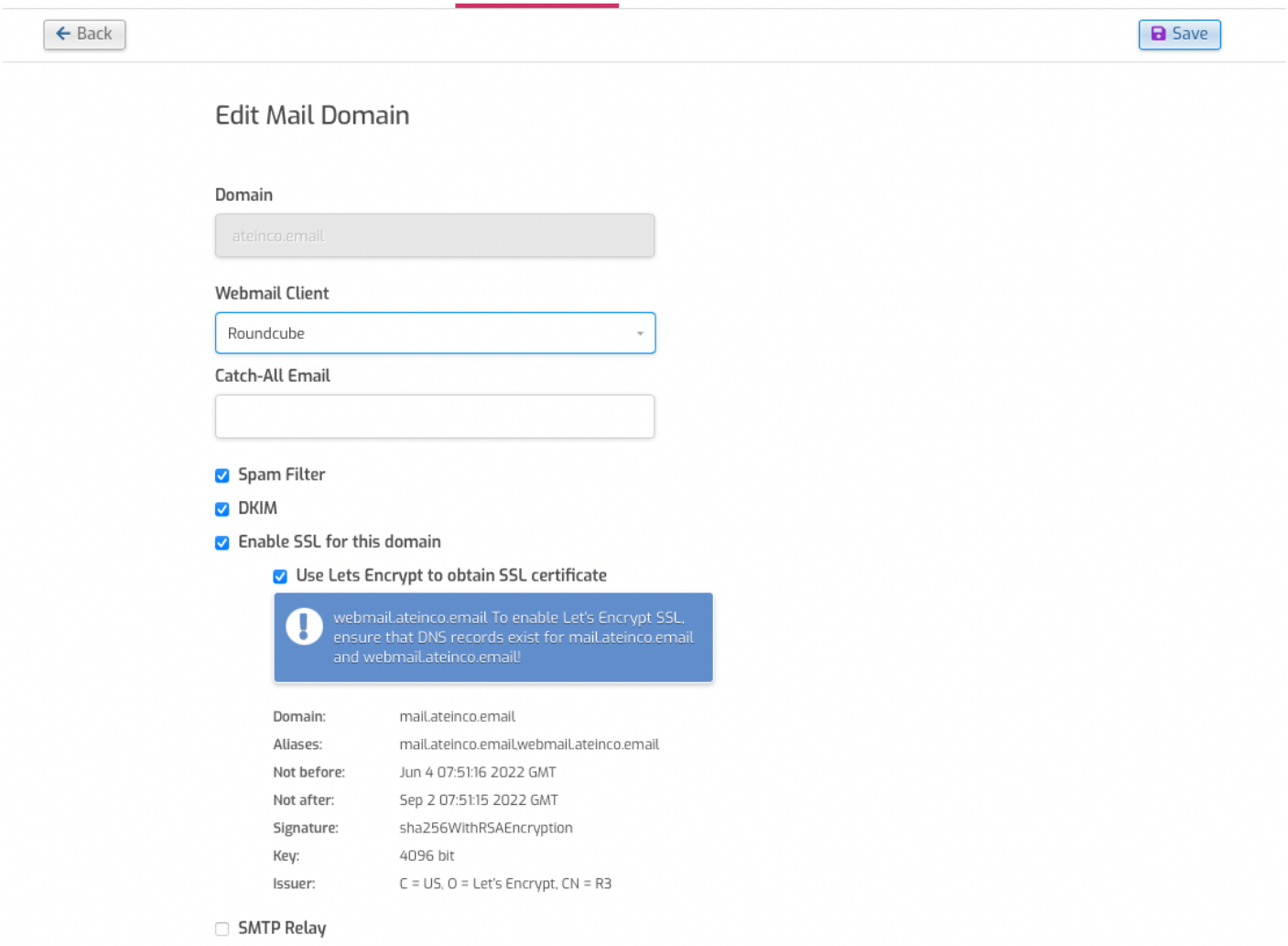
Hestia CP

Panel de Control Hestia

- DKIM y SPF en Hestia CP
- Como añadir SpamAssassin y ClamAV a HestiaCP
- Crear autoconfig y autodiscover

DKIM y SPF en Hestia CP

Al agregar un dominio de email, podemos usar DKIM para validar los correos enviados, para ello, iremos a la pantalla de dominios de correo.



Habilitamos DKIM como vemos en la imagen

Una vez que se haya creado el dominio, ahora debes crear un registro de texto (TXT) para el dominio utilizando su clave pública DKIM.

Usando SSH, el comando que necesita para obtener la clave pública DKIM es el siguiente:

```
v-list-mail-domain-dkim USER DOMAIN [FORMAT]
```

Donde USER será el usuario, DOMAIN el dominio de correo.

La parte inferior de la salida será la clave pública del dominio DKIM.

Después de eso, debes crear un registro TXT, que debe agregarse a nuestro DNS.

La entrada será **mail._domainkey** IN TXT
El contenido de la entrada DNS

```
"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUA4GNADCBiQKBgQDlTDn8Yq
b5kQ0pzaR/4DBTF4Y5jIKSJY1DAE1WFcG88qpIc66cmQdeNjfpvZzUWynuS6Grop
UodNbUsw+wvj/AcU58udlQgKL0BYtMaYSm+xbEdv5N6UAoOhOrxcXmQ/NXNzUDbs
yjr49EaDyRd25B8Jh3U6KSi3WSZzn+rKwIDAQAB"
```

> Ojo, que el registro no tiene que tener retornos de carro. Aunque aquí se muestra cortado por legibilidad

Como añadir SpamAssassin y ClamAV a HestiaCP

SpamAssassin y ClamAV, son un antispam y un antivirus para mail respectivamente, puede sernos bastante útil para ahorrarnos algunos correos molestos o peligrosos en nuestro dominio de correo.

Al instalar un servidor HestiaCP con menos de cierta memoria no instala algunos servicios para que el servidor siga funcionando de forma fluida.

Si acabas de crear un servidor con los recursos mínimos y aún no tiene contenido, en caso de necesitar estos servicios lo más práctico es crear directamente un servidor con 4 GB de RAM o 2 GB en caso de que solo queramos SpamAssassin y luego redimensionar el servidor para los recursos que necesitemos.

Hay que tener en cuenta que tener estos servicios con los recursos mínimos puede causar lentitud, por lo que este artículo está especialmente recomendado si has ido introduciendo correos y webs al servidor y poco a poco has ido añadiendo recursos y en un momento concreto requieres del antispam y antivirus.

Verificación del servidor

Para ver si nuestro servidor tiene instalado estos servicios ves a configuración y verifica que si salen en la lista de servicios, si están igual que en la captura ya los tienes instalados, en caso de que no aparezcan tendrás que realizar la instalación manualmente.

Instalación

Primero actualiza los repositorios:

```
# apt update
```

Primero tienes que instalar clamav:

```
# apt install clamav-daemon
```

Una vez tengas instalado el clamav deberás modificarl el fichero de configuración, para ello utiliza el comando:

```
# mv /etc/clamav/clamd.conf /etc/clamav/clamd.conf.old
```

Una vez tengas el antiguo archivo modificado como una copia, utiliza el comando:

```
# nano /etc/clamav/clamd.conf
```

Y copia el siguiente contenido:

```
#Automatically Generated by clamav-daemon postinst
#To reconfigure clamd run #dpkg-reconfigure clamav-daemon
#Please read /usr/share/doc/clamav-daemon/README.Debian.gz for details
LocalSocket /var/run/clamav/clamd.ctl
FixStaleSocket true
LocalSocketGroup clamav
LocalSocketMode 666
# TemporaryDirectory is not set to its default /tmp here to make overriding
# the default with environment variables TMPDIR/TMP/TEMP possible
User clamav
ScanMail true
ScanArchive true
ArchiveBlockEncrypted false
MaxDirectoryRecursion 15
FollowDirectorySymlinks false
FollowFileSymlinks false
ReadTimeout 180
MaxThreads 12
MaxConnectionQueueLength 15
LogSyslog false
LogRotate true
LogFacility LOG_LOCAL6
LogClean false
LogVerbose true
PreludeEnable no
PreludeAnalyzerName ClamAV
DatabaseDirectory /var/lib/clamav
OfficialDatabaseOnly false
SelfCheck 3600
Foreground false
Debug false
ScanPE true
MaxEmbeddedPE 10M
```

```
ScanOLE2 true
ScanPDF true
ScanHTML true
MaxHTMLNormalize 10M
MaxHTMLNoTags 2M
MaxScriptNormalize 5M
MaxZipTypeRcg 1M
ScanSWF true
ExitOnOOM false
LeaveTemporaryFiles false
AlgorithmicDetection true
ScanELF true
IdleTimeout 30
CrossFilesystems true
PhishingSignatures true
PhishingScanURLs true
PhishingAlwaysBlockSSLMismatch false
PhishingAlwaysBlockCloak false
PartitionIntersection false
DetectPUA false
ScanPartialMessages false
```

Finalmente, ejecuta los siguientes comandos para aplicar los cambios:

```
# update-rc.d clamav-daemon defaults
# service clamav-daemon restart
```

Una vez tengas Clamav hay que instalar SPAMASSASSIN:

```
# apt install spamassassin
```

Una vez tengamos el SpamAssassin instalado tienes que habilitarlo:

```
# update-rc.d spamassassin defaults
# sed -i "s/ENABLED=0/ENABLED=1/" /etc/default/spamassassin
# service spamassassin restart
```

Configuración de Exim:

Para que exim detecte los cambios tendrás que descomentar la parte de su documento de configuración donde están puestos el uso de SpamAssassin y ClamAV:

```
# sed -i "s/^#SPAMASSASSIN/SPAMASSASSIN/g" /etc/exim4/exim4.conf.template
# sed -i "s/^#CLAMD/CLAMD/g" /etc/exim4/exim4.conf.template
# sed -i "s/^#SPAM_SCORE/SPAM_SCORE/g" /etc/exim4/exim4.conf.template
# service exim4 restart
```

Configuración HestiaCP

Para ver los servicios en el panel de configuración de HestiaCP tendrás que añadir que modificar el archivo de configuración:

```
# echo "ANTIVIRUS_SYSTEM='clamav-daemon'" >> /usr/local/hestia/conf/hestia.conf
# echo "ANTISPAM_SYSTEM='spamassassin'" >> /usr/local/hestia/conf/hestia.conf
```

Ahora ya tendrás disponibles el antivirus y el antispam:

Crear autoconfig y autodiscover

Crea un registro A y/o AAAA para "autoconfig" y "autodiscover", TTL = 3600, "tu-ip" en tus servidores DNS.

Cambia al Panel de control de Hestia y crea 2 nuevos dominios (con soporte para DNS):

autodiscover.tudominio.com

autoconfig.tudominio.com

Reemplaza "tudominio.com" con tu nombre de dominio.
Debes realizar este paso para cada dominio que estés utilizando.

Activa letsencrypt para ambos dominios

Para Outlook necesitas la siguiente ruta:
/home/%username%/web/autodiscover.tudominio.com/public_html/autodiscover

autodiscover.php (Debes de reemplazar YOURDOMAIN.COM con tu nombre de dominio)

```
<?php
//get raw POST data so we can extract the email address
$data = file_get_contents("php://input");
preg_match("/\<EMailAddress\>(.*?)\<\/EMailAddress\>/", $data, $matches);
//set Content-Type
header("Content-Type: application/xml");
?>
<?php echo '<?xml version="1.0" encoding="utf-8" ?>'; ?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
<Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
<Account>
<AccountType>email</AccountType>
<Action>settings</Action>
```

```
<Protocol>
<Type>IMAP</Type>
<Server>mail.YOURDOMAIN.COM</Server>
<Port>993</Port>
<SSL>on</SSL>
<LoginName><?php echo $matches[1]; ?></LoginName>
<AuthRequired>on</AuthRequired>
</Protocol>
<Protocol>
<Type>POP3</Type>
<Server>mail.YOURDOMAIN.COM</Server>
<Port>995</Port>
<SSL>on</SSL>
<LoginName><?php echo $matches[1]; ?></LoginName>
<AuthRequired>on</AuthRequired>
</Protocol>
<Protocol>
<Type>SMTP</Type>
<Server>mail.YOURDOMAIN.COM</Server>
<Port>465</Port>
<SSL>on</SSL>
<LoginName><?php echo $matches[1]; ?></LoginName>
<AuthRequired>on</AuthRequired>
</Protocol>
</Account>
</Response>
</Autodiscover>
```

Para Thunderbid, la ruta es:
/home/%username%/web/autoconfig.tudominio.com/public_html/mail

config-v1.1.xml en la carpeta mail (Debes de reemplazar YOURDOMAIN.COM con tu nombre de dominio)

```
<?xml version="1.0" encoding="UTF-8"?>

<clientConfig version="1.1">
  <emailProvider id="mail.YOURDOMAIN.COM">
<domain>YOURDOMAIN.COM</domain>
    <displayName>YOURDOMAIN.COM Mail</displayName>
    <displayShortName>strehmels</displayShortName>
```

```
    <incomingServer type="imap">
      <hostname>mail.YOURDOMAIN.COM</hostname>
      <port>143</port>
      <socketType>STARTTLS</socketType>
      <authentication>password-cleartext</authentication>
      <username>%EMAILADDRESS%</username>
    </incomingServer>
    <incomingServer type="imap">
      <hostname>mail.YOURDOMAIN.COM</hostname>
      <port>993</port>
      <socketType>SSL</socketType>
      <authentication>password-encrypted</authentication>
      <username>%EMAILADDRESS%</username>
    </incomingServer>
    <incomingServer type="pop3">
      <hostname>mail.YOURDOMAIN.COM</hostname>
      <port>995</port>
      <socketType>SSL</socketType>
      <authentication>password-cleartext</authentication>
      <username>%EMAILADDRESS%</username>
    </incomingServer>
    <incomingServer type="pop3">
      <hostname>mail.YOURDOMAIN.COM</hostname>
      <port>110</port>
      <socketType>STARTTLS</socketType>
      <authentication>password-cleartext</authentication>
      <username>%EMAILADDRESS%</username>
    </incomingServer>
    <outgoingServer type="smtp">
      <hostname>mail.YOURDOMAIN.COM</hostname>
      <port>587</port>
      <socketType>STARTTLS</socketType>
      <authentication>password-cleartext</authentication>
      <username>%EMAILADDRESS%</username>
    </outgoingServer>
    <outgoingServer type="smtp">
      <hostname>mail.YOURDOMAIN.COM</hostname>
      <port>465</port>
      <socketType>SSL</socketType>
      <authentication>password-encrypted</authentication>
```

```
      <username>%EMAILADDRESS%</username>
    </outgoingServer>
  </emailProvider>
</clientConfig>
```

Copia los archivos de muestra en el subdirectorio apropiado.