuración general de *Virus Detector*, estos son sus elementos:

- *Block encrypted archives and documents*: Permite bloquear ficheros encriptados.
- *Max recursion*: Permite el análisis recursivo de los ficheros.
- *Max files*: Se determina la cantidad máxima de ficheros que puede contener un mensaje.
- *Max file size*: Se determina el peso máximo en bytes que puede tener un fichero.
- *Max scan size*: Se determina el tamaño máximo en bytes que se pueden escanear de cada fichero.
- *Max credit card numbers*: Se determina el número máximo de tarjetas de crédito que pueden haber.

En este apartado se ha puesto la siguiente configuración: (Mirar la imagen 26)

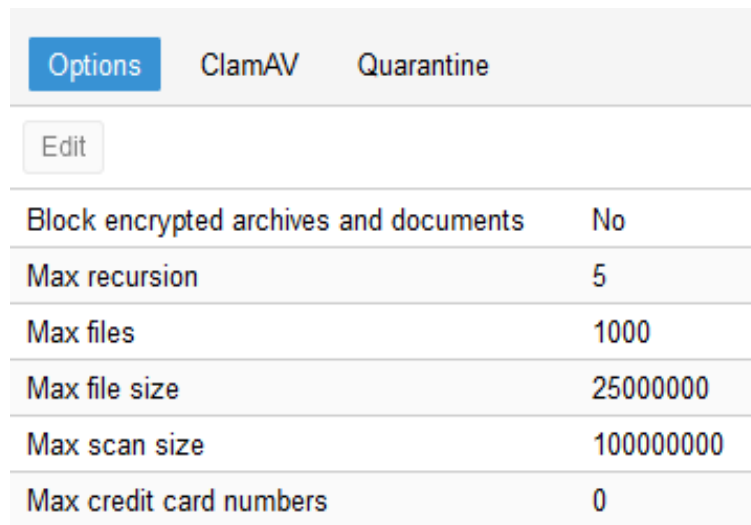


Figura 26: Configuración puesta en la ventana *Options* de *Virus Detector*

#### 4.5.2. *ClamAV*

En esta ventana se configura el detector de malwares *ClamAV*. El detector se autogestiona y lo único que se permite hacer es pulsar el botón *Update Now* para actualizarlo.

#### 4.5.3. *Quarantine*

En esta ventana se gestiona la cuarentena que tienen que pasar los mensajes que contienen algún malware. Estos son los elementos que lo componen:

- *Lifetime*: Se determina la cantidad de días que un mensaje tiene que estar en cuarentena.
- *View Images*: Permite cargar las imágenes de los mensajes en cuarentena.
- *Allow HREFs*: Permite el visionado de hiperlinks.

La configuración puesta en este apartado es el siguiente: (Mirar la imagen 27)

Options

ClamAV

Quarantine

Edit

Lifetime (days)	7
View images	Yes
Allow HREFs	Yes

Figura 27: Configuración establecida en la ventana *Quarantine*

## 5. Gestión de usuarios

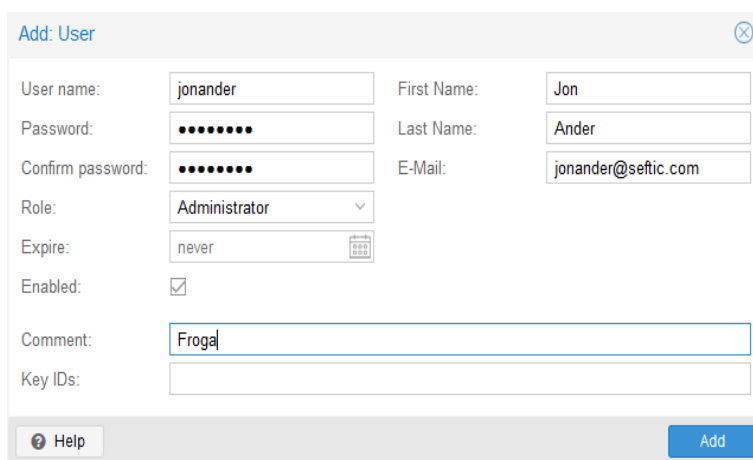
Al acabar con la configuración se van a crear y a gestionar los usuarios que pueden utilizar *Proxmox Mail Gateway*, para ello se va a utilizar la sección *User Managment* que contiene las siguientes tres ventanas:

### 5.0.1. Local

Los usuarios locales pueden utilizar *Proxmox Mail Gateway* para hacer login, estos son los roles que pueden coger:

- *Administrator*: Puede gestionar la configuración de *Proxmox Mail Gateway* menos la configuración de red y las actualizaciones.
- *Quarantine Manager*: Solo puede gestionar las cuarentenas y las listas blancas y negras.
- *Auditor*: Solo puede ver a configuración y los datos.
- *Helpdesk*: Es una mezcla de los roles *Quarantine Manager* y *Auditor*.

Para añadir un usuario local hay que añadir los siguientes datos: (Mirar la imagen 28)



The image shows a 'Add: User' form with the following fields and values:

Field	Value
User name:	jonander
First Name:	Jon
Password:	••••••
Last Name:	Ander
Confirm password:	••••••
E-Mail:	jonander@seftic.com
Role:	Administrator
Expire:	never
Enabled:	<input checked="" type="checkbox"/>
Comment:	Froga
Key IDs:	

Buttons: ? Help, Add

Figura 28: Ventana *pop-up* para añadir un usuario local

### 5.0.2. LDAP

En esta ventana se añaden los usuarios LDAP, gracias a esto se pueden crear reglas específicas para un usuario o grupo.

Para añadir un nuevo usuario LDAP hay que añadir los siguientes datos, los cuadrados en rojo son elementos que hay que añadir por obligación. (Mirar la imagen 29)

**Add: LDAP Profile**

Profile Name:

Protocol: LDAP

Server:

Server:

Port: Default

User name:

Password:

Comment:

Enable: ☒

Base DN:

Base DN for Groups:

Email attribute name(s):

Account attribute name:

LDAP filter:

Group objectclass:

[Help](#) [Add](#)

Figura 29: Ventana *pop-up* para añadir un usuario LDAP

### 5.0.3. Fetchmail

En esta ventana se pueden añadir direcciones de correo para ello se piden los siguientes datos, los cuadrados en rojo indican que esos son datos que hay que añadir obligatoriamente. (Mirar la imagen 30)

**Edit: Fetchmail**

Server:

Protocol: pop3

Port: 110

Username:

Password:

Deliver to:

Enabled: ☒

Interval: 1

Use SSL: ☐

Keep old mails: ☐

[Help](#) [OK](#) [Reset](#)

Figura 30: Ventana *pop-up* para añadir un nuevo correo



## 6. Crear reglas

Antes de crear reglas hay que crear diferentes elementos en el apartado *Mail Filter*:

### 6.1. Listas

Para crear una lista se va a utilizar el apartado *Who Objects*. Ahí se va a clicar en el botón *Create* para crear una nueva lista añadiendo un nombre y una pequeña descripción. (Mirar la imagen 31). Después de eso pulsando en el botón *Add* se pueden añadir elementos a la lista eligiendo el tipo en un desplegable que sale y añadiendo los datos en la ventana *pop-up* que sale. En este caso se ha añadido una dirección de correo. (Mirar la imagen 32)

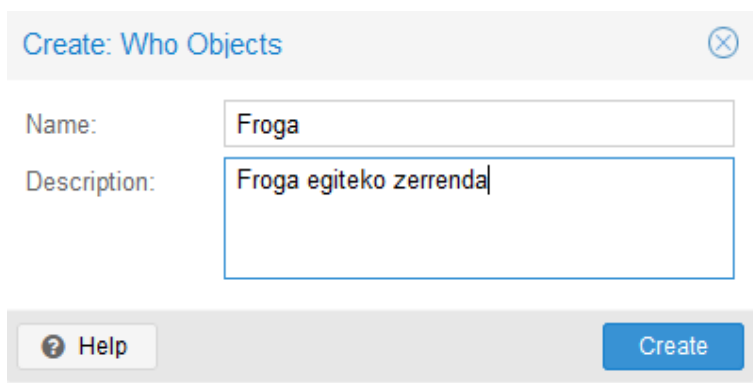


Figura 31: Ventana *pop-up* para crear una lista

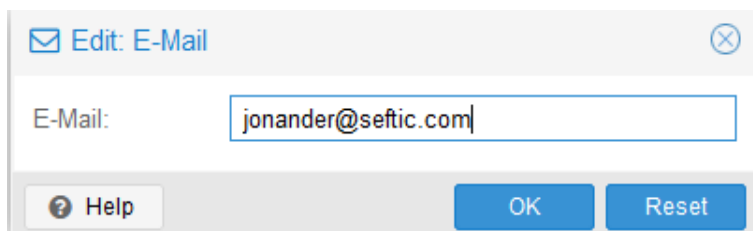


Figura 32: Ventana *pop-up* para añadir un elemento a la lista

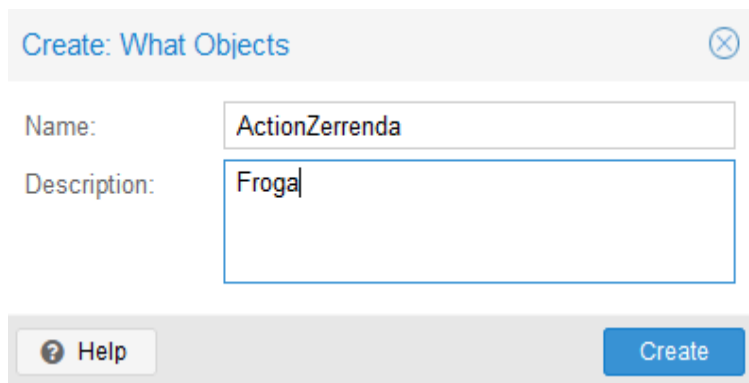
### 6.2. Objetos

En este apartado se van a determinar los objetos *What* explicados en el punto 1.3, para ello se va a utilizar el apartado *What Object*. El servidor por defecto trae las siguientes configuraciones, son las siguientes:

- *Dangeorus content*: Los sobe elementos que trae este elemento se pueden dividir en dos tipos, por un lado los que analizan la cabecera *Content Type* y por el otro los que analizan los nombres de los ficheros. Los del primer tipo cazan el mensaje cuando el *content type* de la cabecera tiene uno de los siguientes valores: *application/javascript*, *application/x-executable*, *application/x-java*, *application/x-ms-dos-executable*, *message/-partial*. En cambio los del segundo tipo cazan el mensaje cuando el nombre de los ficheros contiene uno de estos elementos: *vbs*, *pif*, *lnk*, *shs*, *shb*.
- *Images*: Este elemento captura los mensajes que contengan algún tipo de imagen.
- *Multimedia*: Este elemento captura los mensajes que contengan algún tipo de audio o video.
- *Office Files*: Este elemento analiza el *Content Type* de la cabecera y captura los ficheros que normalmente se utilizan en las oficinas, ficheros excell, word, powerpoint...
- *SPAM (Level 10, 5 or 3)*: Como se ha explicado en el punto 4.4.1 a cada correo de SPAM se le asigna un *score* o puntuación y a partir de eso crear unos niveles. Estos elementos permiten filtrar los mensajes con una puntuación superior a la establecida.
- *Virus*: Este elemento permite habilitar el *Virus Detector* configurado en el punto 4.5.

Para añadir un elemento *Action* se seguirán los siguientes pasos:

- Después de pulsar el botón *Create* aparecerá una ventana *pop-up* y ahí se pondrá el nombre y una pequeña descripción. (Mirar la imagen 33)



The image shows a 'Create: What Objects' dialog box. It has a title bar with a close button. Inside, there are two text input fields: 'Name' with the value 'ActionZerrenda' and 'Description' with the value 'Froga'. At the bottom, there is a 'Help' button with a question mark icon and a 'Create' button.

Figura 33: Ventana *pop-up* para crear una lista en el apartado *Action*

- Al crearlo, para añadir elementos se pulsará el botón *Add* y en el menú que aparece se seleccionará que tipo de elemento se quiere añadir. En este caso un *SPAM Filter*.
- Una vez elegido el tipo de elemento que se quiere añadir aparecerá una ventana *pop-up* y como en este caso se ha elegido un *SPAM Filter* se tendrá que insertar que nivel se quiere. (Mirar la imagen 34)

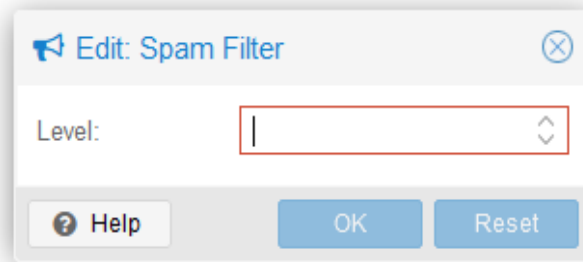


Figura 34: Ventana *pop-up* para añadir un *SPAM Filter* a la lista

### 6.3. Acciones

En este apartado se gestiona el elemento *Action*, en otras palabras, lo que tiene que hacer el servidor de *Proxmox Mail Gateway* cuando ha atrapado un mensaje. El servidor trae por defectos diferentes acciones y son las siguientes:

- *Accept*: Permite pasar el mensaje capturado.
- *Attachment Quarantine*: Borra los ficheros adjuntos y mete el mensaje en cuarentena.
- *Block*: Bloquea el mensaje.
- *Disclaimer*: Crea un *disclaimer*.
- *Modify SPAM level*: Clasifica el mensaje como SPAM añadiendo un elemento a su cabecera.
- *Modify SPAM Subject*: Clasifica el mensaje como SPAM modificando su contenido.
- *Notify Admin*: Le manda un aviso al administrador.
- *Notify Sender*: Le manda un aviso al remitente.
- *Quarantine*: Mete el mensaje en cuarentena.

- *Remove attachment*: Elimina los archivos adjuntos (todos o solo los seleccionados) del mensaje.

Para crear una nueva acción hay que pulsar el botón *Add* y del menú que sale hay que seleccionar que tipo de acción se quiere, en este caso se va a enviar un aviso. Una vez elegido el tipo de acción hay que añadir los datos requeridos. (Mirar la imagen 35)

**Create: Notification**

Name: Froga

Comment: Froga Akzioa

Receiver: \_\_ADMIN\_\_

Subject: Notification: \_\_SUBJECT\_\_

Body: Proxmox Notfication:  
 Sender: \_\_SENDER\_\_  
 Receiver: \_\_RECEIVERS\_\_  
 Targets: \_\_TARGETS\_\_  
 Subject: \_\_SUBJECT\_\_  
 Matching Rule: \_\_RULE\_\_  
 \_\_RULE\_INFO\_\_  
 \_\_VIRUS\_INFO\_\_  
 \_\_SPAM\_INFO\_\_

Attach orig. Mail: ☐

[? Help](#) [Create](#)

Figura 35: Ventana *pop-up* para crear una nueva acción

## 6.4. Periodo de tiempo

En este apartado se gestiona el elemento *When*, las horas en las que el servidor *Proxmox Mail Gateway* está en funcionamiento. Por defecto trae una única configuración, el horario de oficina (de 8:00 a 16:00). Usando una lista creada por defecto se va a añadir un nuevo horario, para ello se pulsará el botón

*Add* y en la ventana que sale se añadirán la hora de inicio (*Start Time*) y la hora final (*End Time*). (Mirar la imagen 36)

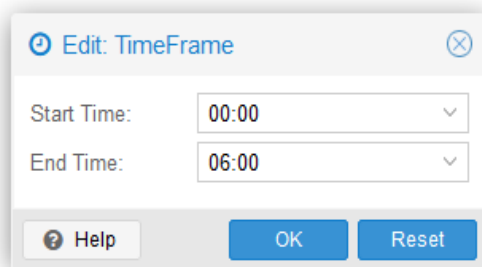


Figura 36: Ventana *pop-up* para añadir una nueva franja horaria

## 6.5. Crear normas

Una vez creado y configurado todo lo anterior se va a crear una nueva norma, para ello se va a pinchar en el botón *Add* en el apartado *Mail Filter*. Al clickar sobre el botón aparecerá una ventana para añadir el nombre de la regla, su prioridad (de 0 a 99, siendo el 0 la prioridad mínima y el 99 la máxima), la dirección (Entrada o salida) y la opción de activación. (Mirar la imagen 37) Una vez creada la norma hay que declarar sus parámetros, para ello se va a utilizar el menú de la parte derecha. En este caso se ha utilizado la siguiente configuración: (Mirar la tabla 3)

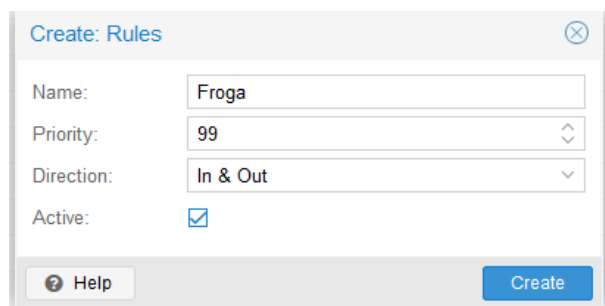


Figura 37: Ventana *pop-up* para la creación de una nueva norma

Atributo	Valor
From (Who)	jasuamiranda1998@gmail.com
To (Who)	root@jonander.xyz
Action	Block
What	Image
When	Horario de oficina (8:00 - 16:00)

Cuadro 3: Atributos de las normas y sus valores

## 6.6. Prueba

Para probar la norma creada en el punto anterior se va a enviar un mensaje desde el correo del atributo *From* al correo del atributo *To*. (Mirar la imagen 38)

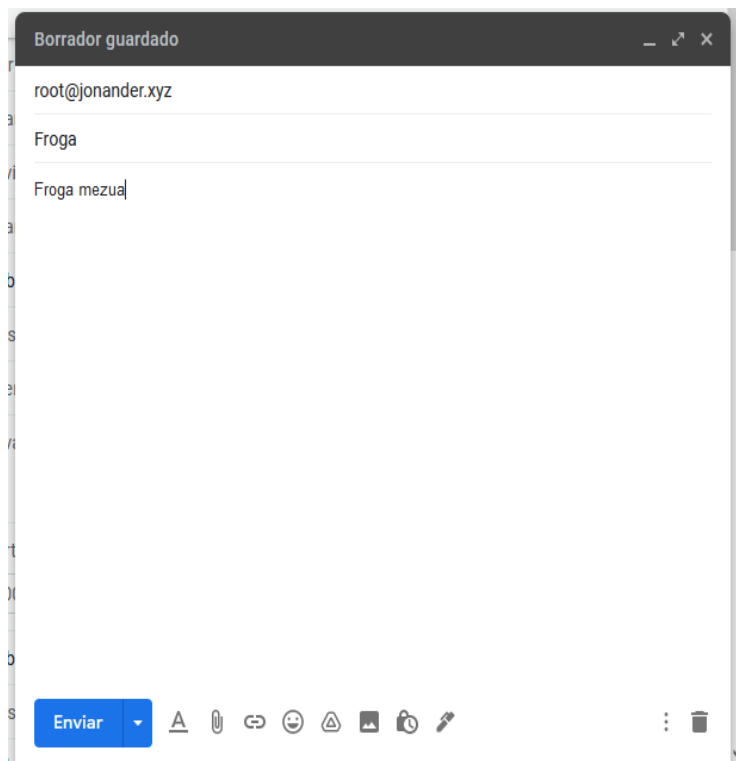


Figura 38: Mensaje enviado desde *From* helbidetik bidalitako mezua

Para ver si ha funcionado hay que mirar el buzón de entrada de la dirección de correo establecida en el atributo *To* y ver el correo ha llegado o no. (Mirar la imagen 39)

```
root@Proxmox-1: ~  
O 21 Jon Ander Asua Mir 2021-08-11 11:45 1452/109823 Froga  
N 22 Jon Ander Asua Mir 2021-08-11 11:47 1452/109824 Froga  
P 0  
held 22 messages in /root/Maildir  
root@Proxmox-1:~# s-nail  
s-nail version v14.9.15. Type '?' for help  
/root/Maildir: 22 messages 4 unread  
P 0  
O 1 cowrie@jonander.xy 2021-07-22 10:26 14/552 *** SECURITY information for Proxmox-1 ***  
O 2 cowrie@jonander.xy 2021-07-22 10:31 14/575 *** SECURITY information for Proxmox-1 ***  
O 3 cowrie@jonander.xy 2021-07-22 10:36 14/588 *** SECURITY information for Proxmox-1 ***  
O 4 cowrie@jonander.xy 2021-07-22 10:37 14/588 *** SECURITY information for Proxmox-1 ***  
O 5 S Soporte Seftic 2021-07-23 10:20 2513/191277 Asunto: froga  
O 6 kippo@jonander.xyz 2021-07-23 13:25 14/565 *** SECURITY information for Proxmox-1 ***  
O 7 kippo@jonander.xyz 2021-07-23 13:48 14/546 *** SECURITY information for Proxmox-1 ***  
O 8 kippo@jonander.xyz 2021-07-30 09:35 14/648 *** SECURITY information for Proxmox-1 ***  
O 9 Cron Daemon 2021-08-02 11:22 20/596 Cron <root@Proxmox-1> echo 'hola'  
O 10 Cron Daemon 2021-08-03 05:00 24/811 Cron <root@Proxmox-1> apt clean  
O 11 Cron Daemon 2021-08-03 05:00 25/757 Cron <root@Proxmox-1> apt autoclean  
O 12 Cron Daemon 2021-08-03 05:00 26/821 Cron <root@Proxmox-1> apt autoremove  
O 13 Cron Daemon 2021-08-03 05:00 33/1077 Cron <root@Proxmox-1> apt upgrade  
O 14 Cron Daemon 2021-08-03 05:00 71/4918 Cron <root@Proxmox-1> apt update  
O 15 Cron Daemon 2021-08-03 11:22 20/596 Cron <root@Proxmox-1> echo 'hola'  
O 16 Jon Ander 2021-08-03 12:53 4484/332108 Prueba que sé que no va a funcionar  
O 17 Jon Ander 2021-08-04 12:51 4485/332158 Hola  
U 18 Jon Ander Asua Mir 2021-08-10 11:32 72/4132 Froga  
U 19 Jon Ander Asua Mir 2021-08-11 11:46 72/4140 Froga  
U 20 Jon Ander Asua Mir 2021-08-11 11:39 6793/521124 Froga 2  
O 21 Jon Ander Asua Mir 2021-08-11 11:45 1452/109823 Froga  
U 22 Jon Ander Asua Mir 2021-08-11 11:47 1452/109824 Froga
```

Figura 39: Buzón de entrada del receptor

## 7. Administración

Para administrar el sistema se va a utilizar la sección *Administration*, tiene las siguientes ventanas:

### 7.1. *Administration*

En esta ventana aparecen los elementos más generales para la administración, son los siguientes:

#### 7.1.1. *Status*

En este apartado aparece la situación del servidor mediante dos gráficos. En el primero aparece el uso de CPU respecto al tiempo y en el segundo la carga del servidor respecto al tiempo. Aparte de esto da la opción para reiniciar y apagar el servidor o acceder a su consola.

#### 7.1.2. *Services*

En esta sección se indican los servicios que tiene *Proxmox Mail Gateway* y su situación. Los servicios son los siguientes:

- *Clamav-daemon*: Daemon del detector de malwares *Clam AV*.
- *Clamav-freshclam*: Actualizador de la base de datos del detector de malwares *Clam AV*.
- *Fetchmail*: Script inicial para el daemon de *Fetchmail*.
- *Pmg-daily*: Actividad diaria de *Proxmox Mail Gateway*.
- *Pmg-hourly*: Actividad horaria de *Proxmox Mail Gateway*.
- *Pmg-smtp-filter*: Daemon del filtro de SMTP.
- *Pmgdaemon*: Daemon de la API de *Proxmox Mail Gateway*.
- *Pmgmirror*: Daemon del espejo de la base de datos de *Proxmox Mail Gateway*.
- *Pmgpolicy*: Daemon de *Proxmox Mail Gateway Policy*.
- *Pmgproxy*: API de *Proxmox Mail Gateway*.
- *Pmgreport*: Manda a diario informes del sistema.
- *Pmgspamreport*: Manda a diario informes de SPAM del sistema.
- *Pmgtunnel*: Daemon del túnel *Cluster* de *Proxmox Mail Gateway*.
- *Postfix*: Agente del servidor *Postfix*.



- *Postgres*: Cluster de PostgreSQL.
- *Rsyslog*: Servicio de login del sistema.
- SSH: Servidor SSH.
- *Systemd-timesyncd*: Sincronización con la hora de la red.

Aparte de esto permite iniciar, terminar, reiniciar o ver los registros de los servicios anteriormente mencionados.

### 7.1.3. Updates

En este apartado se gestionan las actualizaciones del servidor. Aparece el nombre, el identificador de la versión actual y el de la nueva y una pequeña descripción de cada paquete de actualización. (Mirar la imagen 40)

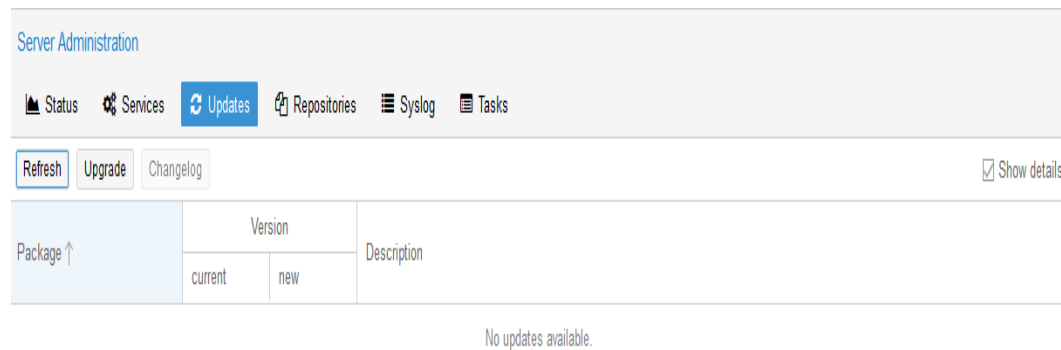


Figura 40: Informe de actualización de paquetes

### 7.1.4. Repositories

En este apartado se determina de donde tiene que coger el servidor los paquetes de actualización. Hay tres tipos de paquetes:

- Paquetes compartidos: En este grupo entran todos los paquetes que comparten los sistemas *Debian*, por ejemplo los paquetes descargados del link <http://deb.debian.org/debian>.
- Paquetes sin suscripción: En este grupo entran los paquetes que no necesitan una suscripción de pago a *Proxmox Mail Gateway*, se descargan del siguiente link: <http://download.proxmox.com/debian/pmg>

- Paquetes para suscriptores: En este grupo entran los paquetes para los que se necesita una suscripción de pago a *Proxmox Mail Gateway*, se descargan del siguiente link: <http://enterprise.proxmox.com/debian/pmg>

Aparte permite añadir nuevos repositorios, en este caso se han añadido los siguientes a la lista: (Mirar la imagen 41))

APT Repositories							
<div> <div>Reload</div> <div>Add</div> <div>Disable</div> </div>							
Enabled	Types	URIs	Suites	Components	Options	Origin	Comment
File: /etc/apt/sources.list (7 repositories)							
<input checked="" type="checkbox"/>	deb	<a href="http://ftp.es.debian.org/debian">http://ftp.es.debian.org/debian</a>	bullseye	main contrib		Debian	
<input checked="" type="checkbox"/>	deb	<a href="http://ftp.es.debian.org/debian">http://ftp.es.debian.org/debian</a>	bullseye-updates	main contrib		Debian	
<input checked="" type="checkbox"/>	deb	<a href="http://security.debian.org">http://security.debian.org</a>	bullseye-security	main contrib		Debian	security updates
<input checked="" type="checkbox"/>	deb	<a href="http://download.proxmox.com/debian/pmg">http://download.proxmox.com/debian/pmg</a>	bullseye	pmg-no-subscription		Proxmox	PMG pmg-no-subscripti...
<input checked="" type="checkbox"/>	deb	<a href="http://deb.debian.org/debian">http://deb.debian.org/debian</a>	bullseye	non-free		Debian	Other Repository Sources
<input checked="" type="checkbox"/>	deb	<a href="http://security.debian.org/debian-security">http://security.debian.org/debian-security</a>	bullseye-security	non-free		Debian	
<input checked="" type="checkbox"/>	deb	<a href="http://deb.debian.org/debian/">http://deb.debian.org/debian/</a>	bullseye-updates	non-free		Debian	

Figura 41: Repositorios que tiene *Proxmox Mail Gateway*

### 7.1.5. Syslog

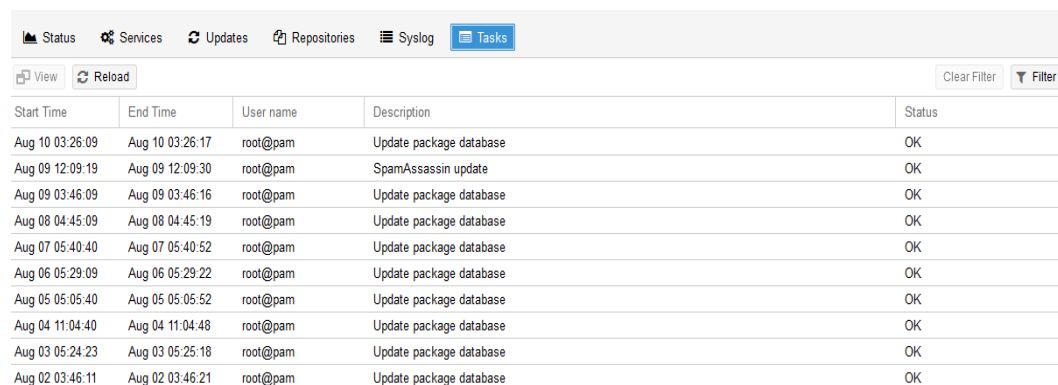
En este apartado aparece el registro del sistema. Hay dos formas para verlo, en la primera el registro sale en vivo, actualizandose en todo momento, y en el segundo se puede revisar el registro determinando una franja horaria. (Mirar la imagen 42)

<div> <div>Status</div> <div>Services</div> <div>Updates</div> <div>Repositories</div> <div>Syslog</div> <div>Tasks</div> </div>			
<div> <div>Live Mode</div> <div>Select Timespan</div> <div>Since: 2021-08-07</div> </div>			
<pre> Aug 10 13:09:54 pxx pmgmirror[1002]: starting cluster synchronization Aug 10 13:09:54 pxx pmgmirror[1002]: cluster synchronization finished (0 errors, 0.01 seconds (files 0.00, database 0.01, config 0.00)) Aug 10 13:10:54 pxx pmgpolicy[1001]: starting policy database maintenance (greylist, rbl) Aug 10 13:10:54 pxx pmgpolicy[1001]: end policy database maintenance (14 ms, 2 ms) Aug 10 13:11:04 pxx pmg-smtp-filter[59120]: starting database maintenance Aug 10 13:11:04 pxx pmg-smtp-filter[59120]: end database maintenance (8 ms) Aug 10 13:11:54 pxx pmgmirror[1002]: starting cluster synchronization Aug 10 13:11:54 pxx pmgmirror[1002]: cluster synchronization finished (0 errors, 0.01 seconds (files 0.00, database 0.01, config 0.00)) Aug 10 13:13:04 pxx pmgpolicy[1001]: starting policy database maintenance (greylist, rbl) Aug 10 13:13:04 pxx pmg-smtp-filter[59120]: starting database maintenance Aug 10 13:13:05 pxx pmg-smtp-filter[59120]: end database maintenance (13 ms) Aug 10 13:13:05 pxx pmgpolicy[1001]: end policy database maintenance (25 ms, 2 ms) </pre>			

Figura 42: Forma del registro

### 7.1.6. *Tasks*

En este apartado se muestra el registro de cada tarea hecha por los usuarios. Por cada registro aparece la hora de inicio y final, el usuario, una pequeña descripción y la situación. (Mirar la imagen 43)



Start Time	End Time	User name	Description	Status
Aug 10 03:26:09	Aug 10 03:26:17	root@pam	Update package database	OK
Aug 09 12:09:19	Aug 09 12:09:30	root@pam	SpamAssassin update	OK
Aug 09 03:46:09	Aug 09 03:46:16	root@pam	Update package database	OK
Aug 08 04:45:09	Aug 08 04:45:19	root@pam	Update package database	OK
Aug 07 05:40:40	Aug 07 05:40:52	root@pam	Update package database	OK
Aug 06 05:29:09	Aug 06 05:29:22	root@pam	Update package database	OK
Aug 05 05:05:40	Aug 05 05:05:52	root@pam	Update package database	OK
Aug 04 11:04:40	Aug 04 11:04:48	root@pam	Update package database	OK
Aug 03 05:24:23	Aug 03 05:25:18	root@pam	Update package database	OK
Aug 02 03:46:11	Aug 02 03:46:21	root@pam	Update package database	OK

Figura 43: Estructura de las tareas

### 7.2. *SPAM Quarantine*

En esta ventana aparece el registro de los mensajes clasificados como SPAM. En cada línea del registro aparece quien es el remitente, el mensaje, el *score*, el tamaño en KBs y cuando se ha hecho. (Mirar la imagen 44)  
Aparte, se pueden buscar direcciones de correo o mensajes específicos.

**Hay que especificar que el correo para hacer las pruebas no era un correo que mande SPAM**

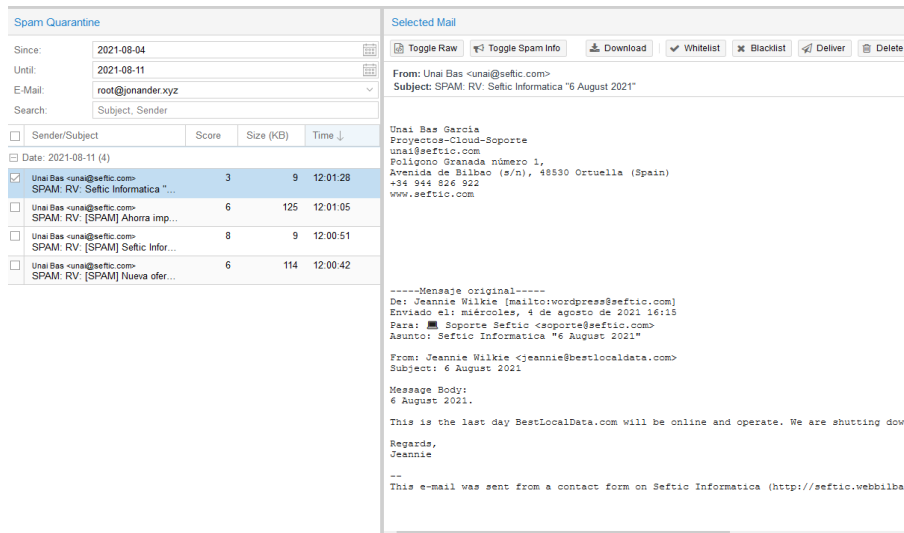


Figura 44: Estructura de un registro de SPAM

### 7.3. Attachment Quarantine

En esta ventana aparece el registro de los mensajes que contienen ficheros adjuntos sospechosos y que han sido capturados. Por cada entrada aparece quien ha sido el emisor, el mensaje, el *score*, el tamaño en KBs y cuando se ha hecho. (Mirar la imagen 45)

Aparte, se pueden buscar direcciones de correo o mensajes específicos.

**Hay que especificar que el correo para hacer las pruebas no era un correo que mande archivos adjuntos sospechosos**

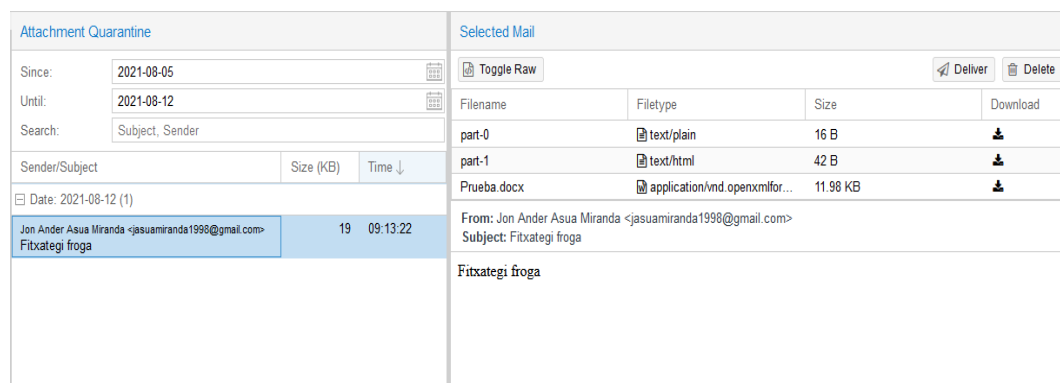


Figura 45: Estructura del registro del filtro de archivos adjuntos

#### 7.4. *Virus Quarantine*

En esta ventana aparece el registro de los mensajes que han sido clasificados como mensajes que tienen un malware. Sigue la misma estructura que los dos registros anteriormente nombrados, así que por cada línea del registro aparece quien ha sido el remitente, el mensaje, el *score*, el tamaño en KBs y cuando se ha hecho.

Aparte de esto, al igual que en los registros del filtro de SPAM y de archivos adjuntos, se puede buscar por franja horaria, email o mensajes específicos.

#### 7.5. *User Whitelist*

En esta sección aparece la lista blanca de cada usuario, la lista de direcciones en las que el usuario confía. Para añadir un elemento a la *whitelist* basta con clicar el botón *Add* y meter la dirección de correo.

#### 7.6. *User Blacklist*

En esta sección se sitúa la lista negra de cada usuario, una lista que se compone de direcciones de correo las cuales no tienen el permiso para enviar mensajes al usuario anteriormente nombrado. Para añadir un elemento a la *whitelist* basta con clicar el botón *Add* y meter la dirección de correo.

#### 7.7. *Tracking Center*

En este apartado aparece el registro del sistema, pero a diferencia del registro mencionado en el punto 7.1.5 el que hay en *Tracking Center* permite el filtrado por franja horaria, emisor, receptor y filtro (SPAM, Malware,...). (Mirar la imagen 46)

Tracking Center

Sender:  Start: 2021-08-03 07:57

Receiver: root@jonander.xyz End: 2021-08-24 00:00

Filter:  ☒ Include Empty Senders ☐ Include Greylist

Search

	Time ↑	From	To	Status
⊞	Aug 04 12:22:10	jonander@seftic.com	root@jonander.xyz	✔ accepted/delivered
⊞	Aug 04 12:51:25	jonander@seftic.com	root@jonander.xyz	✔ accepted/delivered
⊞	Aug 10 12:04:51	jasuamiranda1998@gmail.com	root@jonander.xyz	✔ accepted/delivered
⊞	Aug 11 11:14:35	jasuamiranda1998@gmail.com	root@jonander.xyz	✔ accepted/delivered
⊞	Aug 11 11:39:52	jasuamiranda1998@gmail.com	root@jonander.xyz	✔ accepted/delivered
⊞	Aug 11 11:43:12	jasuamiranda1998@gmail.com	root@jonander.xyz	✖ blocked
⊞	Aug 11 11:45:29	jasuamiranda1998@gmail.com	root@jonander.xyz	✔ accepted/delivered
⊞	Aug 11 11:47:51	jasuamiranda1998@gmail.com	root@jonander.xyz	✔ accepted/delivered
⊞	Aug 11 12:00:46	unai@seftic.com	root@jonander.xyz	🛡 quarantine
⊞	Aug 11 12:00:52	unai@seftic.com	root@jonander.xyz	🛡 quarantine
⊞	Aug 11 12:01:09	unai@seftic.com	root@jonander.xyz	🛡 quarantine
⊞	Aug 11 12:01:29	unai@seftic.com	root@jonander.xyz	🛡 quarantine
⊞	Aug 11 12:30:45	unai@seftic.com	root@jonander.xyz	🛡 quarantine
⊞	Aug 12 00:05:09		root@jonander.xyz	✔ queued/delivered
⊞	Aug 12 09:05:26	jasuamiranda1998@gmail.com	root@jonander.xyz	✖ blocked
⊞	Aug 12 09:09:08	jasuamiranda1998@gmail.com	root@jonander.xyz	✔ accepted/delivered
⊞	Aug 12 09:13:23	jasuamiranda1998@gmail.com	root@jonander.xyz	✔ accepted/delivered
⊞	Aug 18 09:44:25	seftic@seftic.com	root@jonander.xyz	🛡 quarantine
⊞	Aug 19 00:05:20		root@jonander.xyz	✔ queued/delivered
⊞	Aug 20 13:08:21	seftic@seftic.com	root@jonander.xyz	🛡 quarantine
⊞	Aug 21 00:05:21		root@jonander.xyz	✔ queued/delivered

Figura 46: Estructura del registro de *Tracking Center*

## 7.8. Queues

En este apartado se gestiona las filas de correo explicadas en el punto 2.2, tiene dos ventanas principales y son las siguientes:

### 7.8.1. Summary

En esta ventana aparecen los elementos más generales para la gestión de las filas. Aparecen los correos no enviados ordenados por dominio y cuanto tiempo llevan en la fila, aparte ofrece tres opciones:

- *Flush Queue*: El servidor intenta volver a enviar los mensajes de la fila.
- *Delete All Messages*: Borra todos los mensajes que componen la fila.
- *Discard Address Verification Database*: Borra el caché de verificación del receptor.

Su estructura es la siguiente, en este caso la fila está vacía. (Mirar la imagen 47)

Queue Administration

Summary Deferred Mail

Flush Queue Delete all Messages Discard address verification database

Domain	Total	5m	10m	20m	40m	80m	160m	320m	640m	1280m	1280m+
TOTAL	0	0	0	0	0	0	0	0	0	0	0

Figura 47: Estructura del resumen de la fila de correo

### 7.8.2. *Deferred Mail*

En esta ventana se pueden ver los mensajes pospuestos y dando la información del receptor y el emisor se puede ser por que ha sido enviado este correo a la fila de correos mencionada en el punto anterior.

Aparte de todo esto, se pueden ver las cabeceras del emisor y receptor, incluso borrar el mensaje también.

## 8. *Dashboard*

En esta sección aparece información sobre la situación del servidor de *Proxmox Mail Gateway*. Está compuesta por cinco cuadrados generlas y cada uno ofrece una información diferente. (Mirar la imagen 48)

- *Email volume*: En este cuadrado aparecen dos gráficos, el primero está contruido sobre la relación mensaje/minuto y el segundo sobre la relación mensaje de SPAM/minuto.
- *Email processing*: En este apartado aparece el tiempo de procesado de cada mensaje (ya sea de salida o de entrada) y de tráfico.
- *Subscription*: En este punto aparece información sobre la suscripción al servicio de *Proxmox Mail Gateway*.
- Información del servidor: En esta ventana aparece la siguiente información: Uso de la memoria RAM, ocupación del disco duro, retraso en la Entrada/Salida, uso de SWAP, media de carga, versión del kernel y la situación de los repositorios.
- *Top receivers*: En este apartado se muestran los correos con mayor carga de mensaje.

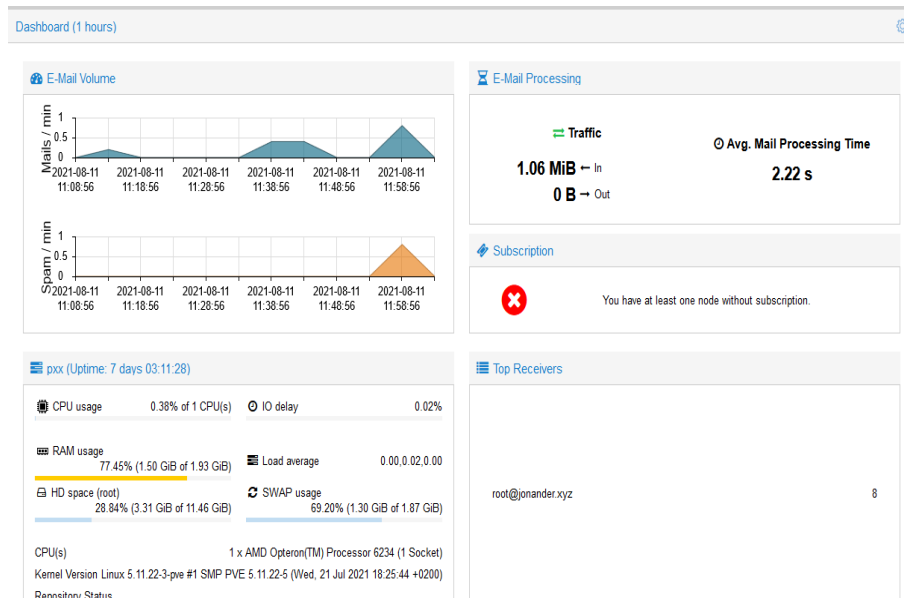
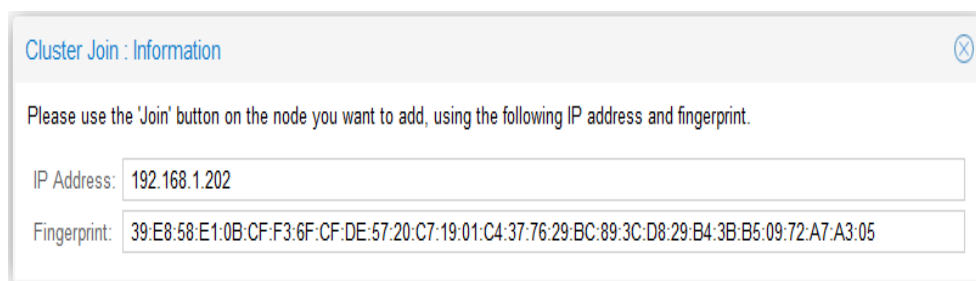


Figura 48: Estructura de la sección *Dashboard*



## 9. Crear y gestionar un *Cluster*

Antes de crear un *cluster* hay que crear como mínimo dos servidores que tengan instalado *Proxmox Mail Gateway*. Una vez se tengan esos servidores hay que pulsar el botón *Add* en el apartado *Cluster* en el servidor que se quiere que sea el *master*. Una vez creado este nodo principal se pulsará sobre el botón *Add* otra vez para guardar la dirección IP y el *fingerprint* que aparecen en la ventana *pop-up*. (Mirar la imagen 49)



Cluster Join : Information

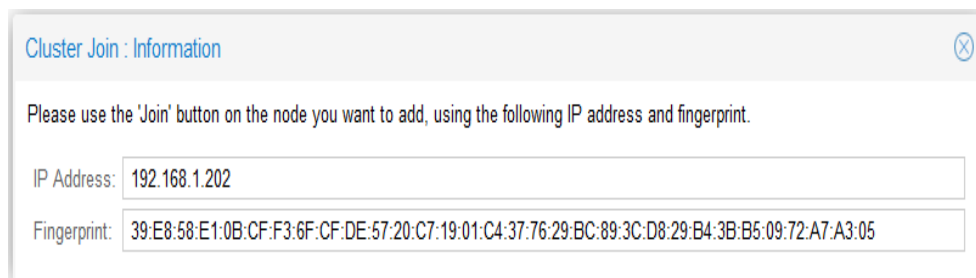
Please use the 'Join' button on the node you want to add, using the following IP address and fingerprint.

IP Address: 192.168.1.202

Fingerprint: 39:E8:58:E1:0B:CF:F3:6F:CF:DE:57:20:C7:19:01:C4:37:76:29:BC:89:3C:D8:29:B4:3B:B5:09:72:A7:A3:05

Figura 49: La dirección IP y el *fingerprint* del *cluster master*

Para añadir otros servidores *Proxmox* al *cluster*, hay que clickar en el botón *Join* en cada servidor y en la ventana que sale añadir la dirección IP y el *fingerprint* anteriormente copiados añadiéndole la contraseña de 'root' del servidor que tiene el rol de *master*. (Mirar la imagen 50)



Cluster Join : Information

Please use the 'Join' button on the node you want to add, using the following IP address and fingerprint.

IP Address: 192.168.1.202

Fingerprint: 39:E8:58:E1:0B:CF:F3:6F:CF:DE:57:20:C7:19:01:C4:37:76:29:BC:89:3C:D8:29:B4:3B:B5:09:72:A7:A3:05

Figura 50: Ventana *pop-up* que sale en un nodo

Al acabar esto la ventana de la API se va a actualizar y se va a comprobar que el *cluster* está bien hecho. Si aparece la misma estructura que aparece en la imagen significa que el *cluster* está bien hecho. (Mirar la imagen 51)

Cluster Join : Information

Please use the 'Join' button on the node you want to add, using the following IP address and fingerprint.

IP Address:

192.168.1.202

Fingerprint:

39:E8:58:E1:0B:CF:F3:6F:CF:DE:57:20:C7:19:01:C4:37:76:29:BC:89:3C:D8:29:B4:3B:B5:09:72:A7:A3:05

Figura 51: Estructura de un *cluster*

## 10. Estadísticas

En esta sección aparecen los datos estadísticos principales del servidor *Proxmox Mail Gateway*. En este primer apartado que aparece hay tres gráficos y son los siguientes:

- *Total Mail Count*: En este gráfico aparecen todos los mensajes analizados por el servidor, bajo él aparecen los siguientes datos: Número total de correos analizados, mensajes de entrada y salida, cuantos malwares ha cazado y el tráfico de correo. (Mirar la imagen 52)

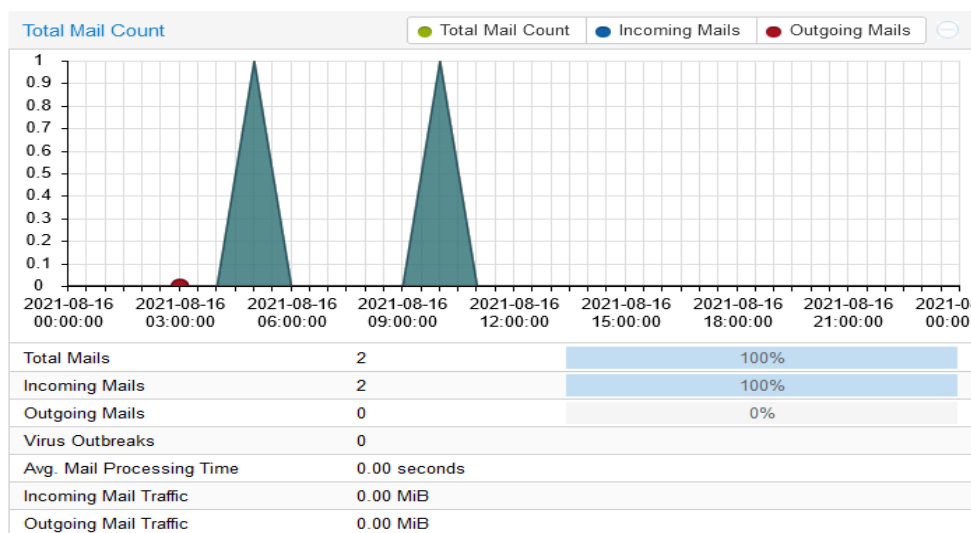


Figura 52: Gráfico de *Total Mail Count*

- *Incoming Mails*: En este gráfico aparecen todos los mensajes que llegan al servidor y bajo él aparecen los siguientes datos: Cantidad total de mensajes recibidos, mensajes cazados, mensajes que han sido enviados por direcciones de la lista gris, mensajes que contienen SPAM, mensajes a los que se ha quitado el SPF, mensajes reenviados y mensajes con algún tipo de malware. (Mirar la imagen 53)

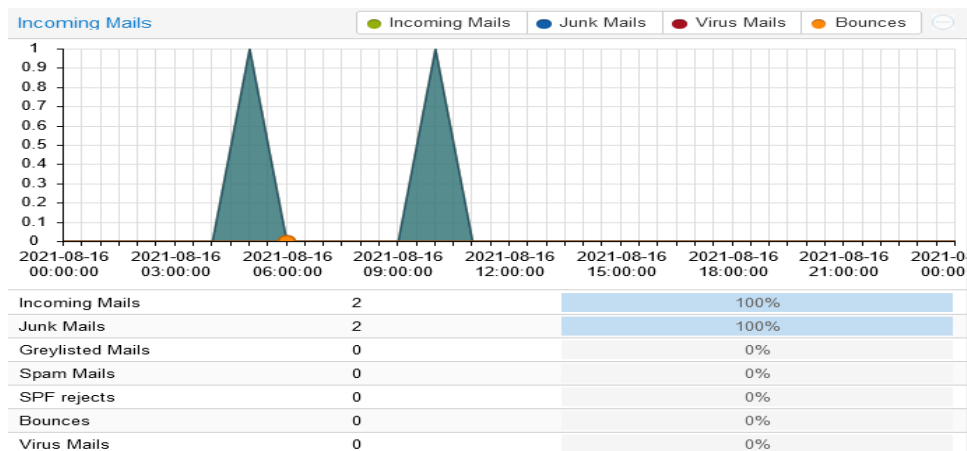


Figura 53: Gráfico de *Incoming Mails*

- *Outgoing mails*: Al contrario que en el gráfico anterior, en este aparecen los mensajes enviados desde este servidor y bajo él aparecen los siguientes datos: Número total de mensajes enviados, mensajes reenviados y mensajes con algún tipo de malware. (Mirar la imagen 54)

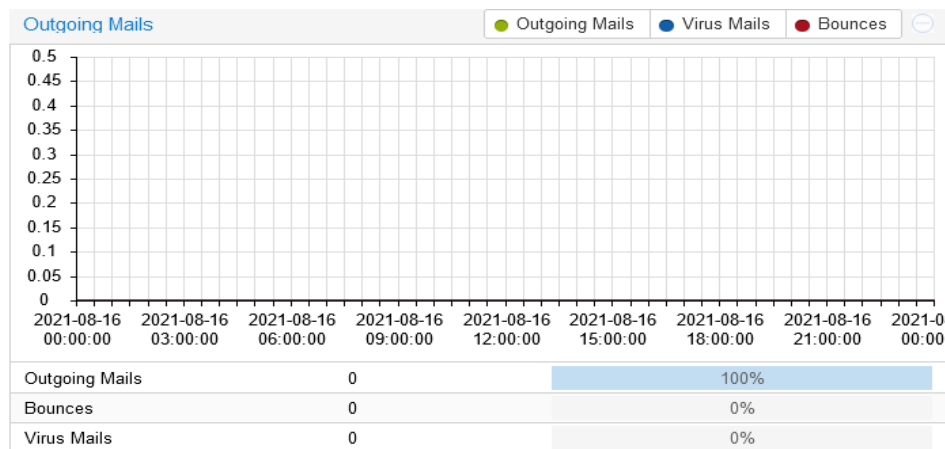


Figura 54: Gráfico de *Outgoing mails*

### 10.1. SPAM Scores

En este apartado se hace el recuento de todos los mensajes con SPAM atrapados y respecto al *score* mencionado en el punto 4 los mensajes son ordenados y se muestra la cantidad de mensajes atrapados con ese *score* y cual es el porcentaje del total. (Mirar la imagen 55)

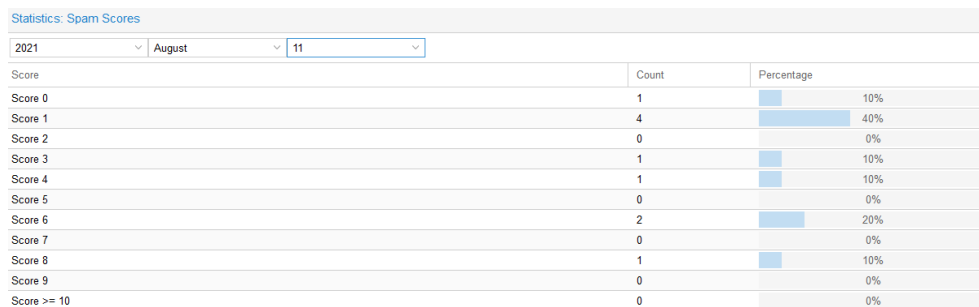


Figura 55: Sección *SPAM Scores*

## 10.2. *Virus Charts*

En esta sección se muestra lo mismo que en el anterior punto pero en vez de ser mensajes atrapados por tener contenido de SPAM son mensajes atrapados por tener algún tipo de archivo sospechoso o malware. Los datos que muestra son muy parecidos: El nombre del malware (en vez del *score*) y la cantidad de mensajes que se han atrapado con cada uno de ellos.

## 10.3. *Hourly Distribution*

En este apartado aparecen dos gráficos, en el primero se muestra cuantos mensajes llegan respecto a la hora y en el segundo se muestra lo mismo pero en vez de analizar los mensajes que entran se analizan los que salen. Las franjas horarias van de hora en hora durante las 24 horas del día. (Mirar la imagen 56)

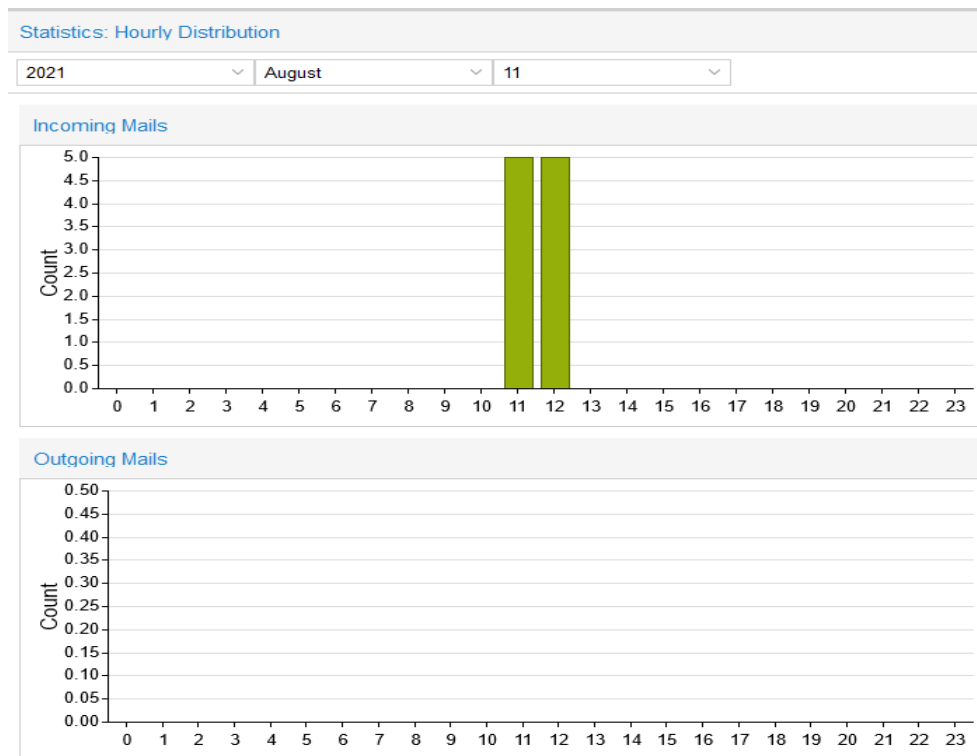


Figura 56: Gráficos que aparecen en la sección *Hourly Distribution*

#### 10.4. *Postscreen*

En este apartado aparecen los datos del servicio *postscreen* que ofrece el servidor *Proxmox Mail Gateway* respecto a los parámetros *RBL* y *PREGREET*. (Mirar la imagen 57)

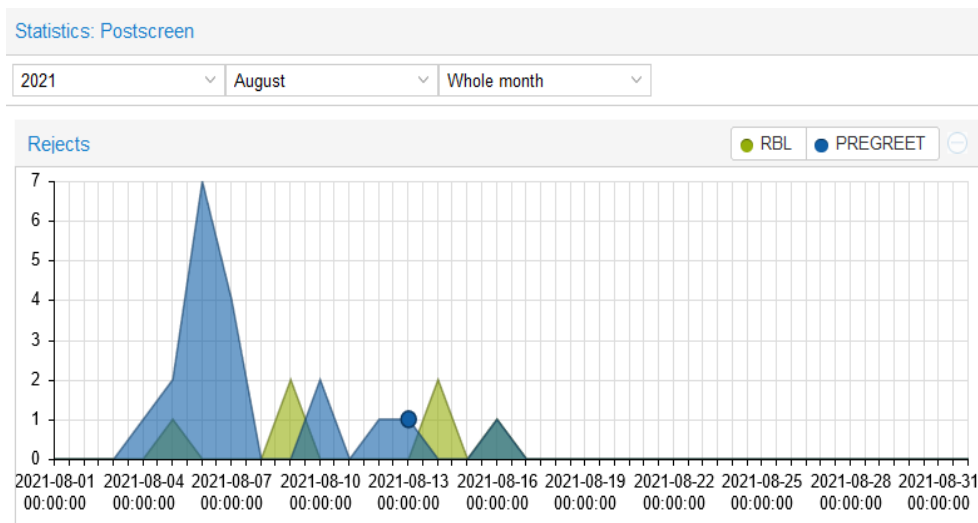


Figura 57: Gráficos que salen en la sección *Postscreen*

## 10.5. *Domain*

En este apartado se muestra el tráfico, la cantidad de mensajes, mensajes normales, mensajes con algún malware o contenido con SPAM respecto a cada dominio.

Statistics: Domain

2021 August Whole month

Incoming Outgoing

Domain (Receiver)	Traffic (MB)	Count		
		Mail	Virus	Spam
jonander.xyz	1.75	15	0	5

Figura 58: Dominios y datos que aparecen en el apartado *Domain*

## 10.6. *Sender, Receiver y Contact*

En estos apartados se filtran los mensajes respecto al emisor, receptor o los dos. La tabla que aparece la componen las siguientes columnas:

- *Sender, Receiver o Contact*: Elemento que ha enviado o recibido el correo.
- *Count*: Cantidad de mensajes que ha enviado el elemento mencionado en el punto anterior, se divide en dos partes:
  - *Mail*: Número total de mensajes en los que ha tomado parte el elemento.
  - *Virus*: Número de mensajes con algún malware que ha enviado o recibido el elemento.

- *SPAM* (Solo en la sección *Receiver*): Cantidad de mensajes clasificados como SPAM en los que ha participado el elemento.
- *Size (KB)*: Tamaño en KB en los que ha tomado parte el elemento.



## 11. Programa para enviar mensajes automáticamente

Para facilitar las pruebas se ha hecho un pequeño programa en Python para enviar correos automáticamente, lo componen los siguientes elementos:  
Para ver el código del programa pulsa sobre el siguiente link:  
<https://github.com/JonAnderAsua/emailBot>

### 11.1. Fichero main.py

#### 11.1.1. Métodos

El código del programa está en este fichero y lo componen los siguientes métodos: (Mirar la tabla 4)

Nombre	Función
getHelbideak(s)	Coger las direcciones a las que se quiera enviar el mensaje
mezuaBidali(smtpServer,login,password,msg)	Enviar el mensaje después de ser creado
getMessage(s)	Coger el texto del mensaje que se quiere enviar
main()	Método principal

Cuadro 4: Métodos que componen el fichero main.py

#### 11.1.2. Liburutegiak

Para poder crear los métodos mencionados en el punto anterior se han importado e instalado las siguientes bibliotecas: (Mirar la tabla 5) (22)

Nombre	Función
MIMEImage	Para adjuntar imágenes al mensaje que se quiere enviar
MIMEText	Para adjuntar texto al mensaje que se quiere enviar
MIMEMultipart	Para que el mensaje que se quiere enviar tenga diferentes elementos

Cuadro 5: Librerías usadas

#### 11.1.3. Parametroak

Para adecuar el programa a cada caso específico hay que modificar unos parámetros que son los siguientes: (Mirar la tabla 6)

Parámetro	NDonde
Dirección de envío	login
Contraseña de la dirección	password
Asunto del mensaje	msg['Subject']
Servidor SMTP y puerto	smtpserver

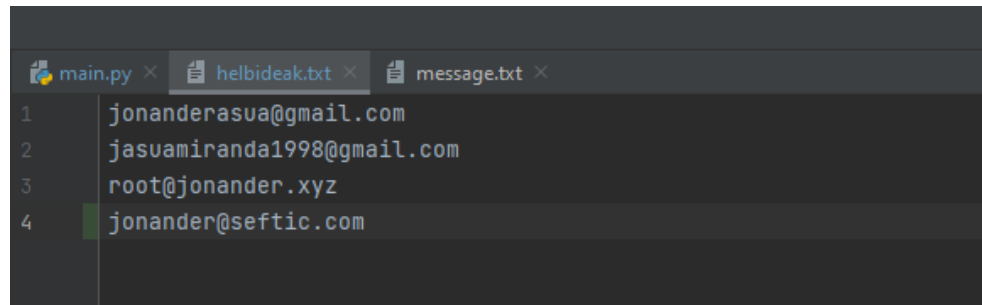
Cuadro 6: Parámetros

## 11.2. Fitxategiak

Para facilitar la creación del programa y el mensaje se han creado dos ficheros que son los siguientes:

### 11.2.1. Fichero de direcciones

En el fichero 'helbideak.txt' se determina a que direcciones de correo se quiere mandar el mensaje. Por cada línea hay un correo para facilitar el trabajo al método 'getHelbideak'. En este caso el fichero tiene la siguiente estructura: (Mirar la imagen 59)



```

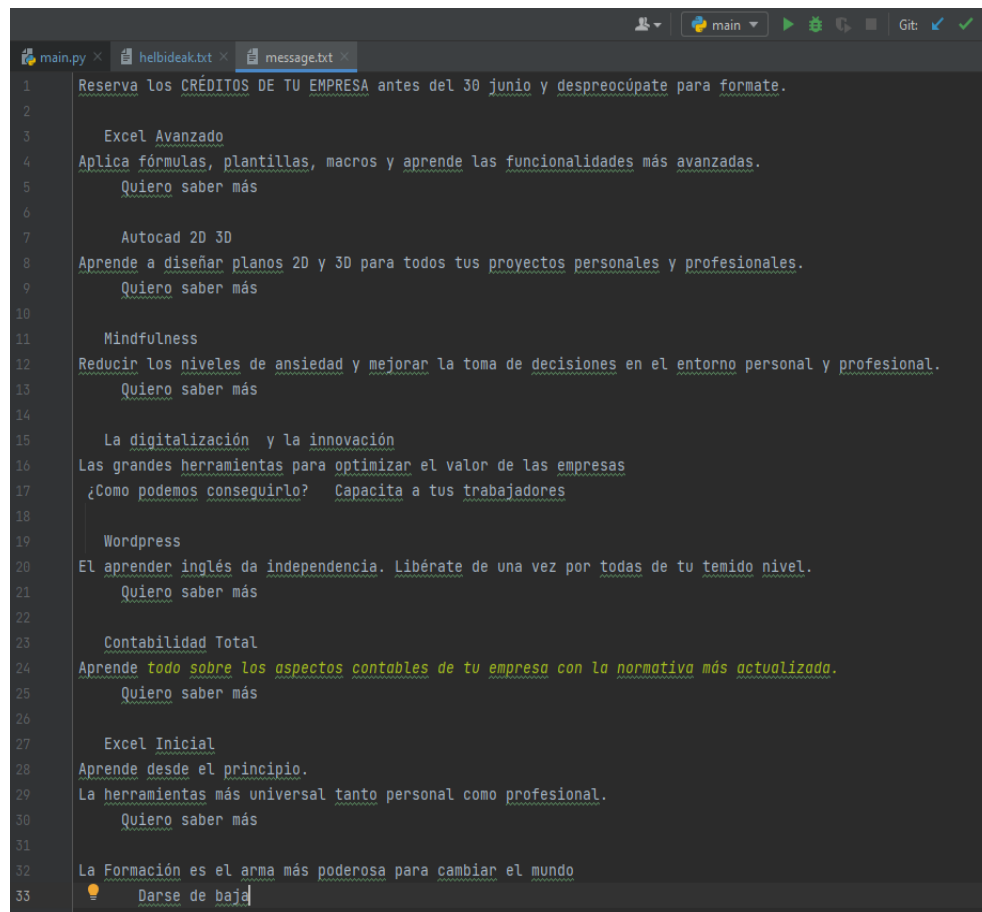
1  jonanderasua@gmail.com
2  jasuamiranda1998@gmail.com
3  root@jonander.xyz
4  jonander@seftic.com

```

Figura 59: Estructura del fichero 'helbideak.txt'

### 11.2.2. Fichero del texto del mensaje

En el fichero 'message.txt' se determina el contenido del mensaje que se quiere enviar. Dentro de él solo puede haber texto codificado en UTF-8 para facilitar el trabajo al método 'getMessage'. Este método va analizando las líneas del fichero una por una y añadiéndolas al parámetro 'message'. La estructura del fichero es la siguiente en este caso: (Mirar la imagen 60)



```
1 Reserva los CRÉDITOS DE TU EMPRESA antes del 30 junio y despreocúpate para formate.
2
3 Excel Avanzado
4 Aplica fórmulas, plantillas, macros y aprende las funcionalidades más avanzadas.
5 Quiero saber más
6
7 Autocad 2D 3D
8 Aprende a diseñar planos 2D y 3D para todos tus proyectos personales y profesionales.
9 Quiero saber más
10
11 Mindfulness
12 Reducir los niveles de ansiedad y mejorar la toma de decisiones en el entorno personal y profesional.
13 Quiero saber más
14
15 La digitalización y la innovación
16 Las grandes herramientas para optimizar el valor de las empresas
17 ¿Cómo podemos conseguirlo? Capacita a tus trabajadores
18
19 Wordpress
20 El aprender inglés da independencia. Libérate de una vez por todas de tu temido nivel.
21 Quiero saber más
22
23 Contabilidad Total
24 Aprende todo sobre los aspectos contables de tu empresa con la normativa más actualizada.
25 Quiero saber más
26
27 Excel Inicial
28 Aprende desde el principio.
29 La herramientas más universal tanto personal como profesional.
30 Quiero saber más
31
32 La Formación es el arma más poderosa para cambiar el mundo
33 📢 Darse de baja
```

Figura 60: Estructura del fichero 'message.txt'

## 12. Bibliografía

- [1] S. Informática, “Clusters de servidores.” [Online]. Available: <https://infosegur.wordpress.com/unidad-2/clusters-de-servidores>
- [2] Z. Yung, “What smtp queue is and how to manage your emails.” [Online]. Available: <https://mailtrap.io/blog/email-queuing/>
- [3] Swhosting, “Transport layer security (tls): qué es y cómo funciona.” [Online]. Available: [https://blog.mailrelay.com/es/2017/04/25/que-es-el-smtp#Como\\_funciona\\_un\\_envio\\_de\\_email\\_por\\_SMTP](https://blog.mailrelay.com/es/2017/04/25/que-es-el-smtp#Como_funciona_un_envio_de_email_por_SMTP)
- [4] A. Silgado, “¿qué es el smtp? ventajas e inconvenientes de un servidor smtp.” [Online]. Available: <https://www.swhosting.com/blog/transport-layer-security-tls-que-es-y-como-funciona/>
- [5] Mimecast, “¿qué es un spf record?” [Online]. Available: <https://www.dmarcanalyzer.com/es/spf-3/spf-record/>
- [6] H. J. Mark Drake, “Cómo instalar y utilizar postfix en ubuntu 20.04.” [Online]. Available: <https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-20-04-es>
- [7] T. SMTP, “What is an email queue.” [Online]. Available: [https://serversmtp.com/email-queue/?doing\\_wp\\_cron=1628151762.8199310302734375000000](https://serversmtp.com/email-queue/?doing_wp_cron=1628151762.8199310302734375000000)
- [8] WatchGuard, “Acerca del proxy http.” [Online]. Available: [https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/proxies/http/http\\_proxy\\_about\\_c.html](https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/proxies/http/http_proxy_about_c.html)
- [9] D. Checker, “Mx lookup.” [Online]. Available: <https://dnschecker.org/mx-lookup.php>
- [10] Msdmaguire, “Reputación del remitente y agente de análisis de protocolo.” [Online]. Available: <https://docs.microsoft.com/es-es/exchange/antispam-and-antimalware/antispam-protection/sender-reputation?view=exchserver-2019>
- [11] dnsbl.info, “What is a dnsbl?” [Online]. Available: <https://www.dnsbl.info/>
- [12] servinetwork, “Que son las listas grises y para qué sirven.” [Online]. Available: <https://blog.deservidores.com/que-son-las-listas-grises-y-para-que-sirven/>
- [13] J. Rife, “Greylisting netmask.” [Online]. Available: <https://mimedefang.roaringpenguin.narkive.com/U4RXuMqQ/greylisting-netmask>
- [14] Dietmar, “Hide internal hosts - what is it doing?” [Online]. Available: <https://forum.proxmox.com/threads/hide-internal-hosts-what-is-it-doing.41588/>

- [15] —, “Client limit.” [Online]. Available: <https://forum.proxmox.com/threads/client-limit.41470/>
- [16] Olprod, “Modificar el banner smtp en conectores de recepción.” [Online]. Available: <https://docs.microsoft.com/es-es/exchange/mail-flow/connectors/modify-smtp-banners?view=exchserver-2019>
- [17] Postfix, “Postfix before-queue content filter.” [Online]. Available: [http://www.postfix.org/SMTPD\\_PROXY\\_README.html](http://www.postfix.org/SMTPD_PROXY_README.html)
- [18] , “Mail::spamassassin::plugin::razor2 - perform razor check of messages.” [Online]. Available: [https://spamassassin.apache.org/full/3.1.x/doc/Mail\\_SpamAssassin\\_Plugin\\_Razor2.html](https://spamassassin.apache.org/full/3.1.x/doc/Mail_SpamAssassin_Plugin_Razor2.html)
- [19] NathanD, “Backscatter score function?” [Online]. Available: <https://forum.proxmox.com/threads/backscatter-score-function.79052/>
- [20] S. Kirmani, “Heuristic evaluation quality score (heqs): Defining heuristic expertise.” [Online]. Available: <https://uxpajournal.org/heuristic-evaluation-quality-score-heqs-defining-heuristic-expertise/>
- [21] Wikipedia, “Spam reporting.” [Online]. Available: [https://en.wikipedia.org/wiki/Spam\\_reporting](https://en.wikipedia.org/wiki/Spam_reporting)
- [22] , “Creating email and mime objects from scratch.” [Online]. Available: <https://docs.python.org/3/library/email.mime.html>